Univerzita Pardubice

Dopravní fakulta Jana Pernera

Analýza rizika aplikace systému ETCS

Jakub Marek

Disertační práce

2014

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.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Černošicích dne 7. 1. 2014

Ing. Jakub Marek

PŘEDSLOV

Při vývoji libovolného bezpečnostně-kritického systému je třeba věnovat patřičnou pozornost správnému stanovení bezpečnostních požadavků. Jejich stanovování se v oblasti železniční zabezpečovací techniky děje na základě analýzy rizika. V době psaní této disertační práce neexistovala žádná popsaná, ucelená a dostupná metodika analýzy rizika. A dosud existuje pouze soubor požadavků, které musí analýza rizika naplňovat, což není postačující. Je třeba nejdříve metodiku analýzy rizika dostatečně podrobně zpracovat a popsat, což je hlavním cílem této disertační práce, a teprve potom ji je možno plnohodnotně aplikovat. Autor této disertační práce se na pracovišti AŽD Praha podílí na vývoji aplikace systému ETCS v ČR, čili případné praktické příklady lze očekávat právě z této oblasti, přičemž dosažené výsledky je snaha zobecňovat na celou oblast železniční zabezpečovací techniky.

Na tomto místě bych také velmi rád poděkoval svému školiteli, panu doc. Ing. Milanu Kunhartovi, CSc., významnému odborníkovi v oblasti železniční zabezpečovací techniky, za jeho užitečné rady, odbornou pomoc a ochotu při vypracovávání mé disertační práce. Stejně tak mu děkuji za vedení mé osoby, jakožto doktoranda, v průběhu celého mého doktorského studia. Děkuji mu též za zprostředkování výuky velmi zajímavých předmětů souvisejících s mým zaměřením, jejichž výuku zajišťovali významní odborníci v oblasti železniční zabezpečovací techniky. Jmenovitě šlo o pana doc. Ing. Ivana Konečného, CSc., (ZČU v Plzni), pana Ing. Václava Chudáčka, CSc., (ZČU v Plzni) a v neposlední řadě o pana prof. Ing. Karola Rástočného, PhD., (ŽU v Žilině).

Rovněž bych na tomto místě chtěl poděkovat pracovníkům Drážní inspekce, státní instituce, která odborně zjišťuje příčiny mimořádných (nehodových) událostí a vykonává státní dozor na dráhách, jmenovitě panu Mgr. Janu Kučerovi a panu Ing. Robertu Hrdinovi, za jejich vstřícnost, za poskytnutí potřebných údajů o mimořádných událostech, které byly následně v předkládané disertační práci použity pro odvození kritérií přijatelnosti rizik.

Neméně pak zde děkuji své rodině a svým blízkým za podporu a pochopení, které mi v průběhu mého dosavadního studia dávali a dávají.

ANOTACE

Práce je z oblasti železniční zabezpečovací techniky, soustřeďuje se na analýzu rizika evropského vlakového zabezpečovacího systému ETCS. Primárně odvozuje metodiku analýzy rizika železničních zabezpečovacích systémů, přičemž se v konkrétních případech věnuje právě analýze rizika aplikace systému ETCS a s tím souvisejícím specifikům. Dosažené výsledky se ale vždy snaží zobecňovat na celou oblast železniční zabezpečovací techniky.

KLÍČOVÁ SLOVA

železniční zabezpečovací technika, ERTMS, ETCS, analýza rizika

TITLE

Risk analysis of ETCS application

ANNOTATION

This work is from the field of railway signalling systems, it is focused on risk analysis of European Train Control System (ETCS). It primarily derives methodology of risk analysis of railway systems; in this process, it is dedicated to risk analysis of ETCS application in particular cases and with it related particularities. However, there is always an attempt to generalise reached results to the whole railway signalling systems field.

KEYWORDS

railway signalling systems, ERTMS, ETCS, risk analysis

OBSAH

ÚVOD

Předkládaná disertační práce se zabývá oblastí analýzy rizika aplikace systému evropského vlakového zabezpečovacího systému ETCS (European Train Control System). Jde tedy o stanovení metodiky téměř neprobádaného a systematicky jednotně nestanoveného procesu analýzy rizika konkrétního železničního zabezpečovacího systému, jehož aplikace je v dnešních dnech v České republice (a to nejen zde v České republice, ale také po celé Evropě, dnes již dokonce můžeme říci i po celém světě – viz např. [***EWC***]) více než aktuální. Je zde totiž racionální snaha nahradit velké množství různých, navzájem nekompatibilních vlakových zabezpečovacích systémů právě systémem ETCS, který má vytvořit jednotný standard vlakového zabezpečovacího systému.

Zmíněné sjednocení různých vlakových zabezpečovacích systémů má přispět k tzv. interoperabilitě evropského železničního systému. Interoperabilita zde znamená takový stav, kdy libovolné interoperabilní vozidlo bude moci pojíždět libovolnou interoperabilní železniční trať. Dosažení tohoto stavu pod vizí získání konkurenceschopnější železniční dopravy je jednou ze snah Evropské unie [***ECE***]. Z tohoto titulu bylo identifikováno šest hlavních nákladních železničních koridorů, na nichž má být v poměrně krátké době nasazena traťová část systému ERTMS/ETCS [***VAR***] (viz též obr. 0.1). Jeden z těchto koridorů (ERTMS koridor E) je trasován přes Českou republiku, která se k nasazení traťové části systému ERTMS/ETCS (dále jen ETCS) na české části tohoto koridoru zavázala podepsáním Dopisu o zájmu na rozvoji koridoru E [***EČR***].

*Obr. 0.1 – Mapa jádra šesti ERTMS koridorů (převzato z [**EDP**])*

Situace v České republice je aktuálně taková, že v provozu již je pilotní projekt ETCS v úseku Kolín–Poříčany [***ŘČB***]. Následný první komerční projekt ETCS v úseku Břeclav–Kolín je v realizaci a v blízké době se očekává, že bude vypsána soutěž na vybavení zbylé části české části ERTMS koridoru E v úseku Kolín–Děčín traťovou částí systému ETCS. Je tedy více než aktuální řešit otázku identifikování rizik plynoucích z nebezpečí souvisejících s tímto systémem a přijímat adekvátní bezpečnostní opatření. Prostředkem k tomu může být právě analýza rizika tohoto železničního zabezpečovacího systému. Pro úplnost jen dodejme, že některá rizika byla již v souvislosti s tímto systémem identifikována na úrovni technických specifikací tohoto systému, tedy na úrovni UNISIG/ERA. Některá z nich jsou na této úrovni řešena a úspěšně vyřešena. Některými se bude třeba zabývat na úrovni konkrétních projektů aplikací systému ETCS, tedy opět patrně v rámci analýzy rizika.

Je tedy zřejmé, že řídit rizika související se systémem ETCS, stejně jako s každým jiným bezpečnostně-kritickým systémem, je nutností. A to nikoli jen proto, že to pro železniční zabezpečovací systémy vyžadují závazné evropské normy, jako jsou normy řady ČSN EN 50126-1:2007, ČSN EN 50129:2003, ČSN EN 50159:2011, ČSN EN 50128:2012, které pro tuto oblast zcela nahrazují evropskou normu ČSN EN 61508:2011, která je jinak platná pro bezpečnostně-kritické systémy obecně. Závaznost těchto norem nevyplývá jen z požadavku směrnice SŽDC č. 34 [***34***], kterážto naplnění požadavků souboru těchto norem považuje za podmínkou nutnou pro vydání kladného hodnocení bezpečnosti zabezpečovacího systému, bez něhož není možno tento systém používat na železniční dopravní cestě ve vlastnictví státu (SŽDC); ale též z požadavků technických specifikací pro interoperabilitu pro oblast řízení a zabezpečení [***TSI***], které jejich použití při návrhu systému ETCS považují za mandatorní.

Z předchozího je patrno, že je třeba a v současné době s ohledem na právě probíhající aplikaci systému ETCS v České republice taktéž velmi aktuální se řízením rizik souvisejících s tímto systémem, obecně s každým železničním zabezpečovacím systémem, řádně zabývat. Že je třeba pro to stanovit vhodný postup, který bohužel není ani ve výše citovaných normách jednotný, avšak vyžadovaný. A že je třeba následně vybrat, případně vytvořit pro tento postup vhodné metody, jejichž použití je z tohoto pohledu výhodné. Tedy je třeba vymyslet a dostatečně podrobně popsat metodiku toto zajišťující, což je hlavním cílem této disertační práce.

V souvislosti s analýzou rizika, obecně s řízením rizik železničních zabezpečovacích systémů obecně taktéž zůstává v našich podmínkách dosud neřešena dle mého názoru velmi klíčová otázka, kterou je vlastní hodnocení rizik. S tím jsou úzce spjata pravidla, na jejichž základě se má (zjednodušeně řečeno) rozhodnout, jaká úroveň rizika je ještě v konkrétních podmínkách dané železnice přijatelná a jaká již nikoli. V podmínkách České republiky, a jsem přesvědčen, že nejen zde v České republice, ale i v mnoha jiných státech, nebyla tato pravidla – označovaná jako kritéria přijatelnosti rizik – dosud stanovena. Čili i toto jejich stanovení bude jedním z cílů této disertační práce. Je samozřejmé, že pro jejich případné následné reálné použití v praxi bude nutno tato pravidla projednat a nechat odsouhlasit od příslušného provozovatele drážní dopravy, kterým je v případě traťové části systému ETCS dle národního implementačního plánu [***NIP***] SŽDC.

Další zajímavé již výše jednou naznačené specifikum v oblasti řízení rizik železničních zabezpečovacích systémů týkající se systému ETCS, jakožto nadnárodního projektu, jehož definice vzniká jak na národní úrovni (specifikace konkrétních projektů ETCS, jinými slovy požadavky na generickou a specifickou aplikaci), tak na úrovni nadnárodní (obecně závazné specifikace systému ETCS, požadavky na generický produkt) v této oblasti k řešení představuje otázka zahrnutí již na nadnárodní úrovni vykonaných bezpečnostních analýz a identifikovaných nebezpečí, potažmo rizik do analýz vykonaných, popřípadě nebezpečí identifikovaných na národní úrovni. Čili i toto bude jedním z podcílů této disertační práce.

Tvrzením, že aktuálních, ovšem také dosud nezodpovězených otázek souvisejících s řízením rizik železničních zabezpečovacích systémů, konkrétně zde s řízením rizik aplikace systému ETCS, je v tuto chvíli mnoho, bych si dovolil ukončit úvod této disertační práce, která se právě hledáním odpovědí na tyto otázky má zabývat. Zajímavé je, že jde o otázky do jisté míry filosofické, a to i přes to, že se primárně týkají technických systémů.

1 SOUČASNÝ STAV POZNÁNÍ V DANÉ OBLASTI

Tato kapitola shrnuje současný stav poznání v oblasti zaměření této disertační práce, tedy v oblasti analýzy rizika železničních systémů. Zaměřuje se na analýzu rizika s ohledem na potřeby aplikace systému evropského vlakového zabezpečovače ETCS v podmínkách České republiky, potažmo obecněji s ohledem na potřeby železniční zabezpečovací techniky (dále v textu jen na analýzu rizika).

1.1 Analýza rizika obecně

Tato podkapitola shrnuje poznatky o analýze rizika a poznatky s ní související získané především ze souboru evropských norem platných pro železniční zabezpečovací techniku, a to [***126-1***], [***129***], [***128***] a [***159***] s ohledem na normu [***508***], jež je platná pro bezpečnostně-kritické systémy obecně, a s ohledem na další pro tuto oblast relevantní odborné články a publikace, především jde o [***BŽZS***], [***ŽZT***], [***BMZS***], [***ARSP***].

1.1.1 Koncepce rizika

Koncepce rizika uvedená v normě [***126-1***] má umožnit, aby byly pro méně kritické funkce navrhovány jednodušší a tím pádem i levnější systémy [***BMZS***]. Tato koncepce vychází ze základní myšlenky, že různé druhy nebezpečí se vyskytují různě často a že jejich možné následky jsou různě závažné. Kombinaci obou těchto faktorů v sobě zahrnuje právě riziko, které je dáno následujícím vztahem:

$$R = Č \times N, \tag{1.1}$$

kde R … riziko plynoucí z nebezpečí,
Č … četnost výskytu nebezpečí (události/událostí jej vyvolávající),
N … možné následky nebezpečí (škody, kterou může způsobit).

Ačkoli je definice pojmu rizika ve výše uvedených normách formulována pokaždé překvapivě poněkud odlišným způsobem, je riziko nejčastěji slovně definováno jako kombinace četnosti výskytu nebezpečí a jeho následků. Jistou nekonzistenci však v této definici rizika spatřuji v tom, že ne každé nebezpečí musí vést k nehodě, čili k nežádoucím ztrátám. Nebezpečí totiž představuje stav systému nebo procesu, ve kterém jsou „pouze“ splněny podmínky příznivé pro vznik nehody [***ŽZT***]. Tento stav je ovšem z bezpečnostního hlediska již samozřejmě nepřípustný, a to i přes to, že vznik škody ve skutečnosti přímo nepředstavuje.

K nehodě při něm totiž ještě nemusí nutně dojít. Výše zmíněnou nekonzistenci tedy vidím v tom, že se zde kombinují dva do jisté míry nesourodé činitelé – četnost výskytu nebezpečí a jeho následků, ke kterým ale i při výskytu daného nebezpečí sice může, ale také nemusí nutně dojít. Tuto nekonzistenci je možno řešit při ohodnocení následků buď uvážením sumy všech možných následků, nebo uvážením jen těch nejhorších možných následků.

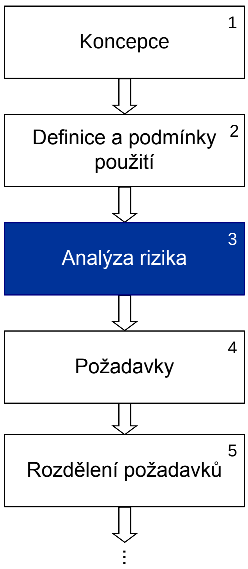
Četnost výskytu lze v této definici rizika v některých případech nahradit pravděpodobností výskytu daného nebezpečí (pozn. tato skutečnost již nebude dále v textu takto explicitně uváděna, bude používána pouze četnost, popř. intenzita výskytu). Riziko potom představuje ukazatel, který souhrnně charakterizuje jednotlivá nebezpečí a který v principu umožňuje provést jejich relativně snadné porovnávání. Z hlediska rizika je například možno konstatovat, že nebezpečí, které nastane jedenkrát za rok a u nějž může v nejhorším uvažovaném případě dojít k lehkému zranění dvou osob, je stejné jako nebezpečí, které nastane dvakrát za rok a může u něj v nejhorším uvažovaném případě dojít k lehkému zranění jen jedné osoby. Je zřejmé, že v tomto případě by i požadavky na bezpečnost funkcí, které mohou způsobit tato nebezpečí, měly být stejné, neboť i rizika plynoucí z obou nebezpečí jsou stejná. Z tohoto příkladu je též patrná existence vztahu mezi rizikem a bezpečnostními požadavky na systém.

1.1.2 Účel analýzy rizika

Účel analýzy rizika není v žádné z výše uvedených norem explicitně stanoven. Tyto normy pouze obsahují požadavky na celkový proces analýzy rizika, které musí být při vývoji zabezpečovacích systémů splněny. Ovšem nástin účelu analýzy rizika lze nalézt například v publikacích [***ŽZT***], [***ARSP***] či [***BŽZS***]. Na základě této znalosti lze říci, že účel vlastní analýzy rizika spočívá v analýze rizik vyplývajících z jednotlivých nebezpečí, která souvisejí s navrhovaným systémem, aby se odhalily jeho slabiny (kritická místa) a určila (navrhnula) ochranná opatření (pro nezbytné snížení rizika) [***ŽZT***]. Na základě analýzy rizika se také stanoví bezpečnostní požadavky na systém [***BŽZS***].

Analýza rizika musí být začleněna do procesu vývoje každého zabezpečovacího systému [***126-1***]. Proces vývoje takového systému je možno definovat jeho životním cyklem, který tvoří posloupnost etap, z nichž každá etapa zahrnuje činnosti, které během ní musí být vykonány. Jednou z počátečních etap tohoto životního cyklu je právě analýza rizika (viz obr. 1.1). U zabezpečovacích systémů musí jejich životní cyklus, resp. činnosti v rámci něj vykonávané odpovídat životnímu cyklu, resp. činnostem stanovených normou [***126-1***], popř. [***129***], anebo může být definován životní cyklus vlastní. Nicméně i při definici vlastního životního cyklu musí být analýza rizika jeho nedílnou součástí, neboť představuje činnost, kterou je nutno bezpodmínečně v rámci vývoje zabezpečovacího systému vykonat.

Začlenění analýzy rizika do procesu vývoje zabezpečovacího systému je patrné z jeho životního cyklu (obr. 1.1). Z tohoto konkrétního životního cyklu je vidět, že se analýza rizika provádí na samém počátku vývoje zabezpečovacího systému. Rovněž je z něj zjevné, že analýza rizika vychází z výsledků získaných v etapách předcházejících, tj. z výsledků etap koncepce a definice systému (1. a 2. etapa). Obdobně lze odvodit, že výsledky analýzy rizika jsou použity při specifikaci požadavků na systém (4. a 5. etapa). V tomto konkrétním případě (obr. 1.1) byl zvolen životní cyklus dle normy [***126-1***]. Ovšem, jak již bylo vysvětleno výše, i při jiném životním cyklu musí analýza rizika předcházet specifikaci požadavků na zabezpečovací systém, a to zejména bezpečnostních.



*Obr. 1.1 – Začlenění analýzy rizika do životního cyklu dle [**126-1**]*

Z normy [***126-1***] tedy vyplývá, že stanovení bezpečnostních požadavků na systém musí vycházet z analýzy rizika. Analýza rizika proto musí být provedena na samém počátku vývoje systému (tedy v době, kdy sice již existuje rámcová představa o systému ve formě koncepce, definice a podmínek použití, ale kdy ještě nebyly specifikovány konkrétní požadavky na vyvíjený systém) a následně upravována během celého životního cyklu, což je další požadavek na analýzu rizika (viz např. [***126-1***]). Shrneme-li předcházející poznatky do jedné věty, pak je možno konstatovat, že *účelem analýzy rizika* jako takové *je příprava podkladů pro stanovení bezpečnostních požadavků* na zabezpečovací systém.

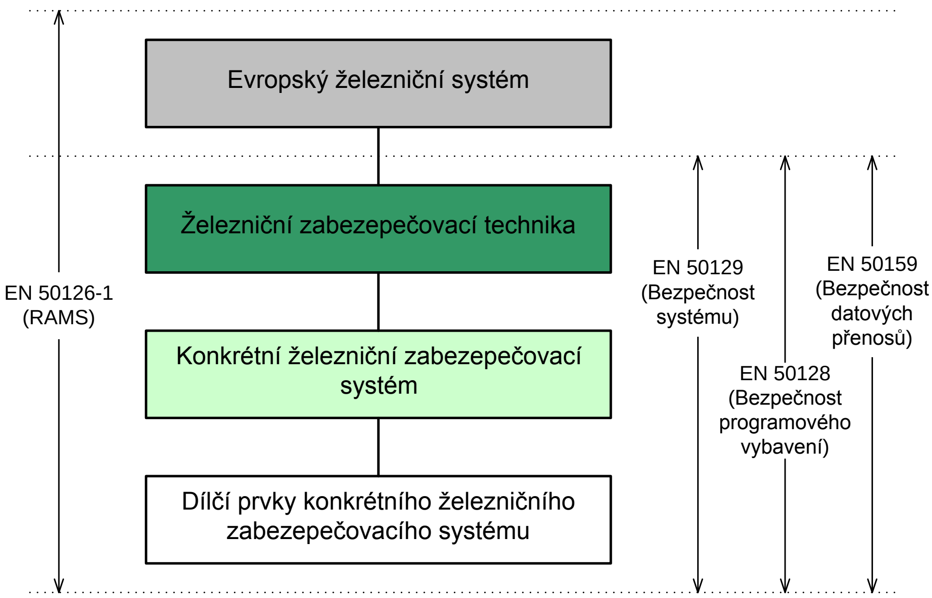
1.2 Analýza rizika dle evropských normativů

Zde je rozebrán a okomentován současný stav poznání v oblasti zaměření této disertační práce s důrazem na různé přístupy k tvorbě analýzy rizika železničních zabezpečovacích systémů (dále jen analýzy rizika) v závislosti na konkrétních požadavcích kladených relevantními, závaznými normativy. Tyto rozdílné přístupy bude třeba v rámci připravované metodiky sjednotit tak, aby navržená metodika naplňovala všechny požadavky těchto evropských norem a směrnic. Za tímto účelem budou posuzovány evropské normy týkající se přímo železničního systému či železniční zabezpečovací techniky, kterými jsou [***126-1***], [***128***], [***129***], [***159***], a evropská směrnice týkající se železničního systému se zaměřením na analyzování dopadů jeho změn 2004/49/EC [***49***], která podobně jako výše uvedené normy vyžaduje provedení analýzy rizika strukturálních systémů, mezi něž se podle ní řadí i zabezpečovací systémy (tedy oblast zabezpečovací techniky).

Připomeňme, že současný stav u nás a v zahraniční v oblasti analýzy rizika železniční zabezpečovací techniky by měl být stejný, sjednocený právě citovanými evropskými normativy, tudíž by se v rámci Evropy (EU) neměl lišit. Přičemž platnost těchto normativů dnes již překračuje hranice EU, viz např. aplikaci souboru evropských norem EN 5012x na železnicích v Rusku [***José***] i [***RusKonf***]. Lze ale předpokládat, že současný stav v této oblasti se zcela jistě liší ve způsobu plnění požadavků těchto normativů, což ale v tuto chvíli nedokážu ani potvrdit ani vyvrátit. Tato má hypotéza ovšem vychází z faktu, že evropské normativy je snaha obecně tvořit takovým způsobem, aby umožnily svou co nejsnazší implementaci, a to s co nejmenším narušením dosavadních národních pravidel a zvyklostí [***DissPpt***]. Záměrně tudíž nepožadují žádný konkrétní způsob naplňování svých požadavků.

Ještě je třeba na tomto místě objasnit výběr evropských normativů. Ač zabezpečovací systémy představují z hlediska nežádoucích důsledků při jejich selhání bezpečnostně-kritický systém, nebyla primárně uvažována jinak pro tyto systémy obecně závazná mezinárodní elektrotechnická norma IEC 61508 [***508***]. Důvodem je skutečnost, že normy řady EN 5012x jsou psány v souladu s touto mezinárodní elektrotechnickou normou, a to takovým způsobem, že platí, že když jsou splněny požadavky souboru norem EN 5012x, jsou automaticky splněny i požadavky normy [***508***]. Toto je mimo jiné stanoveno v úvodní části normy [***129***].

Podíváme-li se dále na souhrn evropských norem, které se zabývají bezpečností železniční zabezpečovací techniky (viz obr. 1.2), je z nich s jistotou nutno respektovat obecnou normu [***126-1***] a [***129***]. Ostatní normy (tj. [***128***] a [***159***]) jsou normy, které ve specifických oblastech blíže upravují požadavky na obecnou bezpečnost železničních zabezpečovacích systémů (konkrétně v oblasti softwaru a datových komunikací v tomto pořadí). Třebaže z obou těchto norem vyplývá, že analýzu rizika je třeba během návrhu zabezpečovacího systému vykonat, relevantní požadavky týkající se konkrétněji této činnosti se v nich nevyskytují. Například norma [***128***] se o analýze rizika zmiňuje jen ve svém úvodu a pouze v souvislosti s odkazy na normy [***126-1***] a [***129***].



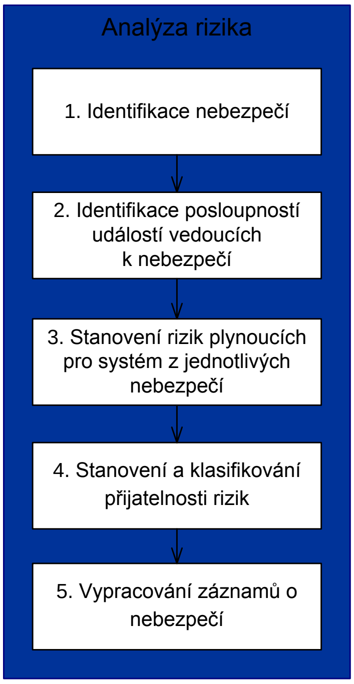
Obr. 1.2 – Působnosti evropských norem týkajících se bezpečnosti železniční zabezpečovací techniky

Můžeme tedy konstatovat, že směrodatné jsou pro hledání požadavků na analýzu rizika zejména normy EN 50126-1, EN 50129 a EN 50159, resp. u nás zezávazněné české verze těchto norem označené jako ČSN EN 50126-1, ČSN EN 50129 a ČSN EN 50159 (dále jen [***126-1***], [***129***], [***159***]). Ovšem český překlad těchto evropských norem není dle mého názoru proveden vždy zcela korektně a konzistentně, tudíž je dále v této práci snaha skutečnosti uvedené v těchto českých mutacích dávat do souladu s jejich originálním anglickým zněním a částečně i do souladu mezi sebou. Bližšími podrobnosti se věnují následující kapitoly 1.2.1, 1.2.2, 1.2.3, popř. 1.2.4. Vedle těchto norem je možno jistý druh inspirace nalézt také v nařízení komise [***49***], jehož závaznost je však v oblasti železniční zabezpečovací techniky diskutabilní (více viz kap. 1.2.5).

Následující podkapitoly jsou zaměřeny nikoli přímo na analýzu rizika, ale na širší souvislosti, tj. jsou rovněž zahrnuty i záležitosti s analýzou rizika související ne zcela přímo. Co se však týče přístupu k tvorbě analýzy rizika, lze říci, že je obecně dán posloupností kroků, které stanovuje příslušná norma, popřípadě nařízení. Ač by se dalo očekávat, že tento postup bude (alespoň v rámci souboru evropských norem vypracovaných pro oblast zabezpečovací techniky de facto současně) jednotný, zdá se, že tomu tak úplně není. Rozdílnost jednotlivých přístupů je zřejmá z následujících komentovaných popisů.

1.2.1 Pohled evropské normy ČSN EN 50126-1:2007

Norma [***126-1***] se analýze rizika systematicky věnuje v kapitole 6.3, ovšem odkazuje se na ni v celém svém textu, což je způsobeno skutečností, že analýza rizika má prostupovat celým životním cyklem vyvíjeného zabezpečovacího systému. Dle této normy má být v rámci analýzy rizika nejprve provedena identifikace nebezpečí (krok 1 dle obr. 1.3), při níž má být vykonáno systematické identifikování všech za normálních okolností předvídatelných nebezpečí spojených se systémem v jeho provozním prostředí a stanovení jejich priorit (pozn. z hlediska nutnosti jejich odstranění). Dále pak mají být identifikovány posloupnosti událostí vedoucí k identifikovaným nebezpečím (krok 2 dle obr. 1.3) a stanovena rizika plynoucí z identifikovaných nebezpečí (krok 3 dle obr. 1.3).



*Obr. 1.3 – Kroky analýzy rizika požadované normou ČSN EN 50126-1 [**126-1**]*

Pro stanovení rizika je třeba nejprve provést hodnocení identifikovaného nebezpečí z hlediska četnosti, resp. pravděpodobnosti jeho výskytu (dále jen četnosti výskytu) a jeho následků. Pro takovéto hodnocení nebezpečí stanovuje norma [***126-1***] několik typických kategorií četností výskytu nebezpečí (uvedeno v tab. 1.1) a několik typických úrovní závažnosti (uvedeno v tab. 1.2).

Kategorie četnosti výskytu	Popis
Častá	Je pravděpodobný častý výskyt. Nebezpečí je trvalé.
Pravděpodobná	Vyskytnou se několikrát. Lze očekávat, že nebezpečí nastane často.
Občasná	Pravděpodobně se vyskytnou několikrát. Lze očekávat, že nebezpečí nastane několikrát.
Malá	Pravděpodobně se vyskytnou někdy během životního cyklu systému. Je rozumné předpokládat, že nebezpečí nastane.
Nepravděpodobná	Výskyt je nepravděpodobný, ale možný. Lze předpokládat, že nebezpečí může výjimečně nastat.
Vysoce nepravděpodobná	Výskyt je krajně nepravděpodobný. Lze předpokládat, že nebezpečí nemusí nastat.

*Tab. 1.1 – Typické kategorie čestnosti výskytu nebezpečí dle [**126-1**]*

Úroveň závažnosti	Důsledky	
	pro osoby	pro provoz
Katastrofická	Oběti na životech a/nebo mnoho vážných zranění a/nebo těžké poškození životního prostředí	
Kritická	Jedno úmrtí a/nebo vážné zranění a/nebo významné poškození životního prostředí	Ztráta důležitého systému
Okrajová	Lehčí zranění a/nebo významné ohrožení životního prostředí	Vážné poškození systému (systémů)
Nevýznamná	Možné lehčí zranění	Malé poškození systému

*Tab. 1.2 – Typické úrovně závažnosti nebezpečí dle [**126-1**]*

U obou kategorií (jak pro výskyt nebezpečí, tak pro jeho následky) je uveden pouze kvalitativní popis. Je zřejmé, že takovéto hodnocení není pro analýzu rizika konkrétního systému dostačující. Proto norma [***126-1***] požaduje, aby jak kategorie četnosti, tedy jejich počet a numerické odstupňování; tak i počet úrovní závažnosti a následky pro každou z nich byly stanoveny provozovatelem dráhy, tak aby byly vhodné pro uvažované použití. Čili i tato kvantifikace, respektive její návrh bude muset být pro připravení podkladů pro realizaci analýzy rizika jedním z cílů této disertační práce [pozn. návrh je v kap. 4.3.3].

Pakliže ohodnotíme četnost výskytu konkrétního nebezpečí a úroveň jeho závažnosti, je možno přistoupit ke stanovení rizika plynoucího z tohoto nebezpečí. Stanovení rizika lze rozdělit do následujících dvou dílčích kroků (pozn.: toto dělení plyne dle mého názoru z normy [***126-1***] pouze nepřímo, ovšem lze si jej z celkového kontextu domyslet):

I. stanovení úrovní rizik, které jsou dány maticí „četnost–následky“, která obsahuje všechny možné kombinace četností výskytu a následků nebezpečí;
II. přiřazení kategorií rizik stanoveným úrovním rizik, přičemž s každou kategorií rizika souvisí i použitá opatření dle tab. 1.3.

První krok stanovení rizika představuje sestavení matice „četnost–následky“, jejímž prostřednictvím lze každému nebezpečí (již ohodnocenému z hlediska četnosti jeho výskytu i následků) přiřadit konkrétní úroveň rizika. V dalším kroku stanovení rizika je třeba každé úrovni rizika, potažmo konkrétním druhům nebezpečí (se známými četnostmi výskytu a následky) přiřadit kategorii rizika, která blíže specifikuje, jaké opatření by se mělo pro danou úroveň rizika použít (uvedeno v tab. 1.3) [***126-1***]. Ke každé úrovni rizika přísluší nápravné opatření pro snížení rizika na přijatelnou úroveň, které se volí dle kategorie rizika.

Podle mého názoru ovšem není vhodné a ani dost dobře možné takto paušalizovat rizika a pro stejné kategorie rizika používat jedno (samo sebou velmi obecné) opatření. Naproti tomu lze ale souhlasit s tím, že některá rizika je třeba bezpodmínečně odstranit. Některá lze přijmout, jen pokud jsou náklady na jeho odstranění nepřiměřeně velké (prakticky nedosažitelné). Rozhodně ale nelze souhlasit s tím, že některá lze přijmout, dokonce bez souhlasu provozovatele dráhy. Přijde mi přinejmenším vhodné u každého identifikovaného nebezpečí provést bezpečnostní analýzu a pokusit se stanovit nápravná opatření pro snížení rizika individuálně v závislosti na právě zkoumaném nebezpečí. V opačném případě, byť následky tohoto nebezpečí mohou být i banální, to pravděpodobně neprospěje celkové důvěryhodnosti zabezpečovacího systému.

Kategorie rizika	**Použitá opatření**
Nepřijatelné	Musí být odstraněno.
Nežádoucí	Smí být přijato pouze tehdy, jestliže snížení rizika je prakticky nedosažitelné, a se souhlasem provozovatele dráhy nebo řídicího orgánu pro otázky bezpečnosti, podle okolností.
Přípustné	Lze ho přijmout při přiměřené kontrole a se souhlasem provozovatele dráhy.
Zanedbatelné	Lze ho přijmout s/bez souhlasu provozovatele dráhy.

Tab. 1.3 – Typické kategorie rizika a související opatření

Výše popsané přiřazení konkrétní kategorie rizika konkrétní úrovni rizika se děje prostřednictvím kritérií přijatelnosti rizika (resp. principů přijetí rizika). Norma [***126-1***] uvádí ve své informativní příloze příklady některých principů přijetí rizika. Jedná se o tři principy, z nichž každý využívá jednu z trojice zásad: ALARP, GAMAB či MEM.

I. Zásada ALARP (As Low As Reasonable Practicable), používaná ve Velké Británii, stanoví, že rizika související s novým dopravním systémem, která leží v tzv. *oblasti ALARP* jsou přípustná pouze tehdy, je-li jejich snížení neproveditelné, anebo jsou-li náklady na jejich snížení vysoce neúměrné dosaženému zlepšení.
II. Zásada GAMAB (Globalement Au Moins Aussi Bon), používaná ve Francii, vychází z myšlenky, že „[v]šechny; nové […] dopravní systémy musí poskytovat úroveň rizika celkově nejméně tak dobrou, jako poskytuje kterýkoli stávající ekvivalentní systém“.
III. Zásada MEM (Minimum Endogenous Mortality), dříve používaná v Německu, operuje s tzv. *technologickými příčinami úmrtí* (nezahrnují např. úmrtí následkem nemocí), se kterými spojuje tzv. riziko endogenní úmrtnosti, a říká, že toto riziko nesmí být novým dopravním systémem výrazně zvýšeno.

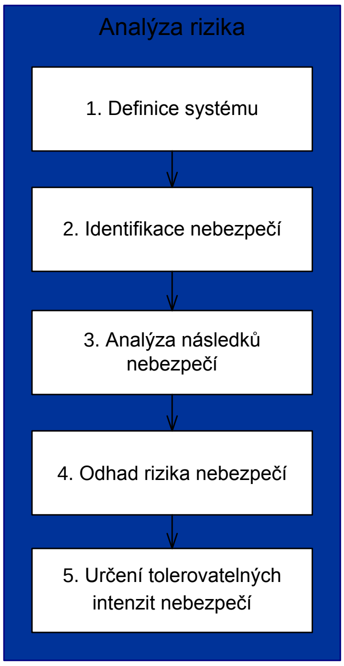
Na základě těchto zásad lze ohodnotit jednotlivé úrovně rizika získané z matice „četnost–následky“ jednou ze čtyř kategorií rizika, jež jsou uvedeny v tab. 1.3. Ani při znalosti těchto zásad dosud nebyl v podmínkách České republiky stanoven a provozovatelem dráhy odsouhlasen možný princip/principy přijetí rizika. Vzhledem k tomu, že analýzu rizika bez znalosti tohoto principu není možno dle přístupu normy [***126-1***] provést, bude dalším z cílů této disertační práce muset být též nalezení vhodného principu přijetí rizika, který by byl akceptovatelný v podmínkách České republiky [pozn. viz kap. 4.3.3].

Kromě výše uvedených záležitostí požaduje norma [***126-1***] při tvorbě analýzy rizika též vypracování záznamů o nebezpečí (krok 5 dle obr. 1.3), jejichž struktura je přesně daná touto normou. V požadavcích na tyto záznamy však obsahuje jisté nesrovnalosti (viz např. požadavek 3 – bod 6.3.3.3). Pro první přiblížení se ovšem lze přidržet normy [***129***], podle které mají tyto záznamy obsahovat každé identifikované nebezpečí spolu s přiřazenou klasifikací rizika vyplývajícího z tohoto nebezpečí a informací o řízení rizika pro každé nebezpečí a mají tvořit základ pro průběžný management rizika. Rovněž je stanoveno, že záznamy o nebezpečí se mají aktualizovat v případech, kdy dojde ke změně již identifikovaného, popřípadě k identifikaci nového nebezpečí.

Lze tedy konstatovat, že přístup dle normy [***126-1***] se zaměřuje na identifikování všech možných (za normálních okolností předvídatelných) nebezpečí souvisejících s analyzovaným systémem, na jejich ohodnocení z hlediska rizika a na zavedení a následné udržování procesu průběžného managementu rizika, jehož základem jsou záznamy o nebezpečí. Zde je vhodné zdůraznit jeden zajímavý poznatek, a to, že norma [***126-1***] jako jediná z norem v této disertační práci zkoumaných požaduje stanovit posloupnost nebezpečí, potažmo posloupnost událostí vedoucích k identifikovaným nebezpečím, což považuji z hlediska systematického zkoumání těchto nebezpečí za pozitivní (viz dále v této práci navrženou metodiku analýzy rizika, které tímto způsobem také postupuje, jak vidno např. z kap. 6.3).

1.2.2 Pohled evropské normy ČSN EN 50129:2003

V normě [***129***] je postup analýzy rizika uveden v její normativní příloze A. Je v ní popsán v části věnované určování požadavků na integritu bezpečnosti. Dle tohoto postupu má být v rámci analýzy rizika provedena definice systému (krok 1 dle obr. 1.4), při níž má být systém definován nezávisle na jeho fyzické realizaci. Dále mají být identifikována, podobně jako při předcházejícím přístupu (pozn. dle normy [***126-1***]), pokud možno všechna nebezpečí spojená se systémem (krok 2 dle obr. 1.4). Rovněž mají být analyzovány následky těchto nebezpečí (krok 3 dle obr. 1.4) a odhadnuta rizika z nich plynoucí (krok 4 dle obr. 1.4). Poslední krok analýzy rizika, kterým se tento přístup na první pohled liší od předcházejícího, spočívá v určení tolerovatelných intenzit nebezpečí (krok 5 dle obr. 1.4).



*Obr. 1.4 – Kroky analýzy rizika požadované normou ČSN EN 50129 [**129**]*

Na tomto místě je ovšem třeba ozřejmit, proč jsem v poslední větě předcházejícího odstavce použil *na první pohled*. Je to z toho důvodu, že podíváme-li se na celkový proces vývoje zabezpečovacích systémů dle normy [***126-1***] blíže, zjistíme, že i tato norma požaduje určení bezpečnostních požadavků. A jako jednu z forem bezpečnostních požadavků lze pokládat právě i určení tolerovatelných intenzit jednotlivých nebezpečí. Z tohoto pohledu (širšího kontextu) se tedy tento přístup (pozn. dle normy [***129***]) de facto neliší od předcházejícího, tj. od přístupu dle normy [***126-1***], ze kterého přístup uvedený v normě [***129***] vychází. Potvrzuje to i fakt, že se norma [***129***] v souvislosti s analýzou rizika velmi často odvolává právě na „základní" normu [***126-1***].

Dále je zajímavé zdůraznit skutečnost, že norma [***129***] považuje analýzu rizika za nedílnou součást procesu určování požadavků na integritu bezpečnosti. Tento proces tvoří vedle analýzy rizika ještě proces řízení nebezpečí. Při určování požadavků na integritu bezpečnosti, tedy jak při analýze rizika, tak při následném řízení nebezpečí, tato norma stanoví, že se má vycházet z rozhraní mezi zabezpečovacím systémem a jeho pracovním prostředím. Toto rozhraní je z hlediska bezpečnosti definováno seznamem nebezpečí, kterými může zabezpečovací systém nepříznivě působit na své pracovní prostředí (tedy zejm. na železniční dopravní proces).

Od tohoto rozhraní, které je definováno seznamem nebezpečí spolu s tolerovatelnými intenzitami jejich výskytu (*Tolerable Hazard Rate, THR*), se při určování požadavků na integritu bezpečnosti postupuje takto [***129***]:

I. směrem zdola–nahoru, což vede k identifikaci možných následků jednotlivých nebezpečí a s nimi souvisejících rizik;
II. směrem shora–dolů, což vede k identifikaci příčin jednotlivých nebezpečí.

Z výše uvedené normy lze dále vyvodit, že od daného „bezpečnostního" rozhraní je směrem nahoru prováděna analýza rizika, směrem dolů je prováděno řízení nebezpečí. Analýza rizika zde má za úkol definovat systém, identifikovat nebezpečí vyskytující se na jeho rozhraní a s ohledem na jejich následky a rizika z nich plynoucí stanovit tolerovatelné intenzity jejich výskytu THR. Poté přistupuje proces řízení nebezpečí, který prostřednictvím identifikace příčin nebezpečí zkoumá, zda je možno požadovaných THR (stanovených v předcházející analýze rizika) daným řešením systému dosáhnout.

Jak již bylo uvedeno, k definici „bezpečnostního" rozhraní slouží analýza rizika, která má dle normy [***129***] za úkol nejprve definovat systém, a to nezávisle na jeho technické realizaci. Následně pak provést identifikaci nebezpečí, kdy tato norma doporučuje použít systematickou identifikaci nebezpečí, která v sobě zahrnuje dvě fáze:

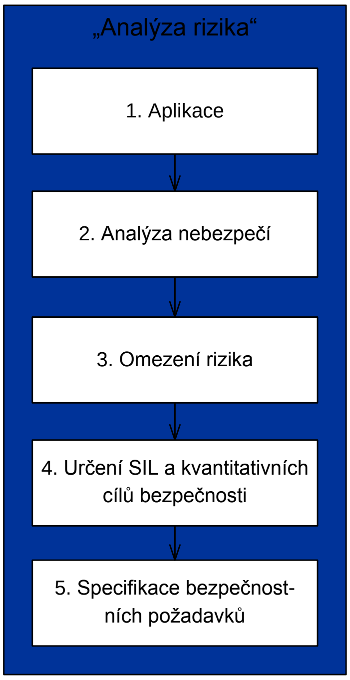
I. empirickou, která využívá zkušeností z minulosti (např. kontrolní seznamy);
II. kreativní, která využívá expertní posouzení systému (např. prostřednictvím strukturované studie „co kdyby" (*what if*)).

Odůvodnění nutnosti použití kombinace obou těchto fází spočívá ve zvýšení důvěry, že budou identifikována všechna významná nebezpečí. Po vykonání identifikace nebezpečí, je třeba analyzovat následky těchto nebezpečí spočívající v předpovědi nehod, možných selhání a bezpečných stavů. Dále je třeba odhadnout rizika a s jejich znalostí určit tolerovatelné intenzity nebezpečí. V této souvislosti norma [***129***] zdůrazňuje požadavek hovořící o tom, aby výsledné intenzity nebezpečí byly odvozeny se zřetelem na kritéria přijatelnosti rizika. Tato kritéria ovšem tato norma blíže nijak nespecifikuje, ale pouze konstatuje, že tato kritéria závisejí na národních nebo evropských legislativních požadavcích.

Lze tedy říci, že přístup dle normy [***129***] je značně ovlivněn základní skutečností, že tato norma na analýzu rizika pohlíží jako na nástroj pro stanovení požadavků na integritu bezpečnosti. V rámci analýzy rizika je potom vyžadováno provedení identifikace nebezpečí souvisejících s analyzovaným systémem, jejich ohodnocení z hlediska rizika a následné určení tolerovatelných intenzit nebezpečí THR, čímž analýza rizika v tomto pojetí končí. Nicméně dle mého názoru je následně potřeba minimálně od těchto THR odvodit úrovně integrity bezpečnosti SIL a s nimi související bezpečnostní požadavky (viz kap. 4.3.5).

1.2.3 Pohled evropské normy ČSN EN 50159:2011

Norma [***159***] se nevěnuje analýze rizika přímo, proto také nebyla v odborné práci [***ODP***] zohledněna. V této disertační práci se však pro úplnost zaměříme i na tuto normu, která z tohoto pohledu obsahuje několik málo záležitostí souvisejících s analýzou rizika nepřímo. I přesto však tyto záležitosti mohou dokreslit celkový pohled na analýzu rizika evropských norem. Norma [***159***] v její informativní příloze D uvádí kroky, jaké je nutno provést, aby byly splněny požadavky normy [***129***] pro návrh systému, potažmo tedy i požadavky normy [***126-1***]. Mezi nimi jsou totiž i kroky – záležitosti, které se týkají provádění analýzy nebezpečí, omezování rizika, přidělování SIL a kvantitativních cílů bezpečnosti (viz obr. 1.5).



*Obr. 1.5 – Kroky s patrnou vazbou na analýzu rizika uváděné normou ČSN EN 50159 [**159**]*

Ač jsou tyto kroky uvedeny pouze v informativní příloze této normy [***159***] a norma je přímo s analýzou rizika nijak nespojuje, jsou z našeho pohledu zajímavé a inspirativní, neboť evidentně velmi úzce právě s prováděním analýzy rizika dle normy [***129***] souvisí. Norma [***159***] na základě těchto kroků ve dvou příkladech stanovuje (bezpečnostní) požadavky na vlastnosti obranných mechanismů datových komunikací.

Při jejich stanovování začíná použitím (krok 1 dle obr. 1.5), kdy zdůrazňuje potřebu návrháře porozumět danému použití datové komunikace v konkrétním systému, tak aby byl schopen se dobře rozhodovat při návrhu této komunikace a stanovování bezpečnostních požadavků na ni. Dále je v rámci tohoto kroku vyžadováno stanovení (a to buď uživatelem, nebo bezpečnostním orgánem) globálního bezpečnostního cílu na celý systém, resp. na jeho aplikaci (ve formě míry, nebo kvalitativních a nefunkčních parametrů). Tento krok dle mého názoru kopíruje první krok analýzy rizika dle normy [***129***], kterým je definice systému.

Další kroky pak již přímo nekopírují kroky analýzy rizika dle normy [***129***], na kterou se však tato norma odvolává. Nicméně i tyto kroky představují jednotlivé dílčí součásti analýzy rizika ve smyslu celkového náhledu na analýzu rizika dle norem analyzovaných v předcházejících kapitolách této práce (tedy ve smyslu [***126-1***], [***129***] a [***159***]).

Další krok v řadě představuje analýza nebezpečí (krok 2 dle obr. 1.5), při němž norma [***159***] požaduje stanovení jednoho nebo více vrcholových nebezpečí, která mohou nastat v důsledku selhání analyzovaného systému. Zde tato norma, vzhledem ke svému zaměření zcela přirozeně, uvádí tři možnosti selhání. Jedná se o selhání vysílače, přijímače a vlastního přenosového spojení. Při analýze nebezpečí je třeba zohlednit všechny provozní i všechny ostatní vnější okolnosti (ty budou posléze zohledněny pro omezení rizika – viz následující odstavec). Tyto úlohy odpovídají krokům 1 a 2 dle normy [***126***]. Tedy kroku identifikace nebezpečí a kroku identifikace posloupností událostí vedoucích k nebezpečí. Navíc norma [***159***] uvádí, že již v rámci analýzy nebezpečí může být pro každou hrozbu (obecně pro každé nebezpečí) navržena možnost zahrnutí obrany do návrhu systému.

Po analýze nebezpečí následuje další krok, kterým je omezení rizika (krok 3 dle obr. 1.5), kde se každé identifikované hrozbě (nebezpečí) na základě globálního kvantitativního cíle[1] a kvalitativní analýze nebezpečí přiřadí bezpečnostní cíl. Norma [***159***] umožňuje, aby tohoto přerozdělování bezpečnostních cílů bylo dosaženo iterativně, tj. postupně například od použití od velmi zjednodušujícího přístupu až po využití přesného a propracovaného přístupu, podpořeného podrobnými analýzami. Zajímavá je také skutečnost, že norma [***159***] v této souvislosti připouští, aby omezování rizika bylo stanoveno v závislosti na výskytu vnějších okolností, které v systému působí hazard. Dokladuje to například na zjednodušeném příkladu, kdy stanovuje pravděpodobnost obsazení úseku a touto pravděpodobností potom omezuje riziko srážky, ke které může dojít jedině po vstupu vlaku do obsazeného úseku.

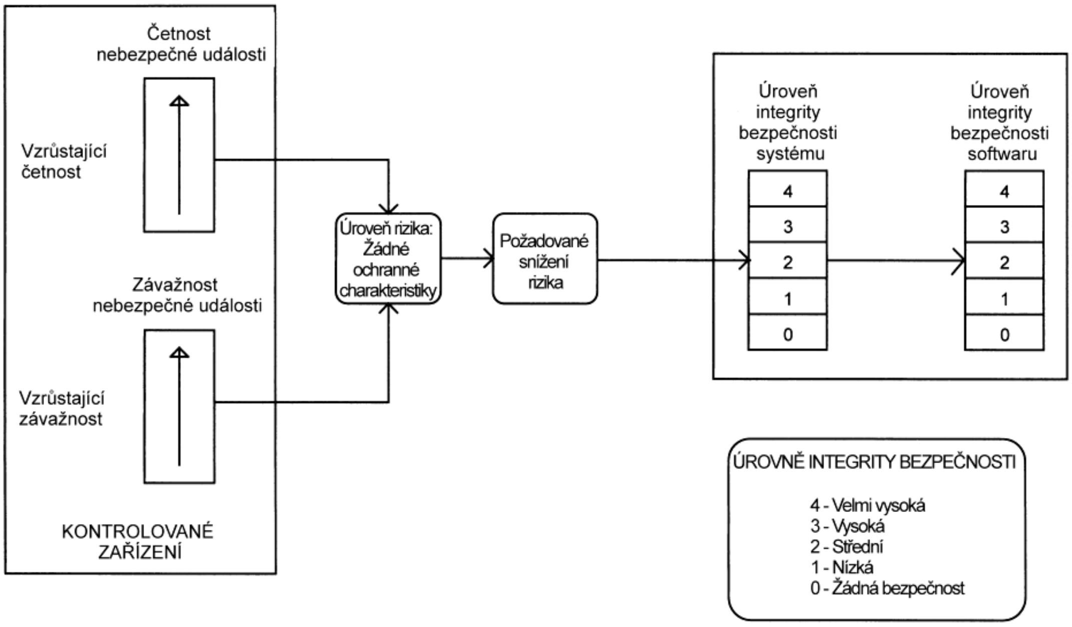
Následující dva kroky (krok 4 a 5 dle obr. 1.5) jdou ruku v ruce. Jsou jimi jednak určení úrovní SIL a kvantitativních bezpečnostních cílů, jednak specifikace bezpečnostních požadavků. Norma [***159***] stanovuje, že úrovně SIL a kvantitativní bezpečnostní cíle mají být přiřazeny v závislosti na rozsahu potřebného omezení rizika (stanoveného v kroku 3, tedy kroku předcházejícím), což umožní použít adekvátní metody a techniky při návrhu systému dle normy [***129***]. Následně je třeba výstupy celého předchozího procesu (kterými – po patřičném zobecnění – jsou: stanovená nápravná opatření pro redukci rizika, úrovně SIL pro implementaci těchto opatření a kvantitativní bezpečnostní cíle pro systém), zanést do požadavkových dokumentů a dohlídnout jejich naplnění.

Norma [***159***] deklaruje, že tento postup naplní požadavky normy [***129***]. Norma [***159***] v rámci tohoto postupu dále popisuje jednotlivé jeho kroky, přičemž přímo neuvádí jejich souvislost s analýzou rizika. Tato souvislost je patrná až z rozboru provedeného v této práci, kde jsou naznačeny vazby s požadavky na analýzu rizika ostatních norem – [***126***] a [***129***].

[1] Poznámka: Zde je třeba upozornit na jistou nekonzistenci v normě [***159***]. Přestože tato norma v kroku 1 přímo nepožaduje stanovení kvantitativního bezpečnostního cíle – dává totiž možnost volby mezi cílem kvantitativním (míra), nebo kvalitativním (kvalitativní a nefunkční parametry) –, v tomto třetím kroku již přímo s tímto kvantitativním bezpečnostním cílem operuje.

1.2.4 Pohled evropské normy ČSN EN 50128:2012

Normy [***128***] (pozn. myšleno jak její první edice z roku 2003, tak i její druhá edice, platná nyní paralelně s první od dubna 2012 do dubna 2014[2] – dále v textu budou, nebude-li uvedeno jinak, komentovány požadavky obou edic normy [***128***]) se o analýze rizika zmiňují jen nepřímo ve svém úvodu. Uvádí zde, že tato norma (myšleno [***128***]) stanovuje opatření, která jsou nutná pro splnění požadavků kladených na bezpečnostní funkce, které jsou (dle postupů uvedených v odkazovaných normách [***126-1***] a [***129***]) přiřazeny softwaru. Toto má údajně ilustrovat z této normy převzatý obr. 1.6.



*Obr. 1.6 – Vztah mezi nebezpečnou událostí a úrovněmi integrity bezpečnosti (převzato z: [**128**][3])*

Zajímavé je, že vztahy, které obr. 1.6 znázorňuje, nejsou v normě [***128***] nikterak více rozvedeny. Norma se na tento obrázek odkazuje pouze v souvislosti s jedním tvrzením, které hovoří o tom, že tato norma stanoví opatření, která jsou nutná pro splnění požadavků na bezpečnostní funkce přiřazené softwaru. Zde je třeba poznamenat, že v textu normy je uvedeno „pro splnění těchto požadavků“, což z kontextu pochopeno s velkou pravděpodobností znamená to, co je uvedeno v mé předcházející větě. Nicméně, můj osobní názor na obrázek je takový, že zachycuje skutečnost, že úroveň rizika by se měla stanovit bez opatření pro snížení rizika. Ta by se měla aplikovat až následně, a to v závislosti na požadované úrovni integrity

[2] Aktuálně se jedná (UNIFE žádá CEN-CENELEC) o prodloužení platnosti první edice normy ČSN EN 50128, aby výrobci nemuseli v relativně krátké době několikrát měnit procesy užívané při vývoji bezpečnostně-kritických počítačově-orientovaných systémů, neboť další změny v těchto procesech se plánují s novým vydáním normy ČSN EN 50126, jejíž jedna část by měla v brzké době normu ČSN EN 50128 zcela nahradit [***E128***].
[3] Tento obrázek a s ním související text se vyskytuje pouze v první edici ČSN EN 50128:2003.

bezpečnosti systému. Toto ovšem podle mého názoru platí pouze pro prvotní hodnocení rizika, což už z obrázku přímo neplyne.

Dále norma [***128***] v souvislosti s analýzou rizika stanoví, že jak norma [***126-1***], tak i norma [***129***] požadují, aby byl zaveden systematický postup pro (následující výčet je zde omezen pouze na činnosti přímo související s analýzou rizika):

I. identifikaci nebezpečí, rizik a kritérií rizik[4];
II. identifikaci nezbytného omezení rizika pro splnění kritérií rizik;
III. definování celkové specifikace požadavků na bezpečnost systému pro bezpečnostní opatření potřebných pro dosažení požadovaného omezení rizika.

Můžeme tedy říci, že norma [***128***] požadavky na analýzu rizika jako takovou nestanovuje. Pouze nepřímo předpokládá, že tato analýza bude vykonána, že toto její vykonání bude v souladu s požadavky příslušných norem [***126-1***] a [***129***], kterými se tato práce již zabývala (viz předcházející kapitoly 1.2.1 a 1.2.2). Dále norma [***128***] stanovuje, že jsou v ní obsažena možná nápravná opatření pro snížení rizika na přijatelnou úroveň, která jsou použitelná pro software v bezpečnostně-kritických zabezpečovacích počítačově-orientovaných systémech, což je uplatnitelné právě v rámci vykonávání analýzy rizika těchto systémů.

1.2.5 Pohled evropské směrnice 2004/49/EC (CSM)

Zajímavý a řekl bych nejúplnější pohled na tvorbu analýzy rizika různých železničních systémů (pozn. netýká se přímo zabezpečovacích systémů jako takových, ale železničních systémů obecně) nabízí také směrnice 2004/49/EC [***49***], označovaná jako tzv. *bezpečnostní směrnice*, respektive ne přímo tato směrnice, ale především různá Evropskou železniční agenturou k této směrnici vydaná doporučení, návody a vodítka[5]. V této práci bylo například vycházeno předně z následujících podkladů, které s touto směrnicí souvisejí:

I. z workshopu Dissemination of the Commission Regulation on Common Safety Methods (CSM) on Risk Evaluation and Risk Assessment [***DissPpt***],
II. ze zprávy Report on the development of the first set of Common Safety Methods [***CsmRep***]

[4] Pozn. 1: Nejde o přesnou citaci, neboť v ČSN EN 50128 první edice je uvedeno „bezpečnost identifikaci nebezpečí, rizik a kritérií rizik“, což je (ve srovnání s originálním anglickým zněním této edice) evidentně chybně. Pozn. 2: Edice dva ČSN EN 50128 uvádí pozměněně: „[…] identifikaci nebezpečí, hodnocení rizik a dospění k rozhodnutím založeným na kritériích rizika“.

[5] Tyto byly následně během psaní této disertační práce vydány jako evropská směrnice 2013/402/EC [***402***].

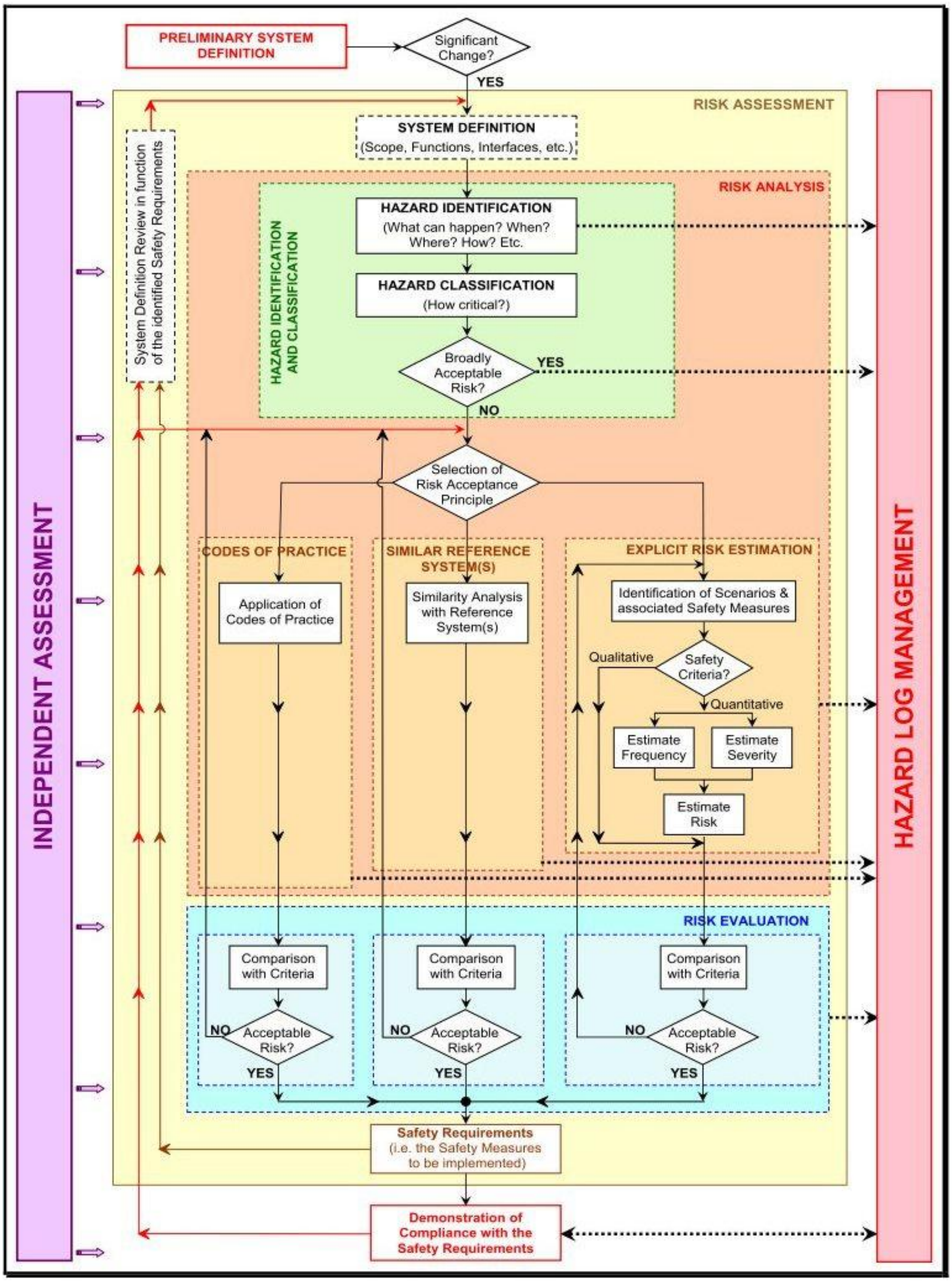
III. z článku Common Safety Method (CSM) on risk evaluation and assessment [***CsmArt***].

Dle směrnice [***49***] má každý provozovatel dráhy i provozovatel drážní dopravy (tedy dopravce) zavést svůj systém řízení bezpečnosti (Safety Management System, SMS). Součásti tohoto systému jsou vyjmenovány v příloze III této směrnice, kde se mimo jiné požaduje zavést postupy a metody pro hodnocení rizika a realizovat opatření pro řízení rizika, a to vždy, když v železničním systému nastane změna, která v něm vyvolá nová rizika. A právě pro hodnocení rizika a řízení rizika lze použít společnou bezpečnostní metodu (Common Safety Method, CSM), dokonce je to doporučeno, a to jak uvedenou bezpečnostní směrnicí [***49***], tak i směrnicí o interoperabilitě [***57***], která se při popisu uvádění systému do provozu na tuto bezpečnostní směrnici odvolává.

Metoda CSM má tedy za úkol harmonizovat postup hodnocení a řízení rizika, který tvoří nedílnou součást analýzy rizika, tudíž i metodiky stanovované v této disertační práci. Při použití tohoto harmonizovaného postupu je třeba dodržet jednotlivé kroky, které jsou na obr. 1.7. Ovšem jedná se opět jen o obecnou harmonizaci postupu, nikoli o stanovení jednotných metod a postupů v rámci jednotlivých kroků. Důvodem je podle mého názoru skutečnost, že tato metoda – podobně jako postupy požadované evropskými normami zmíněné výše – je psána takovým způsobem, aby nevylučovala použití již zažitých a praxí ověřených národních metod a technik. Tedy tak, že jen uvádí, co je třeba udělat, nikoli to, jak je to třeba udělat. Tuto myšlenku podporuje také například článek [***CsmArt***], který se mimo jiné zmiňuje o tom, že metoda CSM má specifikovat pouze to, jaké požadavky mají být naplněny, aniž by specifikovala, jakým způsobem mají být tyto požadavky naplněny.

Metodou CSM harmonizovaný postup hodnocení a řízení rizika uvádí obr. 1.7. Podíváme-li se na něj blíže, zjistíme, že tento harmonizovaný postup tvoří kroky, které představují iterativní postup řízení rizika, jehož součástí je samozřejmě též hodnocení rizika. Jinými slovy, jde o řešení problému (v tomto případě o snižování rizika na přijatelnou úroveň) postupnými stále se opakujícími kroky, přičemž vždy při jejich dalším opakování se řešení přibližuje k žádoucímu výsledku. Každé další opakování tudíž mění kontext, ve kterém probíhá další krok. Pročež jde o proces iterativní. Jak plyne například z [***CsmArt***] a z obr. 1.7, je tento harmonizovaný iterativní postup řízení rizika založen na následujících třech základních krocích:

I. systematická identifikace nebezpečí založená na definici hodnoceného systému, definici souvisejících bezpečnostních opatření a definici z nich plynoucích bezpečnostních požadavků;
II. analýza rizika, vč. ohodnocení jeho přípustnosti;
III. prokázání, že systém splňuje identifikované bezpečnostní požadavky.



*Obr. 1.7 – Harmonizovaný proces hodnocení rizika metodou CSM (převzato z [**CSM**])*

Jak plyne z předchozího, provedení výše uvedených tří kroků harmonizovaného iterativního postupu hodnocení rizika metodou CSM v podstatě požadují též normy [***126-1***] a [***129***]. Neboť to, co je zde v rámci CSM označováno za (iterativní) proces řízení rizika (krok 1 a 2 dle CSM), který je touto směrnicí harmonizován, to je v normě [***126-1***] označováno za analýzu rizika a v normě [***129***] je to navíc rozšířeno o tzv. řízení nebezpečí, což je proces, v rámci nějž je prokazováno plnění cílů bezpečnosti daným zabezpečovacím systémem (krok 3 dle CSM). Přičemž tyto cíle bezpečnosti mají být správně stanoveny v rámci, respektive na základě vypracované analýzy rizika.

V souvislosti s obrázkem uvedeným na předchozí straně (viz obr. 1.7), který uvádí metodou CSM harmonizovaný proces (postup) hodnocení a řízení rizika, bych si dovolil uvést své první dojmy a slovní hodnocení tohoto postupu, které vycházejí mých dosavadních znalostí a zkušeností získaných v této oblasti a samozřejmě z podrobnějšího zamyšlení se nad tímto postupem hodnocení rizika. Předesílám, že toto zamyšlení bylo záměrně provedeno bez předchozího hlubšího nastudování souvislostí uvedených v doporučení k této metodě. Mé komentáře k postupu naznačenému na vývojovém diagramu jsou následovné:

i) z obrázku plyne, že každá činnost provedená v rámci hodnocení rizika (risk assessment) má být nezávisle posouzena (fialové šipky směřující z bloku idnependent assessment) a v případě potřeby zaznamenána do záznamu o nebezpečí (přerušované šipky směřující do bloku hazard log management), což je správně a zajišťuje to jistou míru objektivity dosažených výsledků; jen drobná poznámka: osobně bych do záznamu o nebezpečí nechal zaznamenávat i klasifikaci nebezpečí (hazard classification), což z obrázku neplyne – šipka vede pouze z bloku identifikace nebezpečí (hazard identification)

ii) zajímavé je, že obrázek do hodnocení rizika (risk assessment) zahrnuje i definici systému (system definition), což je podle mého názoru alespoň v první fázi vstupní záležitost, nikoli součást tohoto procesu; i když je pravdou, že v dalších fázích analýzy rizika dochází v závislosti na nových bezpečnostních požadavcích a nově navrhovaných nápravných opatřeních pro snižování rizika na přijatelnou úroveň k revizi a doplnění již existující definice systému (system definition review)

iii) z obrázku plyne, že identifikace a klasifikace nebezpečí (hazard identification and classification) je součástí analýzy rizika (risk analysis), rovněž tak princip přijetí rizika (risk acceptace principle) je její součástí; ovšem ohodnocení rizika dle zvoleného principu přijetí rizika (risk evaluation) již dle obrázku součástí analýzy rizika (risk analysis) není, což podle mého názoru není formálně úplně správně; osobně toto ohodnocení řadím mezi činnosti vykonávané v rámci analýzy rizika; podle mého názoru totiž není formálně správné vybrat vhodný princip přijetí rizika v rámci analýzy rizika (risk analysis), ale vlastní ohodnocení rizika dle zvoleného přístupu provést až jako součást nadřazeného procesu hodnocení rizika (risk assessment), tyto záležitosti jsou spolu velmi úzce spjaty

iv) s ohodnocováním rizika (risk evaluation) dále souvisí další pro mne ne zcela správná a jasná skutečnost, a to, že podle vývojového diagramu na obrázku by se v případě, že je riziko ohodnoceno jako nepřijatelné, což se stane v rozhodovacím bloku „Acceptable Risk?", mělo vrátit na rozhodovací blok „Selection of Risk Acceptance Principle", ve kterém se zřejmě má vybrat jiný princip pro přijetí rizika tak, aby riziko vyhovělo; přičemž jediná možnost, jak se z tohoto cyklu dostat (podle mého názoru by se nemělo vracet na výběr principu, ale do bloku, kde by byla možnost stanovení nápravných opatření pro snížení tohoto rizika) je přes princip přesného stanovení rizika, a to „správným" odhadnutím četnosti a závažnosti následků (Estimate Frequency & Severity), což podle mě není věcně zcela korektní, ba naopak to vývojáře-analytiky nutí vyřešit tento problém pomocí „vhodné" kvantifikace, což řeší problém pouze formálně, nikoli věcně; toto je však u bezpečnostně-kritických systémů zcela nepřípustné!

v) z vývojového diagramu dále plyne, že v případě, že je riziko přijatelné, je třeba stanovit bezpečnostní požadavky související s tímto nebezpečím, což se projeví v úpravě definice tohoto systému (hnědá šipka vedoucí do bloku System Definition Review …), a následně se provede důkaz, zda systém vyhovuje těmto bezpečnostním požadavkům (černá šipka do bloku Demonstration of Compliance with the Safety Requirements); o tom se dále provede záznam do záznamu o nebezpečí (přerušovaná černá šipka – poněkud zvláštní je její obousměrnost);

vi) z diagramu však v tomto případě není patrno, co se stane po provedení revize definice systému po dodefinování bezpečnostního požadavku v souvislosti s nalezeným nebezpečím dané funkce systému (System Definition Review in function of the identified Safety Requirement), kam se přejde těsně před ukončením procesu hodnocení rizika (risk assessment) po dodefinování tohoto bezpečnostního požadavku (hnědá šipka z bloku Safety Requirements – pozn. formálně bych blok v souladu s ostatními pojmenoval Safety Requirements Specification)

vii) na uvedeném vývojovém diagramu mne také zaujala jedna pro mne nová a do jisté míry překvapující skutečnost, kterou také zachycuje, a to, že explicitní odhadnutí rizika (explicit risk estimation) je možno provést i kvalitativním způsobem, který zcela obchází odhadnutí ‚přesných' hodnot četnosti a závažnosti následků (Estimate Frequency & Severity); přičemž doposud jsem měl takovou představu, že při explicitním odhadu rizika (explicit risk estimation) je nutno vykonat explicitní, tedy číselný, tedy kvantitativní odhad rizika, například způsobem, jakým to uvádí literatura [***BŽZS***] v její kapitole 5.2

viii) zajímavé bude se v doporučení dozvědět, jak přistupovat k rozhodovacím blokům „Significant Change?", který rozhoduje o tom, zda je nebo není třeba pro danou změnu systému použít hodnocení rizika (risk assessment), a „Broadly Acceptable Risk?", který rozhoduje o tom, zda je nebo není možno dané riziko přijmout bez použití principu přijatelnosti rizika (risk acceptance principle); výsledek obou bude podle mého názoru vždy výsledkem expertního odhadu, a bude tudíž velmi subjektivně zatížen

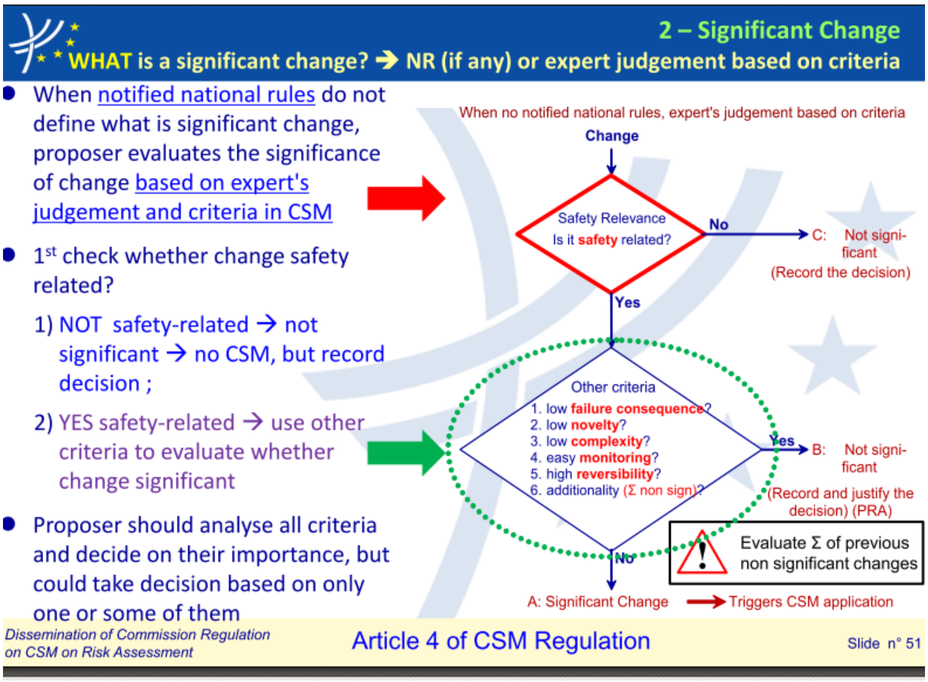
- celkově se mi tento přístup hodnocení a řízení rizika zdá v určitých ohledech poněkud zvláštní, nicméně oproti předcházejícím přístupům nejkomplexnější – své návrhy na zlepšení zapracuji v kapitole 4, která se věnuje návrhu vhodného přístupu k analýze rizika železničních zabezpečovacích systémů s ohledem na systém vlakového zabezpečovače ETCS

Vzhledem ke komplexnosti vývojového diagramu popisujícího metodou CSM harmonizovaný postup řízení a hodnocení rizika a k nejasnostem vyjádřeným k němu v mých komentářích výše považuji za velmi přínosné (ač by se to na první pohled mohlo zdát zbytečné) také zběžné seznámení se s jednotlivými kroky metodou CSM harmonizovaného procesu řízení rizika, tak jak se na ně dívají různá doporučení vydaná Evropskou železniční agenturou (ERA, European Railway Agency) k této metodě. Zaměříme se v této souvislosti navíc pouze na ty kroky touto metodou harmonizovaného řízení rizika, které se liší nebo lépe dokreslují kroky analýzy rizika dostatečně podrobně popsané v již zmíněných normativech. Těmi se tato práce zabývá v předešlých kapitolách (kap. 1.2.1, 1.2.2 a 1.2.3).

Přibližme si tedy nyní v další textu blíže tyto hlavní myšlenky k metodě CSM již výše zmíněných doporučení vydaných Evropskou železniční agenturou. Ještě dříve než se přistoupí k identifikaci nebezpečí (krok 1 dle CSM), je třeba rozhodnout, zda se jedná o tzv. *významnou změnu* systému. Pokud se dojde k názoru, že ano, je třeba dle směrnice [***49***] použít metodu

CSM, tedy harmonizovaný proces řízení rizika. V opačném případě toho třeba není, ovšem je nutno o tomto (dle mého názoru klíčovém) rozhodnutí pořídit záznam. Jak tedy přistupovat k rozhodnutí, zda jde o významnou změnu či nikoli, a to zejména v případě, kdy naše národní pravidla v České republice nedefinují, co je a co není významná změna systému?

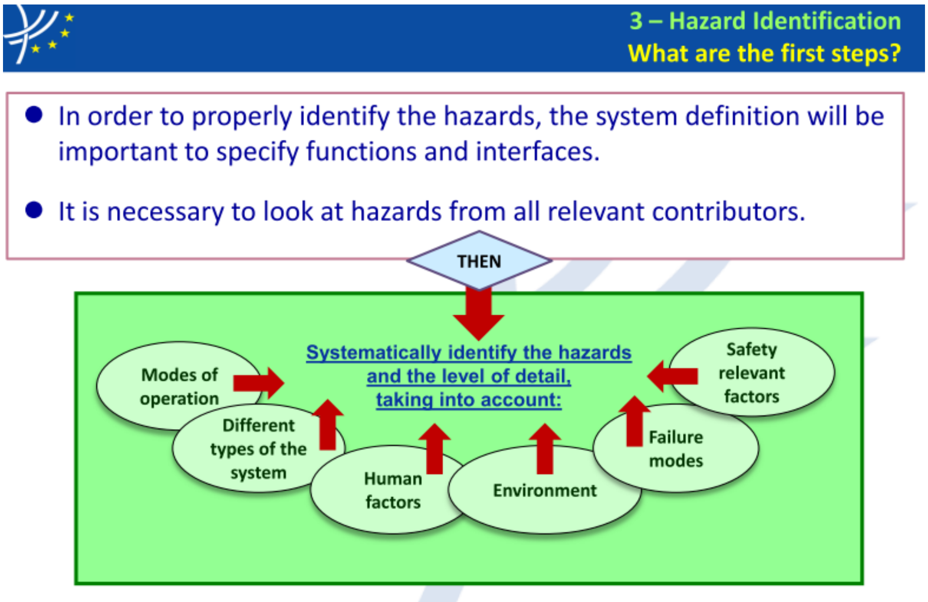
Dle doporučení uvedeného v [***DissPpt***] je v takovém případě rozhodnutí ponecháno na navrhovateli (což je – zjednodušeně řečeno – společné označení, které se zde používá jak pro železniční podnik či provozovatele dráhy, tak pro výrobce jakéhokoli interoperabilního železničního /nejen tedy zabezpečovacího/ zařízení), který má o významnosti změny rozhodnout na základě expertního odhadu a kritérií, které mu mají sloužit jako vodítko ke správnému rozhodnutí (viz str. 34 a 51 v [***DissPpt***]). Doporučený postup je zachycen ve vývojovém diagramu na obr. 1.8.



*Obr. 1.8 – Hodnocení změny podle její závažnosti (převzato z [**DissPpt**])*

Podle tohoto postupu (viz obr. 1.8) je třeba změnu nejprve posoudit z hlediska její bezpečnostní relevance (rozhodovací blok Safety Relevance). V rozhodování o významnosti změny se pokračuje, jen pokud je u ní shledána bezpečnostní relevance. Poté následuje série otázek hodnotící další kritéria změny (viz rozhodovací blok Other criteria). Na základě nich se vyhodnotí, zda posuzovaná změna je nebo není významná [pozn.: toto rozhodnutí nemusí být učiněno podle všech těchto dalších kritérií]. Pakliže se dojde k závěru, že posuzovaná změna není významná, není sice třeba použít metodu CSM pro řízení rizika, ale je třeba o tomto rozhodnutí pořídit záznam. V opačném případě je třeba aplikovat postup řízení rizika dle metody CSM (a dle mého názoru o tomto rozhodnutí taktéž učinit záznam).

U významných změn systému se dále přistupuje k provedení kroku 1 dle CSM, čímž je již zmíněná identifikace nebezpečí (viz obr. 1.9). Při identifikaci nebezpečí je dle [***DissPpt***] doporučováno vyjít z definice posuzovaného systému a z jeho rozhraní. Přitom se má přihlédnout ke všem faktorům, které mohou přispívat k nebezpečí, jako např. k různým provozním režimům systému, k různým typům systému [pozn. patrně je zde myšleno terminologií normy [***129***] k různým generickým i specifickým aplikacím], k vlivu lidského faktoru, k vlivu okolí, k různým druhům poruch, k ostatním bezpečnostně relevantním faktorům.



*Obr. 1.9 – Identifikace nebezpečí dle CSM (převzato z [**DissPpt**])*

Po systematické identifikaci nebezpečí lze přistoupit ke kroku 2 dle CSM, kterým je vlastní analýza rizika, která v tomto pojetí zahrnuje i ohodnocení jeho přípustnosti. Pro hodnocení přípustnost rizika uvádí metoda CSM tři principy pro přijetí rizika, dívá se na ně zcela rovnocenně (žádný nepreferuje) a umožňuje pro každé jednotlivé nebezpečí použít jiný princip, tedy jiné kritérium přijatelnosti rizika [***DissPpt***]. Tyto principy jsou následující:

I. Kodex dobré praxe (CoP, Code of Practice) – za kodex dobré praxe lze dle tohoto principu považovat dokument či soubor dokumentů, které jsou veřejně přístupné, v oblasti dané domény široce všeobecně uznávané, relevantní pro daná nebezpečí a v neposlední řadě taktéž přijatelné pro hodnotitele bezpečnosti.
II. Referenční systém (Reference System) – použitý referenční systém musí dle tohoto principu mít podobné funkce a rozhraní, jako má hodnocený systém. Dále musí

zajišťovat přijatelnou úroveň bezpečnosti, což musí být v daných (zejména provozních, ale i klimatických a dalších) podmínkách prověřeno praxí.

III. Explicitní odhadnutí rizika (Explicit Risk Estimation) – explicitní odhadnutí rizika nemusí mít dle tohoto principu kupodivu kvantitativní charakter, což bych očekával – podobně, jako je tomu například v publikaci [***BŽZS***] –, nýbrž může mít též semikvantitativní charakter (nejsou-li všechny kvantitativní údaje dostupné), či dokonce charakter kvalitativní (není-li kvantifikace možná).

Kromě principů pro určení přijatelnosti rizik uvedených výše, metoda CSM (viz např. opět [***DissPpt***]) dále zmiňuje záznamy o nebezpečí a zdůrazňuje jejich význam při řízení nebezpečí, respektive rizik z nich plynoucích. Stanovuje, že záznamy o nebezpečí musí být vytvořeny a následně řádně aktualizovány [pozn. patrně myšleno po celý životní cyklus železničního systému]. Uvádí, že jeden z jejich hlavních významů je, že umožňují sledovat vývoj procesu, tedy identifikaci nebezpečí, potenciálního rizika z něj plynoucího a způsobu, jakým musí být toto riziko řízeno prostřednictvím jednoho z výše uvedených principů pro určení přijatelnosti rizika.

V rámci metody CSM (tedy ve směrnici [***49***], především pak v příslušných doporučeních k této směrnici vydaných – viz úvod kapitoly) je proces řízení a hodnocení rizika popsán nejobsáhleji, proto také obsahuje nejvíce mých komentářů. Přestože tento postup opět (stejně jako ve výše posuzovaných evropských normativech z oblasti železniční techniky) neobsahuje konkrétní metody a techniky pro vlastní vypracovávání analýzy rizika, lze na tomto postupu velmi kladně hodnotit, že je dle mého názoru popsán nejkomplexněji: obsahuje nejen popis postupu analýzy rizika, ale též určuje, kdy se má provést stanovení bezpečnostních požadavků, následná revize definice systému a předvedení, že daný systém tyto nově stanovené bezpečnostní požadavky splňuje. Určuje rovněž, které výstupy tohoto procesu se mají zaznamenat do záznamu o nebezpečí.

1.3 Shrnutí současného stavu obecné části týkajícího se analýzy rizika

1.3.1 Slovní shrnutí

Jak vyplývá z výše provedeného rozboru současného stavu, existuje v současné době několik postupů tvorby analýzy rizika, které se více či méně vzájemně odlišují. Podrobněji se jim věnují předcházející kapitoly. Lze říci, že tyto postupy stanovují pouze vysokoúrovňové principy a s nimi související mandatorní požadavky. Nespecifikují již konkrétní metody ani nástroje pro jejich naplnění. Tyto jsou uvedeny pouze ve volitelných částech zkoumaných evropských normativů, popřípadě v různých doporučeních a vodítkách. Důvodem je patrně obava z toho, že v opačném případě by mohlo být (a zřejmě i skutečně bylo) vyloučeno použití již zažitých a praxí ověřených národních metod a technik. Tato společná vlastnost výše zmiňovaných přístupů je obecně na evropské úrovni vnímána jako výhoda. Ovšem v našich podmínkách se jedná spíše o nevýhodu, neboť v České republice (a patrně nejen zde) dosud nebyly tyto metody a techniky pro provádění analýzy rizika stanoveny. Proto je důležité se touto otázkou v této práci dále zabývat.

Odpoutáme-li se od konkrétních metod a technik využitelných pro analýzu rizika, je zajímavé podívat se na jednotlivé přístupy k obecnému procesu analýzy rizika. Ač by se dalo předpokládat, že nejvíce komplexní přístup k tvorbě analýzy rizika bude pro železniční zabezpečovací systémy uveden v základní normě [***126-1***], dle mého názoru tomu není tak. Nejvíce komplexní a nejvíce si odpovídající postupy v této oblasti spatřuji uvedené v normě [***129***] a ve směrnici [***49***]. Oba tyto postupy v sobě totiž zahrnují nejen hodnocení rizika, ale i celkový proces řízení rizika. Tedy ukazují vztah ke stanovování a prokazování plnění na základě analýzy rizika stanovených bezpečnostních požadavků na systém, což je dle mého názoru základním smyslem provádění analýzy rizika při vývoji bezpečnostně-kritických systémů obecně, respektive zabezpečovacích systémů konkrétně.

1.3.2 Shrnutí požadavků norem

Zde je uveden souhrn normativních požadavků, které je třeba naplnit. Požadavky jsou označovány následujícím klíčem:

R_RA_nnn_cc,

kde R … požadavek (Requirement),

RA … analýza rizika (Risk Analysis),

nnn … neúplné označení normy, ze které daný požadavek plyne, přičemž vztah k úplnému označení je následující:

126 … ČSN EN 50126-1:2007 [***126***],

129 … ČSN EN 50129:2003 [***129***],

159 … ČSN EN 50159:2011 [***159***],

128 … ČSN EN 50128:2012 [***128***],

cc … číselné označení požadavku.

Normativní požadavek			Naplnění má zajistit	Poznámka
Číslo	Popis	Plyne z		
R_RA_126_01	Systematicky identifikovat všechna za normálních okolností předvídatelných nebezpečí a stanovení jejich „priorit“ (Identifikace nebezpečí)	čl. 6.3.3.1.a	metodika / vlastní analýza	
R_RA_126_02	Identifikace posloupností událostí vedoucích k těmto nebezpečím (Identifikace posloupností událostí vedoucích k nebezpečí)	čl. 6.3.3.1.b		
R_RA_126_03	Stanovit rizika plynoucí pro systém z těchto nebezpečí (Stanovení rizik plynoucích pro systém z jednotlivých nebezpečí)			
R_RA_126_04	(i) Ohodnotit identifikovaná nebezpečí z hlediska jejich četnosti výskytu a závažnosti následků (ii) Na základě matice „četnost–následky“ stanovit úrovně rizik plynoucí z jednotlivých nebezpečí (iii) Na základě kritérií přijatelnosti rizika přiřadit jednotlivým nebezpečím s danou úrovní rizika příslušné kategorie rizika, vč. nápravných opatření (Stanovení a klasifikování přijatelnosti rizik)	čl. 6.3.3.1.c-e a 6.3.3.2		Pro (i) bude třeba stanovit jak jednotlivé kategorie četnosti, jejich počet a numerické odstupňování; tak i počet jednotlivých úrovní závažnosti a následky pro každou z nich. Pro (iii) bude třeba vybrat nebo stanovit vlastní princip přijatelnosti rizika použitelný v ČR
R_RA_126_05	Zavést systém řízení rizika, jehož nedílnou součástí musí být záznamy o každém identifikovaném nebezpečí obsahující důkaz o zvládnutí jejich rizik (Vypracování záznamů o nebez-	čl. 6.3.3.3		

	pečí)			
R_RA_129_01	Definovat systém nezávisle na jeho budoucí realizaci (Definice systému)	A.4.1.1		
R_RA_129_02	Identifikovat pokud možno všechna nebezpečí spojená se systémem (Identifikace nebezpečí)	A.4.1.1		
R_RA_129_03	Analyzovat všechna identi-fikovaná nebezpečí z hlediska jejich následků (Analýza následků nebez-pečí)	A.4.1.2		
R_RA_129_04	Odhadnout rizika plynoucí z identifikovaných nebez-pečí (Odhad rizika nebez-pečí)	A.4.1.2		
R_RA_129_05	Určit bezpečnostní poža-davky na systém (Určení THR)	A.4.1.2		
R_RA_159_01	Porozumět aplikaci daného systému pro schopnost rozhodování + stanovit globální bezpečnostní cíl (Aplikace)	D.1.1 a D.2.1		Zodp.: porozumění = = návrhář, stanovení bezp. cíle = uživatel, bezp. orgán (DÚ)
R_RA_159_02	Stanovit vrcholová nebez-pečí + uvážit provozní a jiné vnější okolnosti, které mohou vystavit systém nebezpečí (Analýzy nebez-pečí)	D.1.2 a D.2.2		
R_RA_159_03	Přiřadit na základě kvantita-tivního globálního bezpeč-nostního cíle a kvalitativní analýzy nebezpečí kvantita-tivní bezpečnostní cíle pro každé jednotlivé ohrožení – obecně nebezpečí (Ome-	D.1.3, D.2.3.1 a D.2.4.1		

	zení rizika)			
R_RA_159_04	Určit v závislosti na riziku úrovně SIL pro jednotlivé obrany + použít vhodné návrhové techniky a metody a určit HRs (Určení SIL a kvalitativních cílů bezpečnosti)	D.1.4, D.2.3.2 a D.2.4.2		
R_RA_159_05	Stanovit bezpečnostní požadavky (Specifikace bezpečnostních požadavků)	D.1.5		
R_RA_128_01	Použít systematický přístup pro: (i) identifikaci nebezpečí, rizik a kritérií (přijatelnosti) rizik; (ii) identifikaci nezbytného omezení rizika pro splnění kritérií (přijatelnosti) rizik; (iii) pro definování celkové specifikace požadavků na bezpečnost systému pro bezpečnostní opatření potřebných pro dosažení požadovaného omezení rizika.	Úvod		V uvedené normě toto není formulováno jako požadavek, nicméně považuji za velmi vhodné, aby tato skutečnost byla v navrhované metodice analýzy rizika zohledněna
R_RA_128_02	Prvotně odhadnout úroveň rizika bez zohlednění vlivu opatření pro snížení rizika. Tato opatření aplikovat následně až v závislosti na požadované úrovni integrity bezpečnosti systému.	Nepřímo z obrázku 1		V uvedené normě toto není formulováno jako požadavek, nicméně považuji za velmi vhodné, aby tato skutečnost byla v navrhované metodice analýzy rizika zohledněna

Tab. 1.4 – Souhrn požadavků evropských normativů na analýzu rizika

1.4 Analýza rizika systému ETCS a její specifika

Systém ETCS je evropský vlakový zabezpečovací systém (*angl. European Train Control System*). Technické specifikace tohoto celoevropského systému obecně vznikají na dvou úrovních (viz např. článek [***ŽEL11***]). Generické specifikace vznikají na úrovni evropské (nadnárodní), připravuje je pod záštitou evropské železniční agentury ERA sdružení výrobců tohoto systému – UNISIG (UNIon of SIGnalling). Toto sdružení dnes čítá devět společností. V abecedním pořadí jde o Alstom, Ansaldo STS, AŽD Praha, Bombardier, CAF Signalling, Invensys/Dimetronic[6], MERMEC, Siemens a Thales. UNISIG má několik pracovních skupin. Analýzou rizika systému ETCS, respektive stanovováním bezpečnostních požadavků na tento systém se zabývá pracovní skupina RAMS WP.

V této souvislosti je třeba konstatovat, že náplní práce skupiny RAMS WP není přímo vypracovávání analýzy rizika v pojetí evropských norem, nýbrž její hlavní náplní jsou – – velmi obecně a zjednodušeně řečeno – dvě základní činnosti, jež tato skupina vykonává a jež souvisejí se stanovováním bezpečnostních požadavků na systém ETCS:

I. Jednak jde o systematické přidělování požadovaných THR jednotlivým komponentám systému ETCS dle referenční architektury, což je provedeno v Subsetu-088 [***SS088***], jenž se skládá ze tří věcných částí a jedné části popisné. Výsledky tohoto Subsetu jsou shrnuty v mandatorním Subsetu-091 [***SS091***], který stanovuje generické bezpečnostní požadavky na systém ETCS úrovně 1 a 2 a který je uveden v příloze A Technických specifikací pro interoperabilitu TSI CCS [***TSI***].
II. Jednak jde o soubor bezpečnostních analýz (iniciovaných obvykle zkušenostmi získanými z běžících projektů aplikací systému ETCS), jejichž výsledkem je v případě, že se skutečně identifikuje nějaké nebezpečí související se systémem ETCS, provedení záznamu do záznamu o nebezpečí. Součástí tohoto záznamu je též navržení nápravného opatření pro snížení, popř. eliminaci tohoto nebezpečí. Tyto záznamy jsou shromažďovány v neveřejném UNISIG Hazard Logu [***UHL***] a následně zveřejňovány ve Zprávě z tohoto Hazard Logu, tedy ve volně na stránkách ERA dostupném Subsetu-113 [***SS113***].

Lze tedy tvrdit, že na této úrovni neexistuje analýza rizika jako taková (tedy v pojetí evropských norem). Spíše jde o soubor bezpečnostních analýz, nežli o analýzu rizika vedenou striktně dle evropských normativů citovaných výše v této kapitole. Spoléhá se pravděpodobně na to, že takovouto analýzu rizika vykoná každý výrobce dané aplikace systému ETCS na svou vlastní zodpovědnost, ovšem se zohledněním zde zmíněných bezpečnostních analýz a stanovených požadavků [pozn. jde o osobní názor autora této práce, člena UNISIG RAMS

[6] Během psaní této disertační práce došlo ke koupení společnosti Invensys společností Siemens.

WP]. Právě možnými způsoby zohlednění bezpečnostních analýz a požadavků vzniknuvších v této pracovní skupině v národních projektech se zabývá kapitola 4.7, „Specifika související s řízením rizika systému ETCS“.

2 CÍL ŘEŠENÉHO VĚDECKÉHO ÚKOLU A ZVOLENÉ METODY ZKOUMÁNÍ

Cíle této disertační práce byly již stanoveny v odborné práci [***ODP***]. Zde jsou pouze zrekapitulovány, případně zpřesněny, rozšířeny. Je třeba připomenout, že se jedná o stanovení metodiky analýzy rizika železničních zabezpečovacích systémů (tj. stanovení postupu při její tvorbě, včetně návrhu metod používaných při této její tvorbě). Práce je v konkrétních záležitostech dále zaměřena na aplikaci vybraného železničního zabezpečovacího systému, kterým je v případě této disertační práce (s ohledem na odborné zaměření jejího autora) systém evropského vlakového zabezpečovacího systému ETCS.

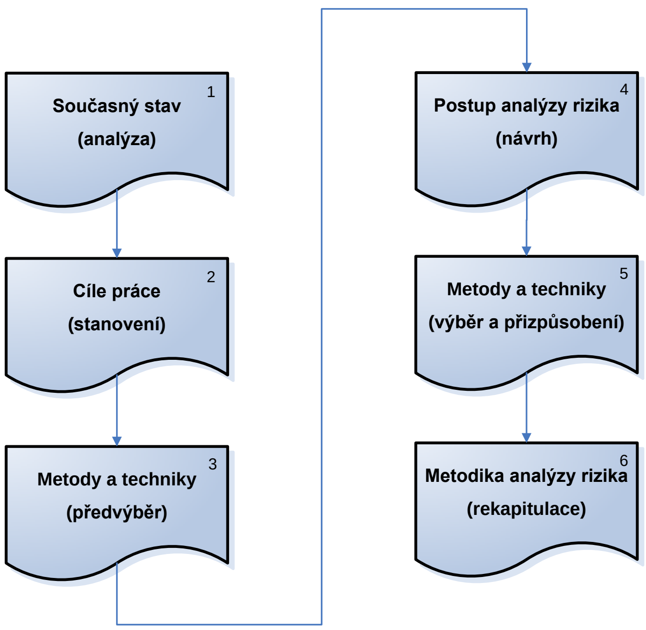
Ve světle uvedeného byly cíle této disertační práce stanoveny následovně:

I. stanovit vhodný přístup k analýze rizika a s ním související kroky analýzy rizika,
II. stanovit postup tvorby analýzy rizika v rámci jejích jednotlivých kroků,
III. vybrat a patřičně přizpůsobit metody vhodné k realizaci jednotlivých kroků analýzy rizika.
IV. rozšiřující bod (rozšiřující je proto, že není obsažen v cílech stanovených již v [***ODP***], byl stanoven dodatečně až při zpracovávání této disertační práce): navrhnout obecně vhodný přístup k řízení rizika bezpečnostně-kritických systémů, jehož nedílnou součástí je právě analýza rizika.

Vlastní disertabilní jádro celé práce bude tedy tvořit můj vlastní pohled na problematiku analýzy rizika železničních zabezpečovacích systémů a vytvoření metodiky (vlastního postupu tvorby, volbu a návrh vhodných metod a dalších náležitostí) analýzy rizika.

Tato disertační práce by se měla snažit přistupovat k zadanému problému co možná nejobecněji a nejkomplexněji, tj. neměla by se zabývat jen analýzou rizika konkrétního zabezpečovacího systému (aplikace systému ETCS v ČR), ale měla by obecně řešit otázky související s řízením rizika bezpečnostně-kritických systémů, přičemž ale v konkrétních případech by se měla zaměřit na vyřešení doposud neprobádaných záležitostí týkajících se systému ETCS. Kupříkladu by měla odpovědět na otázku, jak konkrétně je možno vhodně a průkazně respektovat nebezpečí identifikovaná na evropské úrovni UNISIG/ERA v hazard lozích jednotlivých projektů (aplikací systému ETCS) na národních úrovních.

Ke splnění výše nastíněných cílů bude tato disertační práce přistupovat tak, že nejdříve bude, resp. již byl proveden rozbor současného stavu poznání (viz kap. 1). Tento rozbor je proveden zejména se zaměřením na normativní požadavky týkající se analýzy rizika, jejichž naplnění je nutnou podmínkou pro získání kladného hodnocení bezpečnosti analyzovaného bezpečnostně-kritického systému. Tento rozbor současného stavu bude tvořit esenciální podklad pro následný návrh vhodného přístupu k tvorbě analýzy rizika železničních zabezpečovacích systémů, obecněji pak k řízení rizika bezpečnostně-kritických systémů. Tento přístup je navržen tak, aby naplňoval mandatorní požadavky relevantních evropských normativů.



Obr. 2.1 – Předpokládaná struktura disertační práce

Na obr. 2.1 je uvedena předpokládaná struktura této disertační práce, která reflektuje výše nastíněný přístup k danému tématu, tj. k analýze rizika (aplikace systému ETCS). Členění na tomto obrázku odpovídá členění jednotlivých kapitol této práce. Číslo kapitoly koresponduje s číslem znázorněným v pravém horním rohu každého bloku na obr. 2.1. V každém bloku je dále uvedeno téma a hlavní činnost s ním související. Tyto činnosti jsou uvedeny v závorce. Vědecké metody zkoumání, které předpokládám budou k tomuto účelu použity, byly již uvedeny a popsány v kapitole 4 práce [***ODP***]. Předpokládám, že tímto přístupem bude možno splnit výše v této kapitole stanovené cíle této disertační práce.

Zajímavé bude kromě výběru a přizpůsobení k analýze rizika vhodných metod také najít vhodný a provozovatelem dráhy v podmínkách konkrétního projektu odsouhlasitelný způsob hodnocení rizika (tj. následků nebezpečí, četností jejich výskytů a rizik z nich plynoucích, tedy včetně stanovení nebo lépe odvození kritérií přijatelnosti rizik), pro což dosud neexistuje všeobecně uznávaný postup.

3 METODY A TECHNIKY VYUŽITELNÉ PŘI ANALÝZE RIZIKA

3.1 Předvýběr vhodných metod/technik

Obecné pojednání o vědeckých metodách zkoumání je již zachyceno v odborné práci [***ODP***]. Proto je zde toto pojednání o metodách a technikách (dále jen metodách) zaměřeno už jen na ty, které jsou vhodné (jejich použití se jeví jako potenciálně užitečné) pro oblast zaměření této práce, tedy na jejich použití v rámci analýzy rizika obecně. V této kapitole jsou – prozatím bez znalosti konkrétního přístupu k analýze rizika – vyjmenovány a blíže popsány metody, které splňují stanovené kritérium. Jako kritérium pro jejich bližší zkoumání jsem si stanovil jejich výskyt v normě [***129***], resp. v její příloze E, což považuji za dostatečné. Ovšem platnost této hypotézy se prokáže až v následujících kapitolách, kde se bude rozhodovat o tom, které metody a jakým způsobem při analýze rizika využít.

Výše zmíněné kritérium k výběru metod pro bližší zkoumání jsem stanovil na základě následující úvahy. Nyní předpokládám, že nedílnou součástí analýzy rizika je též analýza nebezpečí. Pokud tedy platí předchozí a analýza nebezpečí je vždy součástí analýzy rizika, je dle mého názoru možno při výběru dílčích metod vyjít ze seznamu metod pro analýzu poruch a nebezpečí stanovených v normě [***129***], respektive v její příloze E. V této příloze jsou ovšem uvedeny jen názvy těchto metod, což není zdaleka dostačující, ba leckdy i zavádějící. Není totiž vždy patrné, o kterou metodu se jedná (např. u těch názvů, jenž sdílí více různých metod, konkrétně např. diagramy „příčina-následek“). Z toho důvodu byl tento jejich seznam v tab. 3.1 rozšířen o poznámky s odkazy na zdroje obsahující popisy, o nichž se lze domnívat, že nejlépe odpovídají požadovanému účelu.

Metoda/technika/opatření	**Úroveň integrity bezpečnosti (SIL)**				**Poznámka**
	1	**2**	**3**	**4**	
Předběžná analýza nebezpečí *(Preliminary hazard analysis)*	HR				[***PZH***], [***STR***], [***508-7***]
Analýza stromu poruchových stavů *(Fault tree analysis)*	R		HR		[***508-7***], [***ZAZS***], [***BŽZS***], [***SCS***], [***PZH***]
Markovovy diagramy *(Markov diagrams)*	R		HR		[***BŽZS***], [***PZH***]
Analýza druhů, důsledků a kritičnosti poruch *(Fault modes, effects, and criticality analysis)*	R		HR		[***508-7***], [***BŽZS***], [***SCS***], [***PZH***]

Studie nebezpečí a provozuschopnosti *(Hazard and operability study)*	R	HR	[***882***], [***SCS***], [***PZH***], [***HAZOP***], [***RHOP***]
Diagramy „příčina-následek“ *(Cause-consequence diagrams)*	R	HR	[***508-7***], [***PZH***], [***DPN***]
Analýza stromu událostí *(Event tree analysis)*[7]	R		[***508-7***], [***SCS***], [***PZH***]
Blokové schéma bezporuchovosti *(Reliability block diagram)*	R		[***BŽZS***], [***SCS***], [***PZH***]
Pásmová analýza *(Zonal analysis)*	R		
Analýza nebezpečí rozhraní *(Interface hazard analysis)*	R	HR	
Analýza poruch se společnou příčinou *(Common cause failure)*	R	HR	
Analýza historické události *(Historical event analysis)*	R	R	

Tab. 3.1 – Metody a techniky, jejichž použití přichází do úvahy v rámci v této práci stanovované metodiky analýzy rizika

Dále jsou popsány vhodné metody s jejich hodnocením z hlediska jejich využitelnosti při tvorbě analýzy rizika. Toto téma bylo již nastíněno v příspěvku [***MRA***], který autor této práce publikoval a přednesl před odbornou veřejností na semináři Elektrotechnická zařízení v dopravě v roce 2012. Blíže zkoumány budou metody z tab. 3.1, pro které platí, že:

I. jsou běžně užívané i v jiných oborech, tudíž i jejich popis je běžně dostupný a jejich použití je prověřeno v praxi;
II. jsou uvedeny pro provedení analýzy rizika též v normě [***126-1***] (tedy nejsou uvedeny pouze v normě [***129***]), což jen potvrzuje správnost jejich výběru k danému účelu.

Uvedeným dvěma kritériím odpovídají následující metody: Předběžná analýza nebezpečí [pozn. tato analýza je sice v normě [***126-1***] uvedena, ovšem jako činnost předcházející vlastní analýze rizika]; Analýza stromu poruchových stavů; Markovovy diagramy; Analýza

[7] V normě [***129***] je metoda “Analýza stromu událostí“ označována jako „Strom událostí *(Event tree)*“, zde byla přeznačena v souladu s „Analýzou stromu poruchových stavů“.

druhů, důsledků a kritičnosti poruch; Studie nebezpečí a provozuschopnosti; Diagramy „příčina-následek“; Analýza stromu událostí; Blokové schéma bezporuchovosti.

3.2 Popis a hodnocení vybraných metod/technik

3.2.1 Předběžná analýza nebezpečí (PHA)

Předběžná analýza nebezpečí, někdy též označovaná jako předběžná analýza zdrojů rizika (PHA, Preliminary Hazard Analysis) slouží k prvotní identifikaci a popisu nebezpečí. Je to technika vojenského původu, která byla odvozena z požadavků bezpečnostního programu amerického vojenského standardního systému [***PZH***]. V běžných oblastech svého použití se analýza PHA soustřeďuje na nebezpečné látky a procesy. Je nejčastěji prováděna na samém počátku vývoje procesu či systému, kdy ještě není známo mnoho detailních informací. Ovšem analýza PHA může být užitečná nejen u právě vyvíjených systémů, ale též při analýze již existujících systémů.

Analýza PHA kromě identifikace nebezpečí souvisejících s analyzovaným systémem, umožňuje navíc kvantitativní popis těchto nebezpečí a jejich seřazení podle úrovní rizik. Toho může být využito například při stanovování doporučení pro snížení rizik v následných fázích životního cyklu analyzovaného systému. Výstupem analýzy PHA je seznam identifikovaných nebezpečí s jejich popisem, jenž je obsahem formuláře, jehož ukázka je na obr. 3.1.

Ozn.	Nebezpečí	Nehoda (následek)	Pravděpodobné příčiny	Nápravná opatření	Četnost	Kritičnost	Pozn.

*Obr. 3.1 – Příklad formuláře PHA [**SRT**]*

Dle [***SRT***] může být analýza PHA použita buď jako počáteční studie rizika v začátku vývoje systému, nebo jako počáteční krok detailní analýzy rizika systému. Popřípadě může být použita jako kompletní analýza rizika, ovšem pouze za předpokladu hodně jednoduchého systému. Detailnější a propracovanější podobu analýzy PHA se stejným účelem představuje analýza FMEA, resp. FMECA (viz bod ε).

Analýza PHA tudíž může být dobře využita například jako podpůrný prostředek při rozhodování, zda jde o významnou změnu či nikoli dle směrnice [***49***], tedy o tom, zda se má na tuto změnu uplatnit harmonizované hodnocení a řízení rizik. Zde se totiž vychází z předběžné definice systému stanovené v etapě koncepce systému.

3.2.2 Studie nebezpečí a provozuschopnosti (HAZOP)

Studie HAZOP (Hazard and Operability Study) umožňuje systematicky prozkoumat daný proces nebo činnost daného systému a na základě toho stanovit, zda jeho procesní odchylky mohou vést k nežádoucím následkům (tj. k nebezpečí nebo provozním problémům). Tato studie pochází z Anglie a byla vyvinuta původně pro analýzu chemických procesů [***VHAZ***]. Je to kvalitativní technika vyvinutá jak pro identifikaci a vyhodnocení nebezpečí, tak i pro identifikaci a vyhodnocení provozních problémů snižujících provozní výkonnost celého procesu, které jsou způsobeny odchylkami od projektového záměru [***PZH***]. Od tohoto faktu je odvozen i vlastní název této studie.

Člen týmu		Charakteristika
Vedoucí studie		někdo se zkušenostmi z oblasti provádění HAZOP, který se ale přímo nepodílí na vývoji analyzovaného procesu; jeho role slouží k zajištění, že metoda je řádně prováděna
Zapisovatel		jeho role slouží k zajištění, že identifikované problémy jsou dokumentovány a doporučení jsou předány dále
Člen odborného týmu	Vývojář	jeho role slouží k poskytování podrobnějších informací, které souvisejí s vývojem analyzovaného procesu
Člen odborného týmu	Uživatel	jeho role slouží k poskytování podrobnějších informací, které souvisejí s použitím a provozuschopností analyzovaného procesu a s dopady případných odchylek
Člen odborného týmu	Specialista	někdo s odpovídajícími technickými znalostmi; jeho role slouží k poskytování další podpůrných informací
Člen odborného týmu	Údržbář	někdo zabývající se údržbou; jeho role slouží k poskytování podrobnějších informací, které souvisejí s procesem údržby

*Tab. 3.2 – Ukázka typických rolí členů týmu HAZOP dle [**882**]*

Studie HAZOP se realizuje formou řízené odborné diskuse mezi členy odborného týmu, kteří systematickým přístupem zkoumají daný proces. Tímto způsobem tým odhaluje potenciální problémy s různými nebezpečími či provozuschopností daného procesu, které jsou způsobeny odchylkami od procesního projektu či záměru a které mohou vést k nebezpečnému či provozně nežádoucímu stavu. Diskusi řídí vedoucí studie. Na kvalitu výsledků studie HAZOP má velký vliv sestavení tzv. HAZOP týmu, který toto zkoumání realizuje. Na jeho sestavení existují různá doporučení. Kupříkladu norma [***882***] doporučuje složit tým z členů, jejichž stručná charakteristika je uvedena v tab. 3.2.

Je vidět, že je důležité HAZOP tým složit ze zástupců se znalostmi a zkušenostmi z různých oblastí (různých etap životního cyklu). Systematický přístup při provádění studie HAZOP potom spočívá v tom, že členové tohoto týmu procházejí jednotlivá procesní schémata a snaží se systematickým způsobem vytvářet odchylky od projektovaných stavů. Systematičnosti při vytváření těchto odchylek napomáhají tři základní záležitosti:

I. stálá sada klíčových slov (ukázka jedné takové sady klíčových slov je uvedena např. v [***HAZOP***]),
II. seznam procesních parametrů,
III. soubor procesních schémat (vč. projektových záměrů v konkrétních bodech).

Klíčová slova jsou v kombinaci s procesními parametry aplikována na určité body v procesních schématech. Tuto teorii si bude lépe osvětlit na krátkém příkladě.

Příklad: Uvažujme například následující sadu klíčových slov: „Není“, „Více“, „Méně“ a procesní parametr: „Povolující návěst“. Máme-li v konkrétním bodě procesního schématu projektový záměr „Rozsvítit povolující návěst“, získáme kombinací uvedených klíčových slov a uvedeného procesního parametru následující odchylky od tohoto záměru: „Není rozsvícena povolující návěst“, „Je rozsvícena méně povolující návěst“, „Je rozsvícena více povolující návěst“. HAZOP tým se potom zabývá možnými příčinami a následky těchto odchylek a dále pak v případě potřeby navrhuje vhodná nápravná opatření.

Tímto postupem je možno systematicky identifikovat a vyhodnocovat téměř všechny odchylky, které mohou (byť i jen hypoteticky) nastat, a navrhovat pro ně nápravná opatření. Celý proces analýzy HAZOP a její výsledky zapisovatel zaznamenává do formuláře HAZOP. Příklad takového formuláře je na obr. 3.2.

Ozn.	Klíčové slovo	Procesní parametr	Odchylka	Možné příčiny	Následky	Exist. ochrany	Pozn.	Požad. činnosti	Zodp.

*Obr. 3.2 – Příklad formuláře (pracovního výkazu) HAZOP [**RHOP**]*

Tato technika může být dle [***PZH***] použita jak pro spojité, tak pro vsádkové procesy a může být též přizpůsobena pro vyhodnocování psaných postupů. Při provádění studie HAZOP je posuzován nejen seznam možných příčin a následků dané odchylky, ale i již existující ochrany zabraňující příčinám či následkům vzniku dané odchylky. V případě, že se zjistí nedostatečná ochrana proti dané odchylce, lze snadno prostřednictvím této studie doporučit další opatření vedoucí ke snížení rizika, včetně stanovení pracovníků zodpovědných za realizaci těchto nápravných opatření.

Ač tato technika byla původně vyvinuta pro předvídání nebezpečí a provozních problémů pro technologii, se kterou měl podnik malé zkušenosti, ukázalo se, že ji lze efektivně využít i pro již existující procesy. Ovšem vždy musí být u těchto procesů k dispozici detailní návrhové informace, jako např. vývojový diagram procesu, vyčerpávající popis procesu, diagramy P&ID, diagramy „příčina-následek“ a další (blíže například v [***HAZOP***]). Je tedy zřejmé, že provedení studie HAZOP vyžaduje podrobnou znalost analyzovaného procesu či systému a je nejčastěji užívána pro analyzování procesů/systémů až během detailní projektové fáze nebo po ni [***PZH***].

Z toho důvodu se studie HAZOP zatím jeví jako nevyhovující pro analýzu rizika, která má dle [***126-1***] proběhnout na samém začátku vývoje zabezpečovacího systému (ve 3. etapě jeho životního cyklu). Do úvahy by ovšem přicházela například při opakované analýze rizika, která se dle [***126-1***] vykonává za určitých okolností v průběhu životního cyklu, tedy již s detailnější znalostí analyzovaného systému.

3.2.3 Analýza stromu poruchových stavů (FTA)

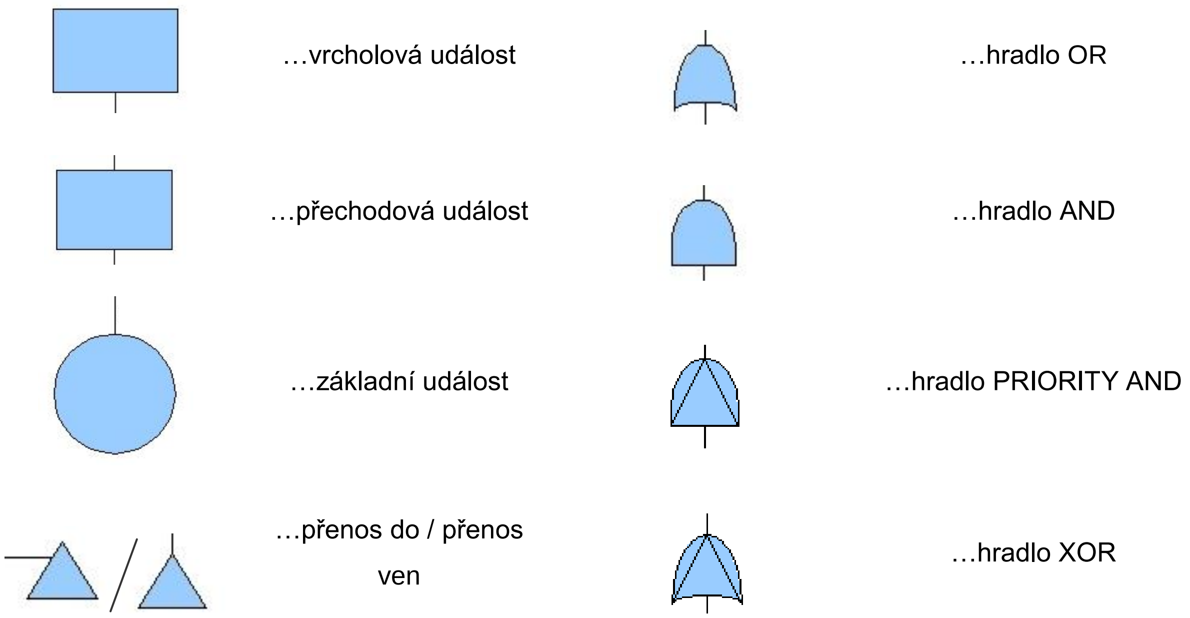
Analýzu stromu poruchových stavů (Fault Tree Analysis) lze úspěšně použít k identifikaci a analýze událostí, které vedou k nežádoucí vrcholové události nacházející se na vrcholu stromu (poruchových stavů). Tato technika vznikla v 60. letech minulého století v Bellových laboratořích původně pro účely amerického vojenského letectví, konkrétně údajně pro analýzu poruch atomové mezikontinentální balistické střely LGM-30 Minuteman [***HFTA***].

Analýza FTA přistupuje ke zkoumání příčin vedoucích k vrcholové události, která představuje poruchový stav, přístupem shora–dolů. Při konstrukci stromu poruchových stavů je nejprve definována vrcholová událost (na úrovni systému) a k ní jsou následně hledány postupně její příčiny (na úrovních nižších). V každém kroku tvorby stromu jsou hledány bezprostřední příčiny, tzn. příčiny na nejbližší nižší úrovni, čímž vzniká strom, jehož „větve“

představují posloupnosti událostí vedoucích k nežádoucí vrcholové události. Tyto dílčí události mohou být dvojího druhu:

I. přechodové události, které se dále (v následujícím kroku) dělí na dílčí příčiny;
II. základní události, které se již dále na dílčí příčiny nedělí.

Základní symboly používané při konstrukci stromu poruchových stavů jsou na obr. 3.3. Pro logické pospojování dílčích událostí (vrcholové, přechodových a základních) se používají hradla, jejichž význam je shodný s jejich použitím v logice, tj. například výstupní událost hradla AND nastane, pouze tehdy pokud nastanou současně všechny jeho vstupní události. Pro simulaci sekvenčnosti některých závislostí lze s výhodou využít tzv. hradlo PRIORITY AND, jehož výstup nastane, pouze tehdy pokud všechny jeho vstupní události nastanou v daném pořadí (obvykle musí nastávat postupně zleva doprava).



Obr. 3.3 – Základní symboly používané při analýze FTA (HTA)

Výsledkem analýzy FTA je strom poruchových stavů, který graficky zobrazuje (logické) vazby mezi nežádoucí vrcholovou událostí na úrovni systému a jejími příčinami na nižších úrovních. Vzniknuvší strom tvoří výsledek kvalitativní analýzy logických či sekvenčních vazeb daného systému. Tento strom ovšem může dále posloužit jako základ pro následnou kvantitativní (četnostní či pravděpodobnostní) analýzu tohoto systému (viz obr. 3.4).

Při zmíněné kvantitativní analýze stromu FTA se, jak vidno z obr. 3.4, využívají znalosti z teorie pravděpodobnosti. Dále je z tohoto obrázku zřejmé, že se v něm předpokládá nezávislost a neslučitelnost výskytu jevů jednotlivých událostí A, B, C a D. V opačném případě by totiž bylo nutno použít následující obecnější vzorce pro logický součin a součet, kdy platí:

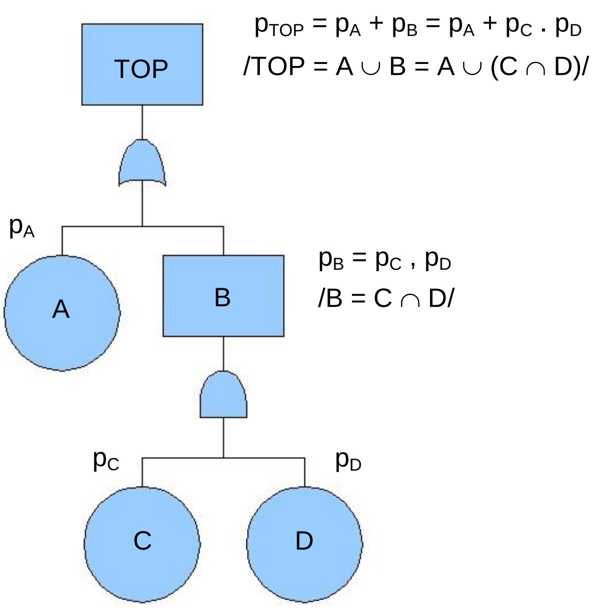
a) pro součet pravděpodobností výskytu dvou (slučitelných) jevů $A \cup B$:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{3.1}$$

b) pro součin pravděpodobností výskytu dvou (závislých) jevů $A \cap B$:

$$P(A \cap B) = P(A) \,.\, P(B \mid A) \tag{3.2}$$

Ovšem jsou-li jevy navzájem nezávislé a neslučitelné, výše uvedené výrazy se velmi zjednoduší, což je názorně předvedeno na následujícím obrázku (obr. 3.4).



Obr. 3.4 – Ukázka stromu poruchových stavů

Tímto způsobem lze zkoumat systém nejen z hlediska jeho spolehlivosti, ale též z hlediska jeho bezpečnosti, neboť bezpečnost má z určitého úhlu pohledu (viz např. publikaci [***ZAZS***]) pravděpodobnostní charakter. Rozdílnost obou přístupů spočívá v tom, že v prvním případě je vrcholovou událostí poruchový stav, zatímco ve druhém případě je jí nebezpečný stav. Zde se lze přidržet terminologie, která byla zavedena v publikaci [***ZAZS***], kde je v druhém případě (vrcholová událost = nebezpečný stav) označován strom poruchových stavů jako tzv. strom ohrožení a vlastní analýza jako tzv. analýza stromu ohrožení (HTA, Hazard Tree Analysis).

3.2.4 Markovovy diagramy (MD)

Markovovy diagramy umožňují prostřednictvím svého matematického aparátu popsat dynamické chování systémů, které splňují určité vlastnosti, a následně provést exaktní matematickou analýzu takto získaného popisu. Obecně platí, že pro popis daného systému Markovovým diagramem musí být možno popsat stavy tohoto systému náhodným procesem, který musí splňovat následující podmínky:

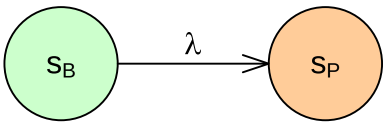
I. tento náhodný proces je tvořen posloupností náhodných veličin X_t: $\{X_t;\ t \geq 0\}$, kde $X_t \in N^+$ a $t \in R^+$ (proces s diskrétním stavovým prostorem a spojitým časem);
II. tato posloupnost musí splňovat tzv. Markovskou vlastnost, což znamená, že pro libovolná reálná nezáporná čísla taková, že $0 \leq t_1 < t_2 < \ldots < t_n < t < t+\Delta t$, a pro všechna přirozená čísla $s_1, s_2, \ldots, s_n, s_i, s_j$ platí vztah: $P(X_{t+\Delta t} = s_j \mid X_t = s_i, X_{tn} = s_n, \ldots, X_2 = s_2, X_1 = s_1) = P(X_{t+\Delta t} = s_j \mid X_t = s_i)$, což znamená, že pravděpodobnost přechodu systému ze stavu s_i do stavu s_j závisí pouze na stavu bezprostředně předcházejícím a nezávisí na stavech dřívějších, tj. stavech, ve kterých se systém nacházel před časem t (Markovův proces);
III. pravděpodobnost přechodu ze stavu s_i do stavu s_j (tj. $P(X_{t+\Delta t} = s_j \mid X_t = s_i)$, kterou též zkráceně označujeme jako $p_{ij}(t, t+\Delta t)$) nezávisí na čase t, ale pouze na délce časového intervalu Δt, tj. $p_{ij}(t, t+\Delta t) = p_{ij}(\Delta t)$, a tudíž i intenzity $a_{ij}(t) = a_{ij}$ a $a_{ii}(t) = a_{ii}$ jsou na čase t též nezávislé (homogenní proces).

Pokud systém splňuje výše uvedené vlastnosti, lze jej popsat následujícím vztahem, který charakterizuje spojitý homogenní Markovův proces (s diskrétním stavovým prostorem):

$$\vec{p}'(t) = \vec{p}(t)\mathbf{A}, \qquad (3.3)$$

kde $\vec{p}(t)$ je vektor absolutních pravděpodobností, přičemž jeho jednotlivé složky $p_i(t)$ vyjadřují pravděpodobnost, že se systém v čase t nachází ve stavu s_i (tj. $p_i(t) = P(X_t = s_i)$), a $\mathbf{A}$ je matice intenzit přechodů (tj. $A = [a_{ij}]$), kde a_{ij}, resp. a_{ii} jsou intenzity přechodů systému ze stavu s_i do stavu s_j, resp. záporně vzaté intenzity výstupu systému ze stavů s_i (viz např. [***BŽZS***]).

Příklad Markovového diagramu ukazuje obr. 3.5, který zachycuje chování neobnovovaného systému, jenž se může nacházet ve dvou stavech: bezporuchovém s_B a poruchovém s_P. Přičemž intenzita přechodu ze stavu s_B do stavu s_P je rovna intenzitě poruch λ. Lze tvrdit, že Markovovy diagramy představují kvantitativní techniku, která umožňuje matematicky (pomocí dvou základních struktur: vektoru počátečních pravděpodobností $\vec{p}(0)$ a matice intenzit přechodů **A**) popsat dynamické chování systémů, které splňují určité vlastnosti, a následně provést exaktní matematickou analýzu tohoto popisu (vedoucí na řešení soustavy diferenciálních rovnic). Tímto postupem lze zkoumat pravděpodobnosti, s nimiž se systém nachází v různých stavech v daných časových okamžicích (intervalech). Markovovy diagramy tedy mohou při analýze rizika velmi dobře posloužit při přesnějším zkoumání vybraných funkčních vlastností zabezpečovacích systémů.



$$\square \quad \mathbf{A} = \begin{pmatrix} -\lambda & \lambda \\ 0 & 0 \end{pmatrix} \quad \square$$
$$\vec{p}(0) = (1, 0)$$

$$\square \quad \begin{array}{c} \vec{p}'(t) = \vec{p}(t).\mathbf{A} \\ \hline p'_{s_B}(t) = -\lambda . p_{s_B}(t) \\ p'_{s_P}(t) = \lambda . p_{s_B}(t) \\ \hline p_{s_B}(t) = e^{-\lambda . t} \\ p_{s_P}(t) = 1 - e^{-\lambda . t} \end{array} \quad \square \quad \vec{p}(t) = \left(e^{-\lambda . t}, 1 - e^{-\lambda . t}\right)$$

Obr. 3.5 – Ukázka Markovového diagramu

Výhoda Markovových diagramů popsaná výše se z určitého pohledu může jevit jako jejich nevýhoda, neboť právě jejich velká komplexnost s sebou pro systémy s velkým počtem dosažitelných stavů (rozsáhlým stavovým prostorem) přináší neúměrné narůstání matematického popisu těchto systémů a činí tak výpočty velmi komplikované. S výhodou je ale lze použít pro menší systémy, či menší části rozsáhlých systémů.

3.2.5 Analýza druhů, důsledků a kritičnosti poruch (FMECA)

Analýza FMECA (Fault Modes, Effects, and Criticality Analysis) vychází z analýzy FMEA (Fault Modes and Effects Analysis), která primárně slouží ke zkoumání důsledků jednotlivých druhů poruch systému a umožňuje též ve spojení s konkrétními prvky systému jejich ohodnocení. Jedná se o techniku, která přístupem zdola–nahoru umožňuje identifikovat prvky systému, které mají významný (kritický) vliv na požadovanou funkci, resp. na její selhání. Při této identifikaci vychází z poruch na úrovni prvků systému a zkoumá, jakým způsobem se projeví jejich důsledky na nejbližší vyšší úrovni, a to až po úroveň celého systému, resp. systémem řízeného procesu.

Porucha			Důsledek poruchy			Hodnocení (poruchy)	Poznámka
číslo	součást	druh	chyba	selhání	výstup		

*Obr. 3.6 – Příklad formuláře (pracovního výkazu) FMEA [**AFME**]*

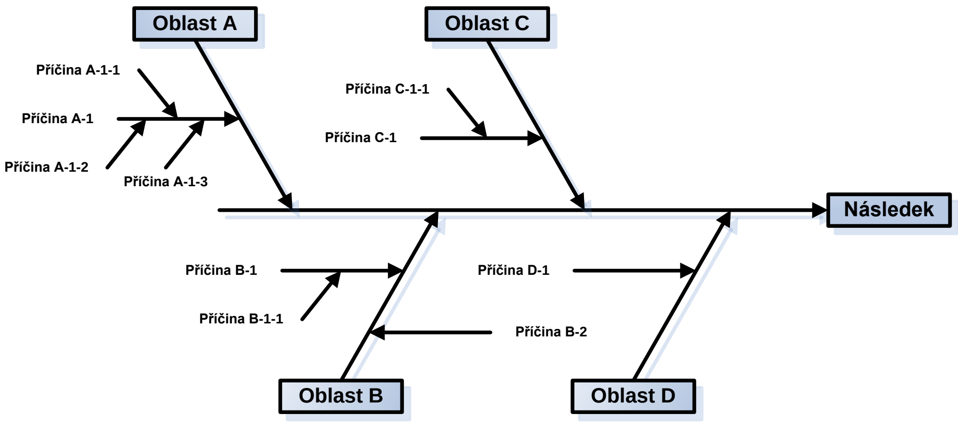
Analýza FMEA je tedy kvalitativní technika umožňující prozkoumat důsledky různých druhů poruch a ohodnotit je. Velmi vhodné a praxí ověřené je například použití analýzy FMEA při rozboru bezpečnosti poruch, při kterém se prokazuje a hodnotí bezpečnost zabezpečovacích systémů pracujících na principu vnitřní bezpečnosti. Tímto způsobem lze totiž relativně snadno a systematicky prokázat splnění požadavků na technickou bezpečnost těchto systémů, tj. jejich bezpečnost při poruše, jak je mimo jiné patrno z článku [***AFME***]. Analýza FMECA umožňuje navíc rovněž ohodnotit i jejich kritičnost, což by mohlo být využitelné pro popis nebezpečí na různých úrovních dekompozice systému a hledání jejich příčin.

Tato metoda se jeví jako velmi dobře využitelná při analýze rizika zabezpečovacích systémů. Zejména použije-li se tato metoda k bližšímu zkoumání nebezpečí (tedy nejen poruch) souvisejících s analyzovaným systémem, jejich příčin a následků. Takto upravený formulář je popsán v kapitole 5.2.2.

3.2.6 Diagramy „příčina–následek“ (CCD)

Diagramy „příčina–následek“ (Cause-Consequence Diagrams), někdy též označované podle svého vzhledu jako diagramy „rybí kostry“, či podle svého tvůrce (Kaorua Ishikawy) jako Ishikawy diagramy, slouží primárně k prozkoumání potenciálních i reálných příčin, které vedou k nežádoucímu následku. Je to velmi jednoduchá grafická technika vyvinutá v 60. letech minulého století původně pro systémy řízení jakosti [***DPN***].

Při konstrukci diagramu „příčina–následek“, neboli diagramu „rybí kostry“ (viz obr. 3.7) se postupuje přístupem shora–dolů. Nejdříve je načrtnuta vodorovná přímka (rybí páteř) ukončená šipkou směřující k nežádoucí události – následku (rybí hlavě). Poté jsou připojeny vedlejší přímky (rybí kosti) se základními oblastmi, ve kterých se předpokládá výskyt hledaných příčin. Konkrétní příčiny jsou poté uspořádány buď podle jejich úrovně důležitosti nebo podle úrovně jejich detailu.



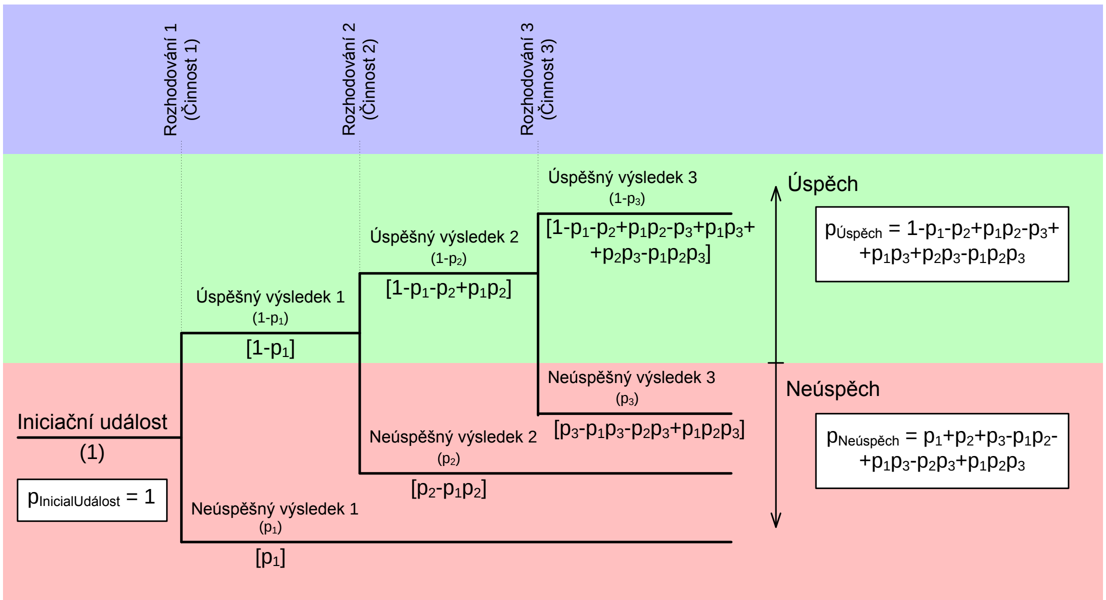
Obr. 3.7 – Ukázka Ishikawa diagramu

Diagramy „příčina–následek“ tedy zobrazují příčinné souvislosti mezi koncovými stavy nehody (resp. jejími následky) a důvody jejího vzniku (resp. jejími příčinami). Vznikají tak diagramy obsahující nehodové sekvence s kvalitativními popisy možných koncových stavů nehod [***PZH***]. Diagramy „příčina–následek“ jsou pro svou relativní jednoduchost, časovou nenáročnost a snadnou pochopitelnost poměrně často používány v různých oblastech.

V souvislosti s analýzou rizika je možno diagramy „příčina–následek“ použít jako doplňkový prostředek pro hledání všech možných příčin daného nebezpečí na dané úrovni zkoumání, tj. kupříkladu v rámci analýzy FMECA při vyplňování sloupce „příčina“ v jejím přizpůsobeném formuláři dle kapitoly 5.2.2.

3.2.7 Analýza stromu událostí (ETA)

Analýza stromu událostí (Event Tree Analysis) slouží k prozkoumání všech možných koncových stavů (tj. následků) nehody, která vznikla po tzv. iniciační události (např. porucha prvku systému, selhání lidského faktoru) [***PZH***]. Při analýze ETA jsou přístupem zdola–nahoru procházeny všechny možné kombinace reakcí systému na definovanou iniciační událost, čímž se lze velmi systematicky dobrat přes všechny možné (úspěšné i neúspěšné) postupné následky iniciační události ke všem možným (koncovým) důsledkům této iniciační události. Tento iterativní proces ilustruje obr. 3.8.



Obr. 3.8 – Ukázka stromu událostí

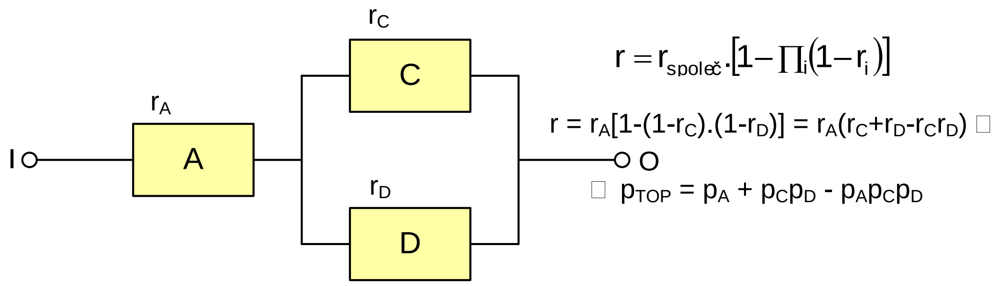
Výsledkem (kvalitativní) analýzy ETA jsou tedy graficky znázorněné scénáře nehod, tj. soubor chyb nebo poruch, které vedou k nehodě. Jinak řečeno, analýza ETA umožňuje vysledovat každou cestu ke konečnému úspěchu/neúspěchu a graficky znázornit všechny hodnověrné kombinace stavů systému [***ETAT***]. Tyto grafické scénáře je možno následně podrobit kvantitativní (pravděpodobnostní) analýze, tak jak to v principu okazuje obr. 3.8.

Modelování stromů tedy obecně slouží pro statické, grafické znázorňování logických nehodových scénářů (platí obdobně i pro strom poruchových stavů – viz bod γ)). V rámci analýzy rizika lze prostřednictvím těchto stromů například hledat všechny možné následky daného nebezpečí.

3.2.8 Blokové diagramy bezporuchovosti (RBD)

Blokové diagramy bezporuchovosti (Reliability Block Diagram) slouží především pro posuzování systému z hlediska spolehlivosti, později se tato technika začala využívat i pro posuzování systému z hlediska bezpečnosti. Přesněji řečeno, je to technika původně vyvinutá pro analýzu ukazatelů bezporuchovosti a pohotovosti (resp. dostupnosti) pro neobnovované objekty, u nichž navíc nezáleží na pořadí vzniku poruch [***BŽZS***]. Při realizaci blokových diagramů bezporuchovosti se předpokládá, že se systém může nacházet pouze v jednom ze dvou předdefinovaných stavů (provozuschopném – poruchovém, popř. bezpečném – nebezpečném apod.).

Při tvorbě diagramů RBD se analyzovaný systém rozdělí na vhodné funkční bloky, které se dle jejich vlivu na zkoumanou vlastnost tohoto systému vzájemně logicky pospojují (uspořádají), čímž vznikne jejich sériové, paralelní, sérioparalelní, popř. všeobecné řazení. Uvažujeme-li např. funkčnost, resp. nefunkčnost systému, pak sériová kombinace jednotlivých funkčních bloků říká, že systém je **funkční** jen tehdy, jsou-li všechny tyto bloky funkční. Jejich paralelní kombinace naopak říká, že systém je **nefunkční** jen tehdy, jsou-li všechny tyto bloky nefunkční. Řazení bloků v diagramu RBD nemusí odpovídat jejich fyzickému uspořádání v systému (např. jeden a týž blok může být v diagramu RBD použit vícekrát, i když v reálném systému se vyskytuje pouze jednou).



Obr. 3.9 – Ukázka blokového schématu bezporuchovosti

Příklad diagramu RBD je na obr. 3.9. Diagramy RBD lze dále kvantitativně analyzovat. K tomu je možno využít několik možných přístupů:

I. přístup využívající vlastnosti základních typů uspořádání jednotlivých funkčních bloků analyzovaného systému, tj. sériového a paralelního uspořádání;
II. přístup využívající booleovské pravdivostní tabulky;
III. přístup využívající metody minimálních řezů nebo minimálních cest.

Jedná se tedy o kvantitativní techniku, která je rovnocenná s logicky komplementární analýzou k analýze FTA, s tzv. STA (*Success Tree Analysis*) a která slouží pro zkoumání určité vlastnosti (parametru) analyzovaného systému [***FTAW***]. Z toho důvodu je v rámci analýzy rizika zabezpečovacích systémů tato metoda s výhodou využitelná v její kvantitativní části. V souvislosti s tím je ovšem třeba zdůraznit jedno zásadní omezení platné pro požití této metody (uvedené např. v [***BŽZS***]) hovořící o tom, že základní podmínkou použití diagramů RBD je vzájemná logická nezávislost jednotlivých funkčních bloků.

3.3 Shrnutí použitelných metod/technik

Máme-li shrnout použitelnost výše uvedených metod v rámci analýzy rizika, je možno konstatovat, že z výše uvedených popisů jednotlivých metod plyne, že ač se jedná o metody původně určené normou [***129***] pro analýzu vlivů poruchových stavů a nebezpečí, bude jich možno použít i pro analýzu rizik vyplývajících z analyzovaného zabezpečovacího systému. Rovněž je patrno, že některé metody umožňují pouze kvalitativní hodnocení rizika (PHA, HAZOP, FME(C)A), jiné též jeho kvantitativní hodnocení (FTA, ETA, RBD, MD). A že některé kvantitativní metody umožňují pouze statickou analýzu (RBD, FTA, ETA), jiné též dynamickou analýzu (MD).

Z uvedených metod se jako velmi vhodné (i pro jejich dobré reference) jeví pro analýzu rizika metoda FTA, která je též užívána v rámci sdružení UNISIG pro tvorbu funkční bezpečnostní analýzy systému ETCS [***SS088***]. Rovněž metoda ETA je v této oblasti použitelná a byla použita například při posuzování bezpečnosti rozhraní pro strojvedoucího (DMI) systému ETCS [***SDMI***]. Z první skupiny metod lze jmenovat například metodu FMECA, která je používána opět v rámci sdružení UNISIG pro analýzu jednotlivých druhů poruch na mandatorních rozhraních systému ETCS [***SS078***], [***SS079***], [***SS080***] [***SS081***]. V tomto kontextu nelze opomenout metodu MD, která může v komplikovanějších případech, kdy matematický aparát výše uvedených metod není postačující, tyto metody vhodně doplňovat.

Detailnější popis vybraných metod (zejména FMEA, FMECA a FTA) a jejich přizpůsobení, aby vyhověly zde navržené metodice analýzy rizika je součástí kapitoly 5, „Přizpůsobení metod vhodných ke zde stanovené metodice analýzy rizika“.

4 PŘÍSTUP K ANALÝZE RIZIKA

V této kapitole je autorem navržen vhodný přístup k analýze rizika železničních zabezpečovacích systémů (aplikace evropského vlakového zabezpečovacího systému ETCS), jehož dodržení plní požadavky v kapitole 1 zkoumaných evropských relevantních normativů. Dále jsou zde podrobněji rozebrány jednotlivé kroky tohoto přístupu a vytipovány příhodné metody, jež byly zkoumány v kapitole 3 a jimiž lze jednotlivé kroky tohoto přístupu naplnit. Modifikace těchto metod, tak aby vyhovovaly danému účelu použití v rámci analýzy rizika, je součástí kapitoly 5. Celkové shrnutí zde navržené metodiky analýzy rizika je v kapitole 6. Je tedy patrné, že tato čtvrtá, pátá a šestá kapitola tvoří hlavní jádro této disertační práce.

4.1 Obecný přístup k analýze rizika

Zde je stanoven obecný přístup k analýze rizika (tedy jednotlivé kroky analýzy rizika) bezpečnostně-kritických systémů vyhovující potřebám železniční zabezpečovací techniky, respektive vyhovující zejména aplikaci systému ETCS v ČR.

4.1.1 Výchozí podklady pro stanovení vhodného přístupu

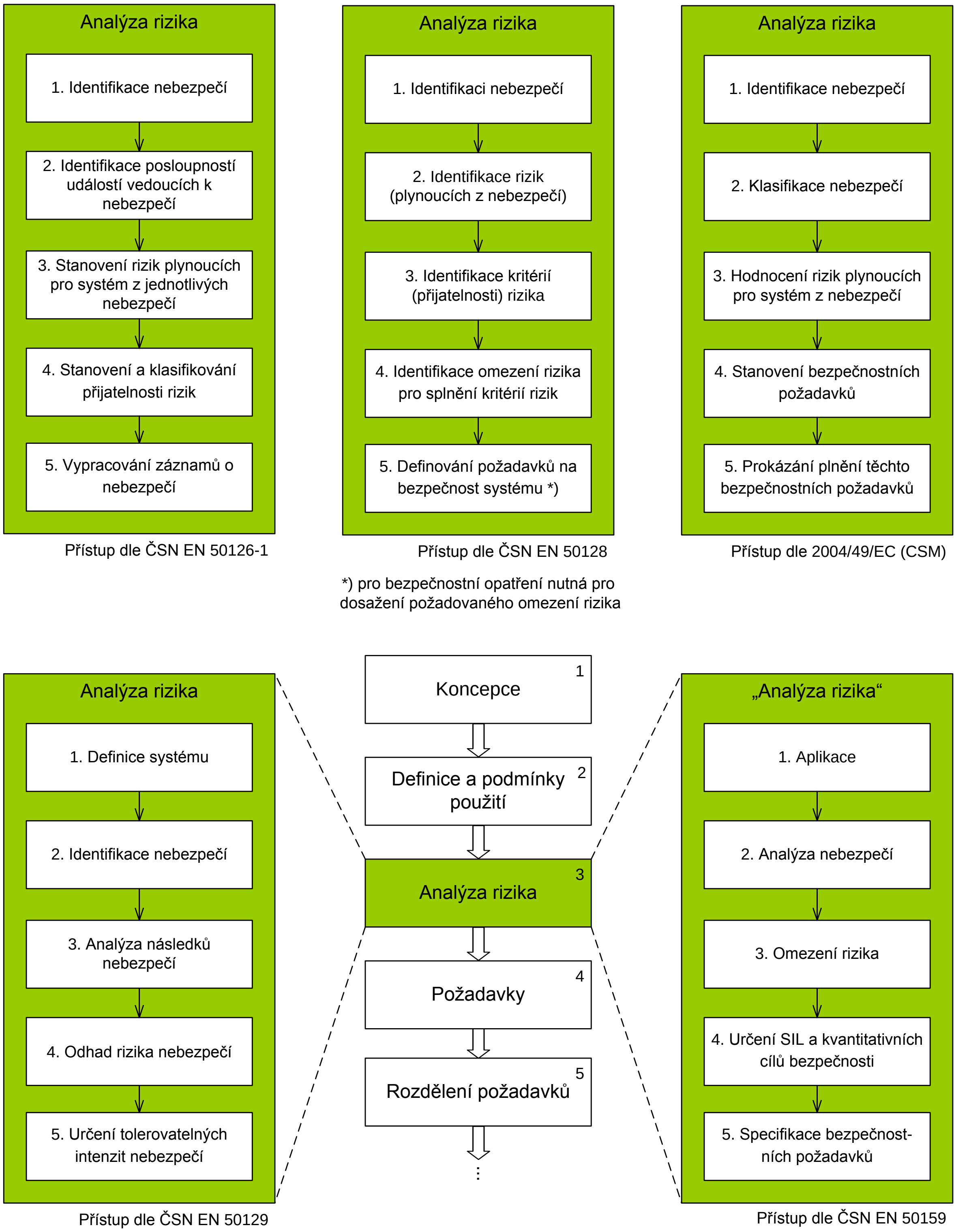
Při stanovování obecného vhodného přístupu tvorby analýzy rizika železničních zabezpečovacích systémů (obecněji přístupu k řízení rizik – blíže viz kap. 4.6) jsem předně vycházel z následujících evropských norem/směrnic/doporučení (dále jen normativů):

I. ČSN EN 50126-1:2007 (Stanovení a prokázání RAMS drážního systému) [***126-1***]
II. ČSN EN 50129:2003 (Elektronické zabezpečovací systémy) [***129***]
III. ČSN EN 50128:2012 (Software pro drážní řídicí a ochranné systémy) [***128***]
IV. ČSN EN 50159:2011 (Bezpečná komunikace v přenosových systémech) [***159***]
V. 2004/49/EC (Drážní bezpečnostní směrnice) [***49***]
VI. Doporučení evropské železniční agentury související se směrnicí 2004/49/EC [***49***], jako např. [***DissPpt***], [***CsmRep***], [***CsmArt***].

A z jejich analýzy provedené v kapitole 1. V následujícím textu bude zkoumána hypotéza, že je možno přístupy jednotlivých evropských norem (a to včetně směrnice 2004/49/EC a doporučení k ní vydaných) zobecnit a sjednotit takovým způsobem, aby vznikl jednotný postup, který by nebyl v rozporu ani s jedním z těchto normativů.

4.1.2 Sjednocení a rozšíření přístupů relevantních evropských normativů

Na obrázku 4.1 jsou znázorněny přístupy k tvorbě analýzy rizika železničních systémů dle evropských normativů citovaných v předcházející kapitole (viz kap. 4.1.1). V následujícím textu budou poupraveny a sjednoceny, aby vyhověly požadovanému použití.



Obr. 4.1 – Přístupy k tvorbě analýzy rizika dle jednotlivých zkoumaných normativů

Zaměřme se tedy postupně na všechny kroky přístupů jednotlivých evropských normativů. Zde je třeba nejprve zdůraznit, že na obrázku výše (viz obr. 4.1) znázorněné kroky analýzy rizika nejsou v leckterých normativech takto explicitně uvedeny, nicméně dle mého názoru, současných poznatků a zkušeností lze toto přiblížení pro dané normativy považovat za dostatečně reprezentativní. Snažil jsem se v těchto přístupech (jednotlivých jejich krocích) shrnout všechny hlavní myšlenky týkající se analýzy rizika, samozřejmě vždy s ohledem na příslušný evropský normativ.

Všechny přístupy zachycené graficky na obrázku 4.1 obsahují identifikaci nebezpečí (i když norma [***159***] tento krok obsahuje implicitně, a to v kroku analýza nebezpečí; lze totiž předpokládat, že pro vykonávání analýzy nebezpečí je nutno nejprve následně analyzovaná nebezpečí identifikovat). Tento krok lze tedy považovat za první krok zde navrhovaného přístupu. Nicméně je třeba si povšimnout, že dva normativy (konkrétně normy [***129***] a [***159***]) požadují provést před vlastní identifikací nebezpečí, jež je tedy součástí každého na obrázku 4.1 uvedeného postupu analýzy rizika, ještě definici systému (pozn. v přístupu normy [***159***] se tento krok skrývá pod krokem aplikace a tato skutečnost je patrná z kontextu). Definici systému jakožto součást analýzy rizika tedy požadují normy [***129***] a [***159***].

Dle mého názoru je považování definice systému za nedílnou součást analýzy rizika nadbytečné, a to i přesto, že tato činnost (důsledná definice systému, specifikace jeho rozhraní a podmínek použití) je nezbytná pro korektní provedení analýzy rizika. Přesto si myslím, že není nutno tuto činnost považovat za její nedílnou součást, tak jak je tomu v přístupech obou zmíněných norem. Důvodem je skutečnost, že definice systému při vývoji zabezpečovacího systému v souladu s životním cyklem dle normy [***126-1***] nezávisle na tom, zdali je vývoj daného zabezpečovacího systému veden přesně podle etap touto normou definovaného životního cyklu, či nikoli, protože předem stanovený jiný životní cyklus musí samozřejmě respektovat základní rysy touto normou definovaného životního cyklu (viz např. [***ARSP***]). Lze tedy předpokládat, že i nově definovaný životní cyklus bude obsahovat jak analýzu rizika, tak definici systému, která bude velmi pravděpodobně vlastní analýze rizika (v pojetí, jak je chápána v této práci) rovněž předcházet.

Pro názorné předvedení předchozího je na obrázku 4.1 naznačeno, jak přístupy norem [***129***] a [***159***] souvisí s životním cyklem železničních systémů, tak jak jej definuje norma [***126-1***]. Definice systému[8] dle zmíněného životního cyklu představuje samostatnou vývojovou etapu předcházejí vlastní analýze rizika. Z toho důvodu zde navržený postup analýzy ri-

[8] „Aplikace“ dle [***159***] v kontextu této normy znamená totéž, co definice systému dle [***129***]. Jde totiž o znalost (pochopení) použití daného systému, samozřejmě při nezbytné znalosti jeho definice.

zika tento krok (tj. krok 1 dle [***129***], či [***159***]) vynechává a začíná identifikací nebezpečí spojených s analyzovaným systémem (tj. krokem 1 dle [***126-1***], [***128***], [***49***], resp. krokem 2 dle [***129***], [***159***]).

Po identifikaci nebezpečí, do níž je možno bezpochyby zahrnout rovněž krok identifikace posloupností událostí vedoucích k identifikovaným nebezpečím (tj. krok 2 dle [***126-1***]), lze sledovat kroky navazující, hodnotící rizika plynoucí z jednotlivých identifikovaných nebezpečí. Konkrétně se jedná o následující kroky:

I. stanovení rizik plynoucích z identifikovaných nebezpečí (tj. krok 3 dle [***126-1***]),
II. identifikace rizik plynoucích z identifikovaných nebezpečí (tj. krok 2 dle [***128***]),
III. klasifikace nebezpečí a hodnocení rizik plynoucích z identifikovaných nebezpečí (tj. krok 2 a 3 dle [***49***]),
IV. analýza následků identifikovaných nebezpečí a odhad rizik plynoucích z těchto nebezpečí (tj. kroky 3 a 4 dle [***129***]),
V. analýza nebezpečí (tj. krok 2 dle [***159***]).

Po ohodnocení nebezpečí z hlediska rizika je třeba na základě předem stanovených (tj. krok 3 dle [***128***]) kritérií přijatelnosti rizika rozhodnout, zda je konkrétní riziko přijatelné, či nikoli (tj. např. krok 4 dle [***126-1***], v ostatních normativech není tento krok explicitně jmenován, ale vždy je třeba, aby tato kritéria byla řádně stanovena před krokem hodnotícím rizika související s identifikovanými nebezpečími). Pokud se ukáže (dle téže kritérií), že riziko je přijatelné, není třeba podnikat další kroky (pouze je třeba toto dokumentovat, což při v této práci navržené metodice analýzy rizika bude splněno automaticky). Pokud se ukáže, že riziko není přijatelné, je třeba v dalším kroku analýzy rizika navrhnout vhodná nápravná opatření pro snížení tohoto rizika na přijatelnou mez (tj. krok 4 dle [***128***] a krok 3 dle [***159***]). Toto se zákonitě musí odrazit v bezpečnostních požadavcích na analyzovaný systém (tj. krok 5 dle [***128***], krok 4 dle [***49***] a krok 5 dle [***159***]).

Požadavek na implementaci dodatečného opatření, které během analýzy rizika identifikované riziko redukuje na přijatelnou úroveň, vyvolává v podstatě bezpečnostní požadavek na analyzovaný systém. Dále je bezpodmínečně nutno zajistit a prokázat plnění takto stanovených bezpečnostních požadavků během následující části životního cyklu daného systému (krok 5 dle [***49***]). Mezi bezpečnostní požadavky se potom řadí jak kvalitativní požadavky – požadavky na tolerovatelnou četnost hazardů THR, tak kvalitativní požadavky – požadavky na úroveň integrity bezpečnosti SIL pro jednotlivé funkce, u nichž se požaduje, aby byly odvozeny na základě analýzy rizika (viz např. krok 5 dle [***129***], resp. krok 4 dle [***159***]).

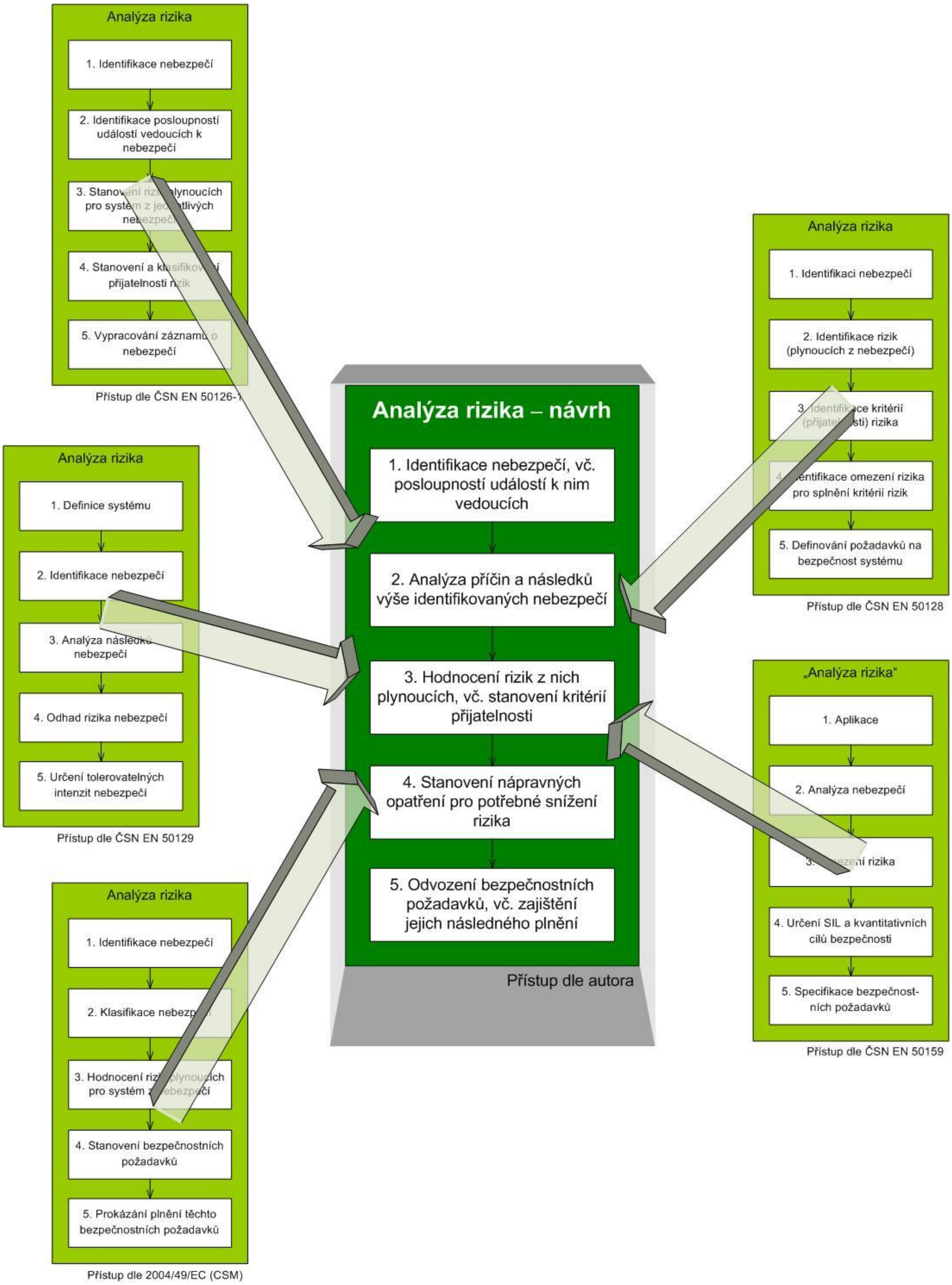
Vedle řízení rizik prostřednictvím analýzy rizika, čemuž byl věnován předchozí text, je velmi důležité sledovat a řídit případná rizika objevená mimo analýzu rizika, respektive po jejím vykonání. S tím se domnívám souvisí záznamy o nebezpečí (krok 5 dle [***126-1***]), které tvoří „samostatnou kapitolu“ v procesu řízení rizik a kterým se v této disertační práci věnuje kapitola o řízení rizika (viz kap. 4.5). Ovšem zde je na místě si položit otázku týkající se vypracovávání záznamů o nebezpečích identifikovaných v rámci analýzy rizika, u nichž bylo identifikováno zbytkové riziko: Je nutno tyto záznamy pro dokumentování a odsouhlasení řízení těchto nebezpečí, které již jednou byly zadokumentovány v rámci analýzy rizika, vypracovávat? Podle mého názoru jsou dvě možné cesty. Buď lze nechat celkově odsouhlasit analýzu rizika, pak nemá smysl z důvodu duplicity tyto záznamy o nebezpečí vůbec zakládat; nebo lze nechat odsouhlasit jen záležitosti uvedené v záznamech o nebezpečí, pak toto ovšem smysl má, ba dokonce je to nezbytnost. Osobně se kloním k první variantě.

4.1.3 Stanovení vhodného přístupu k analýze rizika

Před vlastním stanovením dílčích kroků analýzy rizika považuji za vhodné uvést výčet činností, které jsou dle mého názoru zásadní. Na podkladě rozborů a informací uvedených v předcházejících kapitolách se domnívám, že optimální obecný přístup k analýze rizika spočívá v provedení následující posloupnosti činností:

I. provede se identifikace nebezpečí spojených se systémem
II. analyzují se příčiny a následky těchto nebezpečí
III. ohodnotí se tato nebezpečí z hlediska rizika
IV. stanoví se nápravná opatření pro omezení rizika
V. definuje se postup pro řízení rizik identifikovaných následně

Činnostem prováděným v rámci analýzy rizika (tj. činnostem vyjmenovaným výše, zejména pak identifikaci nebezpečí) musí předcházet definice systému, podmínek použití a specifikace jeho rozhraní (viz druhá etapa životního cyklu dle [***126-1***]). Tyto činnosti mohou probíhat opakovaně v několika iteracích. Naopak po těchto činnostech musí následovat stanovení bezpečnostních požadavků odvozených právě ze závěrů analýzy rizika (viz čtvrtá, resp. pátá etapa životního cyklu dle [***126-1***]). Výše uvedené činnosti s jejich začleněním do jednotivých kroků analýzy rizika železničních zabezpečovacích systémů shrnuje s ohledem na relevantní evropské normativy obrázek 4.2.



Obr. 4.2 – Návrh přístupu k analýze rizika zabezpečovacích systémů

Na základě předchozího navrhuji následující přístup k analýze rizika, při němž je analýza rizika prováděna v následujících krocích [pozn. v závorkách jsou uvedeny odkazy na kapitoly této práce pojednávající o daných krocích podrobněji]:

I. identifikace nebezpečí spojených se systémem, resp. s jeho okolím (viz kap. 4.3.2)
II. ohodnocení rizik plynoucích z nebezpečí identifikovaných v kroku 1, vč. stanovení kritérií pro určení jejich přijatelnosti (viz kap. 4.3.3)
III. určení přijatelnosti rizik, vč. stanovení nápravných opatření snižujících riziko na přijatelnou úroveň (viz kap. 4.3.4)
IV. odvození bezpečnostních požadavků na analyzovaný systém, vč. zajištění jejich plnění během životního cyklu tohoto systému (viz kap. 4.3.5)

V. ošetření nebezpečí identifikovaných mimo analýzu rizika, tj. před a po této činnosti (viz kap. 4.5)

Dodejme jen, že vlastní analýze rizika v tomto pojetí předchází stanovení definice systému (viz kap. 4.3.1). Souhrnně je ale možno říci, že tento přístup zajišťující řízení rizika v rámci analýzy rizika spočívá v identifikaci nebezpečí (v této první fázi jde o kvalitativní část řízení rizika). Ta se provádí systematicky v oblastech dle normy [***126-1***]). Dále pak v analýze těchto nebezpečí, při níž se hledají posloupnosti událostí (příčiny a následky), četnosti a kritičnosti důsledků těchto nebezpečí. Poté přistupuje analýza rizik, kdy se kvantitativně ohodnocují rizika plynoucí z těchto identifikovaných nebezpečí, snižují se a na základě vhodného kritéria se přijímají [pozn. v rámci jedné a téže analýzy rizika je přípustné používat pro různá nebezpečí různá kritéria přijatelnosti]. Na základě analýzy rizika se poté stanovují bezpečnostní požadavky (odvozují se a procesně se zajišťuje jejich plnění v rámci celého životního cyklu analyzovaného zabezpečovacího zařízení).

Popsané pojetí analýzy rizika – samozřejmě za předpokladu, že do identifikace nebezpečí v něm patří též identifikace posloupností událostí vedoucích k identifikovaným nebezpečím – primárně vychází z normy [***126-1***], jejíž přístup rozšiřuje, a současně respektuje požadavky všech ostatních relevantních norem zmíněných v kapitole 4.1.1. Velmi podobné celkové pojetí analýzy rizika bylo již autorem této práce v praxi použito při analýze rizika jedné komponenty aplikace systému ETCS na Pilotním projektu ETCS v ČR v úseku Kolín––Poříčany, a to při analýze rizika elektronického rozhraní IRI (tj. rozhraní mezi RBC a stavědly upravujícího rozdílné bezpečnostní a komunikační principy obou zařízení – bližší informace o tomto rozhraní se lze dozvědět např. v práci [***MKha***]).

4.2 Návrh metod vhodných k jednotlivým krokům analýzy rizika

Jak již bylo uvedeno výše, identifikace nebezpečí spojených se systémem, resp. s jeho okolím (tj. krok 1 dle v této práci navrhovaného přístupu) je doporučováno podle evropských normativů provádět a podle zde navrženého přístupu se také provádí v oblastech vyjmenovaných v kapitole 4.3.2, vycházejících z oblastí vyjmenovaných v článku 6.3.3.1 normy [***126--1***]. Vlastní identifikaci nebezpečí spojených se systémem v daných oblastech provádí úvahou osoba, respektive skupina osob dostatečně v této oblasti erudovaných. Nebezpečí identifikovaná v jednotlivých oblastech mají být dle zde stanovené metodiky natolik obecná, aby v každé oblasti bylo identifikováno pouze jedno vrcholové tzv. základní nebezpečí.

K následné analýze těchto základních nebezpečí (tj. k hledání posloupností událostí /příčin a následků/, četností a kritičností důsledků těchto nebezpečí) se mi jako velmi výhodné jeví použití analýzy FMECA, a to v několika úrovních – krocích (viz dále). K tomuto účelu byly autorem této práce navrženy dva typy formulářů (jeden hodnotící kritičnost – FMECA pro následné kroky analýzy nebezpečí, druhý nikoli – FMEA pro první /resp. nultý/ krok analýzy nebezpečí; blíže viz kap. 6). Lze očekávat, že tyto formuláře budou v principu obsahovat několik částí, které budou charakterizovat:

I. analyzované nebezpečí
II. důsledky tohoto nebezpečí
III. hodnocení tohoto nebezpečí z hlediska rizika
IV. příčiny tohoto nebezpečí

Rozpracování výše uvedených částí navrhovaných formulářů a další bližší podrobnosti z této oblasti stanovuje kapitola 5.2.2. Takto získané příčiny, potažmo opět nebezpečí, ovšem na nižší úrovni podrobnosti (bod IV) navrhuji zapracovat do stromu FTA (Fault Tree Analysis), přesněji řečeno do stromu HTA (Hazard Tree Analysis) – viz [***ZAZS***], kde toto nebezpečí bude představovat dočasnou (tj. pro daný krok analýzy nebezpečí) základní událost, ze které se v následujícícm kroku této analýzy stane přechodová událost. V následujícím kroku analýzy se provede opět rozbor nebezpečí identifikovaných na této úrovni podrobnosti strukturovanou formou díky formuláři FMECA, jehož výsledky (příčiny základních nebezpečí) se opět zapracují do stromu FTA, respektive HTA (dále v textu budu používat jen sice méně přesnější, zato známější označení FTA).

Jak patrno, ohodnocení četností, následků a rizik plynoucích z identifikovaných nebezpečí a určení přijatelnosti rizik (tj. části kroků 2 a 3 dle v této práci navrhovaného přístupu s výjimkou stanovení kritérií pro určení jejich přijatelnosti a stanovení nápravných opatření snižujících riziko na přijatelnou úroveň) jsou součástí analýzy FMECA. Hodnocení rizik se děje v opět rámci analýzy FMECA, v její části III, a to na základě kritérií přijatelnosti rizik stanovených v kapitole 4.3.3. Chybějícím částem zmíněných kroků se věnuje kapitola 4.3.3 (hodnocení a přijetí rizika) a kapitola 4.3.4 (stanovení nápravných opatření).

Co se týká bezpečnostních požadavků odvozených z analýzy rizika (tj. krok 4 dle v této práci navrhovaného přístupu), lze tyto bezpečnostní požadavky kategorizovat do následujících dvou druhů:

I. kvalitativní – stanovení a (zajištění) realizace nápravných opatření
II. kvantitativní – stanovení požadavků na THR na jednotlivé funkce, potažmo na SIL, stanovující metody, jejichž použití je dle [***129***], popř. [***128***] při vývoji zabezpečovacího systému nutné).

Pro odvození bezpečnostních požadavků (zejména požadavků na THR) na jednotlivé funkce analyzovaného zabezpečovacího systému navrhuji provést prostřednictvím analýzy FTA (Fault Tree Analysis), respektive HTA (Hazard Tree Analysis) – pro věcný rozdíl mezi nimi odkazuji na [***ZAZS***]. Přičemž základní událostí tohoto stromu FTA, respektive základním nebezpečím tohoto stromu HTA je nebezpečí identifikované v oblasti, ve které se tato nebezpečí dle [***126-1***] hledají. Z toho plyne, že počet stromů FTA, respektive HTA (dále jen obecnější pojem FTA) bude maximálně tolik, kolik je oblastí, ve kterých se mají nebezpečí hledat. Maximálně je použito proto, že je nelze vyloučit, že se některá nebezpečí nebudou v různých oblastech shodovat.

Známe-li požadavek na THR (Tolerable Hazard Rate) vrcholového nebezpečí každého stromu FTA, je možno po ukončení kvalitativní části tvorby stromu pokračovat v kvalitativní části tvorby stromu. V kvantitativním ohodnocování jednotlivých událostí stromu doporučuji postupovat zde navrženou metodou vážení (viz kap. 5.3). Tato metoda vychází z esenciálního požadavku: Čím vyšší je riziko plynoucí z dané události (nebezpečí), tím vyšší má tato událost (nebezpečí) přidělenou váhu, a tím přísnější jsou požadavky kladené na bezpečnost funkce, jejíž selhání vyvolá nastání tohoto nebezpečí, tj. tím nižší musí být intenzita THR požadovaná pro tuto funkci. Podrobněji je tato metoda popsána v kapitole 5.3.4. Podrobnější popis a modifikace v této kapitole zmíněných metod pro jejich optimální využití ve zde stanovené metodice analýzy rizika železničních zabezpečovacích systémů lze nalézt v kapitole 5.

4.3 Podrobnější popis dílčích kroků analýzy rizika

4.3.1 Definice systému (není součástí analýzy rizika)

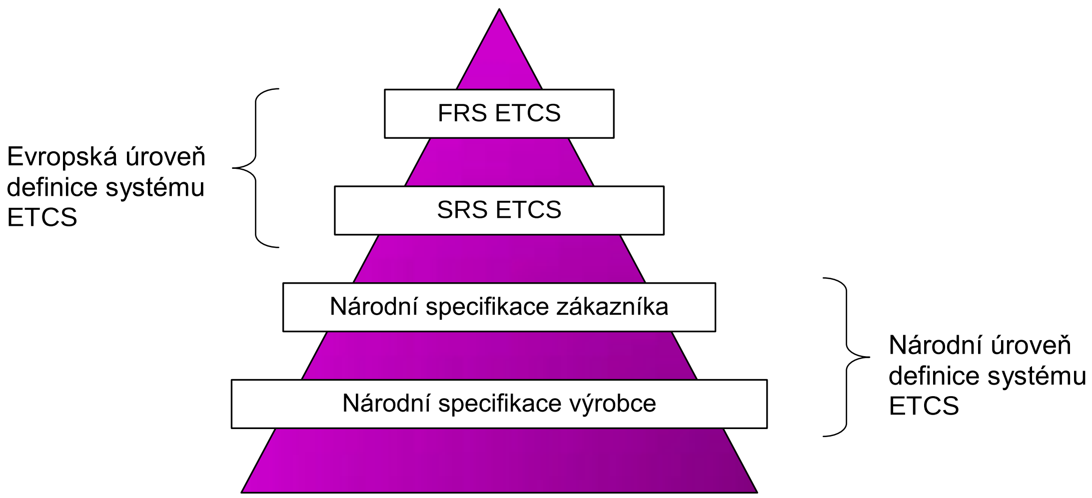
Jak již bylo zmíněno výše, otázka definice systému a stanovení vhodného okamžiku pro její vykonání je v různých evropských normativech rozporuplná. Někdy tvoří nedílnou součást analýzy rizika (např. v normě [***129***] a [***159***]), někdy vlastní analýze rizika předchází (podobně jako tomu je např. v [***126-1***], [***128***] a [***CSM***]). Je ovšem bezesporu nutné definici vyvíjeného systému v každém případě provést a dokumentovat na samém počátku vývoje daného systému, a to i přes to, že během následného vývoje lze očekávat její modifikaci ve formě dodatečného zpřesňování, doplňování.

Ačkoli krok definice systému osobně nepovažuji za součást analýzy rizika, úzce s ní souvisí a je velmi důležitý pro korektní identifikaci potenciálních nebezpečí souvisejících s vyvíjeným systémem. Definice systému a jeho rozhraní dle mého názoru tedy předchází vlastní analýze rizika. Tudíž každou její modifikaci, k níž dojde v době, kdy vypracovávání analýzy rizika již bylo zahájeno či dokonce již zcela proběhlo, je třeba posoudit z hlediska jejího vlivu na provedenou analýzu rizika či jen její část. Dále je zřejmé, že definice systému tvoří esenciální podklad pro analýzu rizika, obecněji pro řízení rizika bezpečnostně-kritických (zabezpečovacích) systémů. Na základě ní jsou totiž identifikována nebezpečí související s vyvíjeným systémem.

S definicí systému, jakožto základního podkladu pro identifikaci nebezpečí, souvisí i míra detailnosti této definice. Uvážíme-li okamžik v rámci celého životního cyklu dle [***126-1***], ve kterém k analýze rizika dochází, a současně výsledky, které má analýza rizika přinést, lze relativně snadno určit požadovanou míru detailnosti. Když zohledníme to, co bude teprve napsáno v dalším textu, lze konstatovat, že definice systému má jít do takové hloubky, do které chceme stanovovat bezpečnostní požadavky (THR, SIL atp.). Například určení SIL na počátku vývoje systému je velmi důležité proto, abychom následně byli schopni odvodit metody, které je dle [***129***] třeba používat při návrhu systému s danými požadavky na integritu bezpečnosti.

Obecně je možno k definici systému konstatovat, že tvoří nedílnou součást vývoje každého technického systému a současně tvoří též případně základní podklad pro analýzu rizika tohoto systému. V takovém případě musí definice systému předcházet analýze rizika jako takové – zde se tedy přikláním k přístupům normativů [***126-1***], [***128***], [***CSM***] a definici systému předřazuji před vlastní analýzu rizika (a do ní ji, i přes její nezbytnost, nezahrnuji). Přičemž toto je automaticky splněno, pokud se daný bezpečnostně-kritický systém vyvíjí dle životního cyklu stanoveného v normě [***126-1***], kterážto je pro železniční – tedy i zabezpečovací – systémy mandatorní. Předchozí (definice systému proběhne před analýzou rizika) je nutno považovat za předpoklad zde stanovované metodiky analýzy rizika.

Například systém ETCS (definice systému je již specifická záležitost, a tak je lépe se zaměřit již na definici konkrétního systému) je definován specifikacemi požadavků. Tyto specifikace – vzhledem k tomu, že tento systém představuje evropský (dnes již o něm lze dokonce hovořit jako o zcela obecně nadnárodním [***EWC***], tj. bez omezení na hranice Evropy) projekt – principiálně vznikají na dvou úrovních: evropské a národní. Tyto úrovně a jejich hierarchické uspořádání je naznačeno na obr. 4.3. Základním pravidlem v této hierarchii je, že požadavky specifikací na nižších úrovních vždy plně respektují požadavky specifikací na vyšších úrovních. Pokud by tomu tak nebylo, mohla by být narušena interoperabilita systému, čili jedna z jeho klíčových vlastností. Dále platí, že čím níže se na obrázku daná specifikace nachází, tím větší úroveň podrobnosti mají její požadavky.



Obr. 4.3 – Hierarchická struktura specifikací systému ETCS z hlediska jeho funkčního chování

Vzhledem k tomu, že analýza rizika se převážně zabývá provozními situacemi, které v provozu již představují mimořádnou událost dle [***Dp17***], při nichž může vzniknout škoda, věnuje se tento obrázek (obr. 4.3) i následující text záměrně zejména specifikaci požadavků na funkční chování systému ETCS, jež tvoří pro analýzu rizika podstatnou část celé specifikace, která je dána Subsety citovanými v příloze A technických specifikací TSI CCS [***TSI***].

Déle je samozřejmě při analýze rizika nutno přihlížet ke specifikacím ostatních Subsetů, zdůrazněme zde například Subset-040 „Dimensioning and Engineering rules“ [***SS040***], který lze použít pro získání mezních hodnot pro výchozí předpoklady analýzy, pokud je neudává přímo projekt, pro který je analýza rizika vykonávána (např. předpoklady o chování mobilní části ETCS – maximální počet současně zapamatovaných TSR, maximální/minimální přípustná vzdálenost antény pro čtení balíz od první nápravy, maximální přípustný konfidenční interval apod.).

Definice systému ETCS na evropské úrovni

Tato definice, terminologií normy [***129***], zahrnuje specifikaci požadavků na generický produkt, který může být používán pro různé nezávislé aplikace. To znamená s ohledem na systém ETCS kupříkladu pro jeho aplikace na různých železnicích. Specifikace požadavků na generický produkt sestává z:

I. specifikace funkčních požadavků (*Functional Requirement Specification*)[9],
II. specifikace systémových požadavků (*System Requirement Specification*).

Tyto specifikace se průběžně udržují, aktualizují a vyvíjí se jejich nové verze, což se děje pod záštitou Evropské železniční agentury ERA. Ta má také dle [***TSI***] za povinnost zveřejňovat plné verze těchto specifikací, což činí na svých webových stránkách. Na těchto jejích stránkách tak lze nalézt seznamy všech povinných [***ManSp***] i informativních [***InfSp***] specifikací systému ETCS. Závazný seznam všech na evropské úrovni vzniklých specifikací systému ETCS spolu s uvedením jejich aktuálně platné verze je v příloze A specifikací TSI pro oblast řízení a zabezpečení [***TSI***]. Tento seznam byl naposledy aktualizován v únoru roku 2012 [***AnA***], kdy současně došlo k přesunutí informativních specifikací systému ETCS do tzv. Příručky pro aplikaci TSI CCS (Guide for the Application of the TSI for the CCS) [***GTS***].

Ad 1. Specifikace funkčních požadavků na systém ETCS (FRS ETCS)

- aktuálně platná verze:

Baseline 2	Baseline 3
5.0	neexistuje (odstraněno)

[9] FRS ETCS nebyly pro Baseline 3 aktualizovány a byly vyřazeny z přílohy A specifikací TSI CCS, zůstávají ovšem stále platné (zařazené v příloze A) pro Baseline 2.

FRS obsahují dva druhy požadavků. Mandatorní (M), které jsou z hlediska interoperability nutné a které tudíž musí být vždy respektovány, a volitelné (O), které nejsou z hlediska interoperability nepostradatelné a které tudíž nemusí být vždy respektovány. Ovšem z hlediska bezpečnosti může být jejich respektování v některých případech vyžadováno, a to požadavky specifikací TSI pro oblast řízení a zabezpečení. Obecně lze říci, že se požadavky specifikací FRS zabývají převážně provozními záležitostmi a obsahují pouze několik technických pojmů. Z Baseline 3 byly FRS ETCS vyřazeny, tudíž se jimi není třena v rámci analýzy rizika aplikace systému ETCS dále zabývat.

Ad 2. Specifikace systémových požadavků na systém ETCS (SRS ETCS)

- aktuálně platná verze:

Baseline 2	Baseline 3
2.3.0d[10]	3.3.0

SRS rovněž obsahují mandatorní a volitelné požadavky, ovšem s odlišným významem oproti požadavkům FRS. Mandatorní požadavek v SRS znamená, že pokud bude daná funkce v konkrétní aplikaci použita, pak bude použita tak, jak to vyžaduje příslušný mandatorní požadavek, zatímco uplatnění požadavků volitelných je pro realizaci dané funkce volitelné. Požadavky SRS de facto zahrnují mandatorní (M) požadavky FRS transformované v technickou specifikaci určenou pro vývojové pracovníky. Požadavky SRS jsou rozděleny do několika tematických částí – kapitol popisujících: základní definici systému ETCS, principy systému ETCS (např. princip balízového souřadného systému, oprávnění k jízdě, vytváření dynamického rychlostního profilu), módy mobilní části systému ETCS (popis jednotlivých módů spolu s popisem podmínek přechodů mezi nimi), procedury probíhající v systému ETCS (např. začátek mise, konec mise), jazyk ETCS (jeho zprávy, pakety a proměnné).

Podrobněji se, vedle definice systému ETCS, strukturou a obsahem SRS (dále jen Subsetu-026) zabývá například článek [***ŽEL11***].

<u>Definice systému ETCS na národní úrovni</u>

Tato definice, terminologií normy [***129***], obsahuje specifikace požadavků na generickou a specifickou aplikaci, přičemž generická aplikace může být používána pro daný typ aplikace se společnými funkcemi (tj. v případě ETCS např. pro aplikaci v konkrétním státě) a

[10] SRS verze 2.3.0d (debugged) obsahuje všechny požadavky Subsetu-026 verze 2.3.0 se zahrnutím požadavků na změny (CRs) označených v Subsetu-108 verze 1.2.0 jako „IN“.

specifická aplikace může být použita pouze pro jednu určitou instalaci (např. pro určitý úsek tratě v daném státě). Specifikace požadavků na generickou a specifickou aplikaci sestává z:

I. specifikace požadavků zákazníka,
II. specifikace požadavků výrobce.

Ad 1. Specifikace požadavků zákazníka

V České republice, respektive na železničních tratích ve vlastnictví státu (SŽDC) tuto specifikaci obsahuje dokument [***TP***] (aktuálně platná verze 1.0.0). Jedná se o technický dokument, jenž obsahuje popis koncepce nasazování systému ETCS v ČR. Současně blíže určuje požadavky na projektování, realizaci, testování, schvalování a certifikaci systému ETCS pro použití na železničních tratích ve vlastnictví státu (SŽDC).

Ad 2. Specifikace požadavků výrobce

Jedním z výrobců systému ETCS je i česká společnost AŽD Praha, kde působí též autor této práce. Zde vzniká specifikace požadavků na systém ETCS ve formě případů užití (PU) (více o těchto PU lze nalézt např. v článku [***PUP***]), které popisují funkční chování celého systému ETCS v různých provozních situacích a které slouží pro snadnou komunikaci se zákazníkem stejně tak jako k následné tvorbě FRS na národní úrovni. Z těchto FRS pak vznikají SRS na národní úrovni. Tyto dokumenty (obsahující PU, FRS, SRS, příp. SSRS pro významné subsystémy systému ETCS) lze považovat za úplný výčet specifikací vznikajících na národní úrovni v podmínkách ČR (AŽD Praha).

<u>Definice systému ETCS pro potřeby analýzy rizika</u>

Jak již bylo napsáno výše, definice systému má jít do takové hloubky, do které chceme stanovovat bezpečnostní požadavky. Bezpečnostní požadavky je velmi výhodné a žádoucí stanovovat na jednotlivé funkce vyvíjeného systému. Tyto funkce jsou pro mobilní část systému ETCS stanoveny v Subsetu-026 [***SS026***], neboť tuto část je třeba pro dosažení interoperability harmonizovat (její funkční chování). Naopak pro traťovou část systému ETCS tyto požadavky na jednotlivé funkce stanoveny explicitně nejsou. Zde jsou jen Subsetem-026 [***SS026***] stanoveny principy a procedury, které je třeba prostřednictvím nikoli harmonizovaných funkcí traťové části systému ETCS (zejména RBC) realizovat.

Při definici systému ETCS, respektive jeho funkcí se tedy pro mobilní část systému ETCS lze přidržet definice těchto funkcí, tak jak je stanovuje kapitola 4.5 Subsetu-026

[***SS026***]. Pro definici funkcí traťové části systému ETCS je třeba hledat v dokumentaci zákazníka, respektive výrobce tohoto systému. V ČR je pro zdejší Komerční projekt ETCS v traťovém úseku Břeclav–Kolín [pozn. výrobcem a dodavatelem traťové části ETCS je v tomto projektu česká společnost AŽD Praha s.r.o.] možno tuto definici najít ve specifikaci systémových požadavků na traťovou část ETCS L2 [***SRS***].

Dále je patrné, že je velmi důležité věnovat se definovaným rozhraním mezi analyzovaným systémem a jeho okolím. Důvodem je skutečnost, že selhání jakékoli funkce určitého systému se projeví právě na rozhraní tohoto systému. A může dále v případě řídicího systému přes toto rozhraní přímou vazbou prostřednictvím akčních členů ovlivňovat řízený systém (tj. v případě železničního zabezpečovacího systému může tento ovlivňovat železniční dopravu). Rozhraní systému ETCS jsou definovaná jeho referenční architekturou, kterou stanovuje Subset-026 [***SS026***] ve své kapitole 2.5.3 a která je též zachycena na obrázku v kapitole 4.7 této práce (viz obr. 4.6). Detailněji se jednotlivým rozhraním po funkční stránce věnují následující dokumenty, Subsety:

I. Subset-034 definující rozhraní k vozidlu
II. dokument ERA_ERTMS_015560 definující rozhraní ke strojvedoucímu
III. Subset-036 definující rozhraní k Eurobalíze
IV. Subset-044 definující rozhraní ke Eurosmyčce
V. Subset-037 a dokument A 11 T 6001 definující rozhraní prostřednictvím Eurorádia jak k mobilním zařízením, tak k pevným zařízením GSM-R
VI. Subset-047 definující výše uvedená rozhraní (bod V) využívající doplňkového (infill) Eurorádia
VII. Subset-114 definující rozhraní k centru správy klíčů (KMC)
VIII. Subset-038 definující rozhraní mezi sousedními centry správy klíčů (KMC)
IX. Subset-100 definující rozhraní mezi balízou a národním systémem
X. Subset-101 definující rozhraní mezi moduly BTM a STM
XI. Subset-035, -056, -057 a -058 definující rozhraní k modulu STM
XII. Subset-027 definující rozhraní k záznamové jednotce JRU
XIII. Subset-039 a Subset-098 definující rozhraní mezi sousedními RBC

*Poznámka k explicitně neuvedeným referencím: Všechny výše uvedené dokumenty je možno nalézt, spolu s ostatními dokumenty definujícími technické specifikace systému ETCS, na webových stránkách Evropské železniční agentury ERA [**ERA**].*

Systém ETCS je obecně bezpečný systém, který plní své funkce s požadovanou mírou bezpečnosti. Ovšem některá rozhraní definovaná specifikacemi uvedenými výše se týkají komponent nikoli-bezpečných. V takovém případě je třeba v rámci analýzy rizika stanovit na toto rozhraní alespoň jeden bezpečnostní požadavek, a to takový, že je třeba během následujícího vývoje systému prokázat, že toto rozhraní neovlivní negativně bezpečnostně-kritické části systému ETCS.

Podíváme-li se dále z obecného pohledu na rozhraní systému ETCS definovaná jeho referenční architekturou, potažmo dokumenty uvedenými na předcházející straně a na rozbor již vykonaných bezpečnostních analýz na úrovni ERA/UNISIG (viz kap. 4.7.1), zjistíme, že všechna významná rozhraní (až na jedno) byla již analyzována. Jediné rozhraní, kterým je třeba se zabývat, je rozhraní ke stávajícímu zabezpečovacímu zařízení (blok „Interlocking" na obr. 4.6), pro které nebyla na této úrovni žádná analýza zpracována. Jde o rozhraní, jenž vlakovému zabezpečovači ETCS poskytuje informace nezbytné pro bezpečnou jízdu vlaku pod dohledem ETCS. Důvodem, proč nebylo na úrovni ERA/UNISIG analyzováno, je podle mého názoru skutečnost, že harmonizace toto rozhraní není z hlediska dosažení interoperability nutná, tudíž ani není na této úrovni harmonizováno, a tudíž jeho analyzování bez znalosti jeho definice je na této úrovni genericky neproveditelná. Nicméně, právě proto se předpokládá, že toto rozhraní bude analyzováno v konkrétních projektech aplikací systému ETCS.

*Komentář související s definicí systému ETCS a jeho referenční architekturou (viz obr. 4.6): Osobně nesouhlasím s tím, že traťová elektronická jednotka (LEU) není součástí systému ETCS (traťové části), nýbrž systému národního, což vyplývá z obrázku referenční architektury ETCS. Z hlediska své úlohy je LEU velmi podobná RBC, kterážto součástí systému ETCS dle téže architektury je. Úlohou obou je shromáždit, transformovat a zajistit přenos informací ze stávajících ZZ na vozidlo (OBU), aby bylo možno dohlížet jeho bezpečnou jízdu. Navíc potřeba obou (jak RBC, tak LEU) vznikla až s příchodem ETCS, obě představují tzv. konstituenty interoperability dle TSI CCS [**TSI**].*

4.3.2 Identifikace nebezpečí

Při identifikaci nebezpečí souvisejících s analyzovaným systémem je třeba identifikovat pokud možno všechna tato nebezpečí. Aby se tak stalo, respektive aby se zvýšila pravděpodobnost, že se tak stane, je třeba postupovat při procesu identifikace co možná nejsystematičtěji. Můžeme tedy říci, že esenciální požadavek pro identifikaci nebezpečí, jakožto základního podkladu pro následné hodnocení rizik, spočívá v nutnosti zajištění úplnosti seznamu identifikovaných nebezpečí. K této úplnosti samozřejmě přispívá – vedle požadované erudovanosti osob tuto identifikaci provádějících – také systematičnost procesu této identifikace. Pro dosažení systematičnosti tohoto procesu identifikace navrhuji:

I. nejprve identifikovat tzv. základní nebezpečí související s analyzovaným systémem, a to ze znalosti jeho účelu (záměru), jehož stanovení je součástí koncepce systému, tedy první etapy životního cyklu dle [***126-1***];
II. následně identifikovat tzv. ostatní nebezpečí, a to za pomoci oblastí, jež jsou doporučeny pro hledání nebezpečí normou [***126-1***];
III. vždy plně respektovat základní podklad pro identifikaci nebezpečí, což je definice analyzovaného systému a jeho rozhraní, tedy výstup druhé etapy životního cyklu dle [***126-1***].

Základní podklad pro analýzu rizika (přesněji pro identifikaci nebezpečí souvisejících s analyzovaným systémem) tedy bezesporu představuje definice systému, a to včetně definice jeho rozhraní, kterážto podle mého názoru ale není součástí analýzy rizika jako takové, neboť jí předchází – diskuse a odůvodnění pro toto tvrzení je provedena v kapitole 4.1.3. Jak je uvedeno výše, vychází se při hledání ostatních nebezpečí z oblastí, ve kterých se mají nebezpečí související s analyzovaným systémem hledat dle normy [***126-1***]. Tyto oblasti jsou uvedeny v následující tabulce (viz tab. 4.1), v níž jsou rovněž doplněny o mé vlastní komentáře, kterými se snažím upřesnit významy jednotlivých oblastí, které nejsou z normy [***126-1***] dost dobře patrné.

Oblast možných nebezpečí plynoucích z	Komentář
normálního provozu systému	týká se funkční bezpečnosti
nouzového provozu systému	jde o součást funkční bezpečnosti, týká se provozu s určitými omezeními, kdy jsou dostupné jen vybrané funkce (například nouzový provoz staničního zabezpečovacího zařízení při výpadku hlavního napájení)
poruchových stavů systému[11]	týká se technické bezpečnosti

[11] zde je použit nový návrh označení této oblasti – původní označení dle normy [***126-1***] je: „podmínek při poruchových stavech systému“ – navrhuji změnu na: „poruchových stavů systému“

chybného použití systému	týká se buď nedodržení správně stanovených podmínek použití daného systému, nebo jejich chybného stanovení
rozhraní systému	týká se buď obdržení, nebo poskytnutí chybných informací daným systémem
funkčnosti systému	týká se možnosti jednak nežádoucího ovlivňování daného systému sousedními zařízení, jednak nežádoucího ovlivňování sousedních zařízení daným systémem; přičemž toto ovlivňování může být jak logické, tak fyzické
otázek provozu, údržby a podpory systému	týká se provoz daného systému (zde přichází do úvahy kupř. jeho případné opravy), s jeho údržbou a podporou (tj. s konfigurací, diagnostikou apod.)
úvah o likvidaci systému	týká se ekologické likvidace daného systému (tj. činností prováděných po vypnutí a odstavení systému z provozu)
lidského činitele	týká se vliv lidského činitele na vývoj, návrh, projekci, výrobu, montáž, provoz a údržbu daného systému
problémů nemocí z povolání	týká se pouze systémů s definovaným rozhraním pro obsluhu/údržbu
mechanických vlivů prostředí	týká se mechanických vlivů okolí
elektrických vlivů prostředí	týká se elektrických vlivů okolí
klimatických vlivů prostředí[12]	týká se klimatických vlivů okolí

Tab. 4.1 – Komentovaný seznam oblastí pro hledání nebezpečí souvisejících s analyzovaným systémem

Přestože norma [***126-1***] uvádí výše uvedené oblasti, ve kterých je nutno hledat nebezpečí, podle mého názoru mají (při provozu bezpečnostně-kritického řídicího systému, zde konkrétně železničního zabezpečovacího systému) rozhodující význam zejména ta nebezpečí, která vznikají při provozu tohoto systému v jím řízeném procesu, kterým je (v případě želez-

[12] zde je použit nový návrh označení této oblasti – původní označení dle normy [***126-1***] je: „venkovních vlivů prostředí, které zahrnuje např. sníh, záplavy, vichřice, deště, sesuvy půdy atd." – navrhuji změnu na: „klimatických vlivů prostředí"

ničních zabezpečovacích systémů) železniční doprava. Také proto je zpravidla nebezpečí související s provozem železniční dopravy identifikováno jako základní a také proto většina ostatních nebezpečí identifikovaných v oblastech dle [***126-1***] jsou s tímto základním nebezpečím shodná (viz např. ukázku identifikace nebezpečí souvisejících s aplikací systému ETCS v příloze č. 5).

4.3.3 Hodnocení a přijetí rizika

Obecně je třeba před hodnocením rizik železničních zabezpečovacích systémů říci, že s řízením železniční dopravy souvisí – a to nezávisle na použití či nepoužití zabezpečovacích systémů – jistá rizika (vykolejení železničních vozidel, jejich srážka atp.), kterým se snažíme ideálně prostřednictvím technických prostředků (zejména železničních zabezpečovacích systémů) zabránit. Ovšem při selhání zabezpečovacího systému mohou tato rizika nastat. Proto se dle mého názoru vypracovává analýza rizika, aby se ukázalo, selháním které konkrétní části zabezpečovacího systému mohou tato rizika nastat (funkční bezpečnost), a aby se toto jejich nastání snížilo na všeobecně přijatelnou úroveň, a to samozřejmě i při uvažovaných poruchách nasazeného zabezpečovacího systému (technická bezpečnost).

V této kapitole jsou stanovena kritéria pro hodnocení četnosti výskytu nebezpečí, závažnosti jejich následků a rizik z nich plynoucích a nastíněn postup přijetí rizika s ohledem na národní legislativu a statistiku nehodových událostí evidovaných v ČR. Všechny parametry související s hodnocením nebezpečí se pro konkrétní nebezpečí ve zde stanovené metodice analýzy rizika určují v rámci přizpůsobeného formuláře FMECA, jehož návrh je na obr. 5.3. Stanovení vhodného způsobu přiřazování intenzit THR jednotlivým funkcím analyzovaného systému v závislosti na riziku je součástí kapitoly 5.3.4.

<u>Četnost výskytu nebezpečí</u>

Ohodnocení četnosti výskytu nebezpečí navrhuji provádět na základě tabulky uvedené níže (viz tab. 4.2), v níž jsou jednotlivé kategorie četností též numericky odstupňovány. Při stanovování tohoto numerického odstupňování jsem vycházel z těchto předpokladů:

I. Pro stanovení počtu výskytů nebezpečí za hodinu (přesněji pro stanovení intenzity výskytů[13]) se předpokládá, že délka životního cyklu (LC) aplikace systému ETCS je 25 let (5 let na vývoj, 20 let je – stejně jako u všech ostatních elektronických systémů – předpokládaný užitečný život, v tomto konkrétním případě užitečný ži-

[13] Intenzitou zde myslím počet výskytů daného jevu (nebezpečí) za časovou jednotku.

vot traťové části systému ETCS), potom 1 rok = 365 dní, 1 den = 24 h (tj. 1 LC = 2,19.10^5 h = $k_{h \to LC}$).

Pro stanovení počtu výskytů za hodinu se předpokládá použití následujícího vzorce:

$$\lambda = \frac{n}{k_{h \to LC}} \; [h^{-1}], \tag{4.1}$$

kde n je počet výskytů za LC; $k_{h \to LC}$ je převodní koeficient z bodu I.

II. Pro stanovení pravděpodobností výskytů nebezpečí se pro první přiblížení zjednodušeně předpokládá, že četnost výskytu nebezpečí je konstantní, což je ovšem pravda jen pro střední část vanové křivky. Rozdělení pravděpodobností výskytů nebezpečí lze aproximovat exponenciálním rozdělením dle vzorce:

$$p = 1 - e^{\lambda t} \; [-], \tag{4.2}$$

kde λ je počet výskytů nebezpečí za hodinu.

Kategorie četnosti	Popis kategorie dle [***126-1***] (pouze informativně)	Navržený počet (intenzita) výskytů nebezpečí		Vypočítaná pravděpodobnost výskytu nebezpečí
		za LC	za hod.	
Častá	Je pravděpodobný častý výskyt. Nebezpečí je trvalé.	> 1 000x	> 4,57.10^{-3}	> 4,57.10^{-3}
Pravděpodobná	Vyskytnou se několikrát. Lze očekávat, že nebezpečí nastane často.	≤ 1 000x	≤ 4,57.10^{-3}	≤ 4,57.10^{-3}
Občasná	Pravděpodobně se vyskytnou několikrát. Lze očekávat, že nebezpečí nastane několikrát.	≤ 100x	≤ 4,57.10^{-4}	≤ 4,57.10^{-4}
Malá	Pravděpodobně se vyskytnou někdy během životního cyklu systému. Je rozumné předpokládat, že nebezpečí nastane.	≤ 10x	≤ 4,57.10^{-5}	≤ 4,57.10^{-5}
Nepravděpodobná	Výskyt je nepravděpodobný, ale možný. Lze předpokládat, že nebezpečí může výjimečně nastat.	≤ 1x	≤ 4,57.10^{-6}	≤ 4,57.10^{-6}

Vysoce nepravděpodobná	Výskyt je krajně nepravděpodobný. Lze předpokládat, že nebezpečí nemusí nastat.	≤ 0,1x	≤ $4{,}57.10^{-7}$	≤ $4{,}57.10^{-7}$

Tab. 4.2 – Návrh kvantifikace intenzit výskytu nebezpečí

Tabulka výše (viz tab. 4.2) tedy uvádí kategorie četností, jejich počet a numerické odstupňování, které principiálně vychází zejména z interpretace/kvantifikace textového popisu uvedeného v normě [***126-1***] a které by pro úplnost a dosažení co možná nejvyšší míry objektivity hodnocení mělo být pro hodnocení rizik spojených se systémem ETCS odsouhlaseno provozovatelem dráhy [pozn.: provozovatelem dráhy je v podmínkách České republiky na tratích, na nichž se dle národního implementačního plánu [***NIP***] očekává nasazení systému ETCS, tedy v podmínkách dráhy celostátní ve vlastnictví státu, státní organizace SŽDC, s. o. (dále jen SŽDC)].

V souvislosti s touto tabulkou (viz tab. 4.2) je ještě zajímavé upozornit na skutečnost, že pro velmi malé hodnoty četností výskytů nebezpečí za hodinu se tyto co do absolutní hodnoty (při uvažování tří platných číslic a zjednodušujícího předpokladu konstantní intenzity výskytu nebezpečí po celý užitečný život daného systému) shodují s odpovídajícími hodnotami pravděpodobností výskytu daného nebezpečí.

Závažnost následků nebezpečí

Výskyt každého nebezpečí může způsobit nehodu. A právě následky nehod (mimořádných událostí) souvisejících s řízením železniční dopravy se v podmínkách České republiky zabývá předpis SŽDC Dp17 [***Dp17***], o hlášení a šetření mimořádných událostí, který platí pro dráhu celostátní, na níž se dle národního implementačního plánu [***NIP***] očekává aplikace systému ETCS. Tento předpis v oblasti mimořádných událostí blíže specifikuje obecná ustanovení zákona č. 266/1994 Sb., o dráhách, a uvádí mimo jiné definici (kategorizaci) mimořádných událostí. S tímto předpisem též souvisejí metodické návody a postupy, které uvádí prováděcí opatření k tomuto předpisu, označené jako SŽDC Dp17-1 [***Dp17-1***].

Předpis [***Dp17***] rozlišuje následující tři skupiny mimořádných událostí – cituji[14]:

„[...] MU [se] zařazují do skupin podle příčin, následků a okolností jejich vzniku na:

a) ***MU skupiny A***

[14] V uvedené citaci se pro mimořádnou událost používá zkratka „MU“.

***Závažné nehody**, kterými se rozumí srážka [pozn. autora: dle čl. 20 tohoto předpisu se srážkou rozumí též najetí vozidla na překážku na dopravní cestě dráhy] nebo vykolejení drážních vozidel, ke kterým došlo v souvislosti s provozováním drážní dopravy, s následkem smrti či újmy na zdraví nejméně 5 osob nebo škody velkého rozsahu [pozn. autora: dle čl. 18 tohoto předpisu jde o škodu převyšující částku 5 mil. Kč].*

*b) **MU skupiny B***

***Nehody**, kterými se rozumí události, k nimž došlo v souvislosti s provozováním drážní dopravy[,] s následkem smrti, újmy na zdraví nebo značné škody [1. pozn. autora: dle čl. 19 tohoto předpisu jde o škodu převyšující částku 0,5 mil. Kč]. [2. pozn. autora: patrně se myslí, že počet úmrtí, újem na zdraví či škod nepřevyšuje tytéž ukazatele uvedené u MU skupiny A, v opačném případě by tato definice v kontextu předcházející definice byla nejednoznačná; naštěstí v tomto „nepřevyšujícím“ smyslu jsou definice uvedeny v prováděcím opatření k tomuto předpisu]*

*c) **MU skupiny C***

***Ohrožení**, kterými se rozumí jiné mimořádné události, které nejsou závažnou nehodou nebo nehodou [pozn. autora: do této kategorie se dle prováděcího opatření k tomuto předpisu řadí také únik nebezpečné věci při její přepravě, jakož i pouhé ohrožení bezprostředním rizikem tohoto jejího úniku, což koresponduje s posuzováním vlivu na životní prostředí při kategorizaci závažnosti následků nebezpečí dle ČSN EN 50126-1:2007 (viz tab. 1.2)].“*[15]

Z výše uvedených hodnot ukazatelů pro kategorizaci mimořádných událostí vychází níže uvedený návrh kvantifikace závažnosti následků nebezpečí (viz tab. 4.3). Před vlastním stanovením tohoto návrhu bylo ale třeba výše citované informace uvedené v předpisu [***Dp17***], respektive v prováděcím opatření [***Dp17-1***] podrobit menší diskusi:

V kategorizaci nehod uvedené v [***Dp7-1***] (pomineme-li dle mého názoru dosti nejednoznačné definice v předpisu [***Dp17***]) mi vadí, že z definice závažné nehody není zřejmé, k čemu se vztahuje 5 osob při rozlišování mezi jednotlivými skupinami MU. Zda pouze k újmě na zdraví (nejméně 5 zraněných osob), či jak k újmě na zdraví (nejméně 5 zraněných osob), tak k úmrtí (nejméně 5 usmrcených osob); nebo k součtu újem na zdraví i úmrtí (celkem nejméně 5 osob zraněných či usmrcených). V prvním případě by jinými slovy byl jeden usmrcený na úrovni 5 zraněných osob, ovšem není zde jasné, proč v MU skupiny B opět figuruje úmrtí. Ve druhém případě jsou usmrcené a zraněné osoby zvláštně na stejné úrovni a na-

[15] Předpis SŽDC Dp17, s. 26., čl. 146.

víc není jasné, proč v MU skupiny B figuruje úmrtí pouze jedné osoby a ne nejvíce 4 osob. Třetí případ zase značí, že se újma na zdraví (či životu) při závažné nehodě musí celkově týkat více osob. Z výše popsaných možností se kloním k variantě třetí, tedy k tomu, že 5 osob se váže k sumě případných mrtvých či zraněných (tj. 5 a více úmrtí nebo zranění znamená závažnou nehodu /MU skupiny A/; nejvíce 5 zraněných nebo usmrcených osob znamená nehodu /MU skupiny B/).

Kromě výše uvedené nejednoznačnosti, nejsou tyto definice úplné, protože nepokrývají všechny možné MU. Kupříkladu MU, při níž dojde ke zranění 4 osob, anebo ke 4 úmrtím, nelze striktně vzato dle samotného předpisu [***Dp17***] zařadit. Ovšem se zohledněním prováděcího opatření k tomuto předpisu [***Dp17-1***] již tato zařadit lze.

Ohodnocení závažnosti následků nebezpečí pak navrhuji provádět na základě tabulky uvedené níže (viz tab. 4.3). Tato vychází z národní legislativy analyzované výše.

úroveň závažnosti	ztráty v důsledku vzniku nebezpečí		
	na lidských životech	na lidském zdraví	na hmotném majetku
katastrofická	více než *k* úmrtí, přičemž celkový součet úmrtí a zranění (k + l) je rovno nebo vyšší než 5	více než *l* zranění, přičemž celkový součet úmrtí a zranění (l + k) je rovno nebo vyšší než 5	hmotná škoda převyšující částku 5 mil. Kč
kritická	nejvíce *n* úmrtí, přičemž celkový součet úmrtí a zranění (n + m) je menší než 5	nejvíce *m* zranění, přičemž celkový součet úmrtí a zranění (m + n) je menší než 5	hmotná škoda v rozsahu od 0,5 mil. Kč (včetně) do 5 mil. Kč (mimo)
okrajová	žádné	žádné	hmotná škoda v rozsahu od 50 tis. Kč (včetně) do 0,5 mil. Kč (mimo)[16]
nevýznamná	žádné	žádné	hmotná škoda nižší než 50 tis. Kč[16]

Tab. 4.3 – Návrh kvantifikace závažnosti následků nebezpečí

Tabulka výše (viz tab. 4.3) tedy uvádí počet úrovní závažnosti a důsledky pro každou tuto úroveň, které by opět pro úplnost a dosažení co možná nejvyšší míry objektivity hodnocení měly být pro hodnocení rizik spojených se systémem ETCS odsouhlaseny provozovatelem dráhy. Toto by však podle mého názoru u státní organizace SŽDC neměl být problém,

[16] Jako určující hranici hmotné škody mezi kategoriemi „nevýznamná“ a „okrajová“ jsem stanovil hodnotu 50 000,- Kč, což je dle zákona č. 140/1961 Sb., trestního zákona, hranice větší škody.

neboť ukazatele jednotlivých úrovní závažnosti v této tabulce vychází z kategorizace mimořádných událostí na závažné nehody, nehody a ohrožení, tak jak je uvádí zákon č. 266/1994 Sb., o dráhách, a rozšiřuje a doplňuje je předpis SŽDC Dp17 [***Dp17***] a jeho prováděcí opatření, označené jako SŽDC Dp17-1 [***Dp17-1***]. Z tohoto důvodu také neobsahuje ukazatele týkající se ohrožení či poškození životního prostředí, což naopak uvažuje například norma [***126-1***], neboť ty naše současná národní legislativa explicitně neuvádí. Uvádí je pouze implicitně jako součást kategorie ohrožení (popř. též ostatních kategorií, u nichž se ovšem rozhodující ukazatele týkají pouze osob a hmotného majetku).

*Poznámka: Zajímavé také je, že dle předpisu [**Dp17**] se újma na zdraví, popřípadě úmrtí osoby v obvodu dráhy, která není způsobena pohybem drážního vozidla, jako mimořádná událost neeviduje. Toto dle mého názoru jen potvrzuje mou hypotézu vyslovenou výše (viz kap. 4.3.2), a to, že rozhodující nebezpečí jsou ta nebezpečí, která přímo souvisejí s provozem železniční dopravy. Tedy nikoli úvahy o likvidaci systému, nemocí z povolání apod. Těmito oblastmi nebezpečí doporučuji zabývat se z hlediska úplnosti pouze okrajově.*

Ohodnocení rizika plynoucího z nebezpečí

Ohodnocením rizika je zde myšleno přiřazení jedné z kategorií rizika, s níž je dle tab. 4.4 spojena definovaná přijatelnost, každé úrovni rizika, která je dána kombinací četnosti a následků hodnoceného nebezpečí.

kategorie rizika	přijatelnost
nepřípustné	riziko je nepřijatelné, musí být odstraněno
nežádoucí	riziko je přijatelné pouze tehdy, jestliže je jeho snížení prakticky nedosažitelné a jestliže s ním souhlasí provozovatel dráhy nebo řídicí orgán pro otázky bezpečnosti
přípustné	riziko je přijatelné při přiměřené kontrole a se souhlasem provozovatele dráhy
zanedbatelné	riziko je přijatelné bez souhlasu provozovatele dráhy

Tab. 4.4 – Návrh stanovení přijatelnosti jednotlivých kategorií, resp. úrovní rizik

V souvislosti s touto tabulkou (tab. 4.4) bych si dovolil jednu poznámku k popisu kategorie rizika „nežádoucí“: Zde je uvedeno, že s přijatelností rizika musí souhlasit provozovatel dráhy nebo řídicí orgán pro otázky bezpečnosti. Čili v podmínkách ČR je přijatelné, jestliže souhlasí, jde-li o dráhu celostátní, státní organizace SŽDC (provozovatel dráhy) nebo Drážní úřad (řídicí orgán pro otázky bezpečnosti). Použití spojky „nebo“ byť vychází z normy [***126-***

-1] je zde z formálního hlediska nevhodné, neboť dává při výkladu tohoto požadavku možnost volby, zda je postačující, aby alespoň jeden z nich souhlasil, nebo zda musí souhlasit oba, což působí jistý – dle mého názoru v tomto případě nežádoucí – stupeň volnosti.

Vzhledem k tomu, že s kategorií rizika úzce souvisí i přijatelnost tohoto rizika, je zřejmé, že ohodnocení rizika musí být založeno na kritériích přijatelnosti rizika, o nichž pojednává následující oddíl tohoto textu.

Kritéria přijatelnosti rizika

Kritérium přijatelnosti rizika slouží pro přiřazení určité kategorie rizika, s níž je spojena přijatelnost rizika (viz např. tab. 4.4), určité úrovni rizika, jež je dána kombinací četnosti výskytu a následků nebezpečí. Při stanovování těchto kritérií (pravidel) se nabízí vyjít ze současného stavu, tedy ze statistik nehodových (mimořádných) událostí. Šetřením příčin a okolností vzniku mimořádných událostí souvisejících s řízením železniční dopravy a evidencí výše zmíněných následků těchto událostí se v České republice zabývá na provozovatelích dráhy a drážní dopravy nezávislý národní orgán – Drážní inspekce. Ta také vede statistiky šetřených mimořádných událostí, čehož je následně v této práci využito pro stanovení kritérií přijatelnosti rizik.

Jako správní úřad vznikla Drážní inspekce ustanovením zákona č. 77/2002 Sb., o akciové společnosti České dráhy, státní organizaci Správa železniční dopravní cesty, 1. ledna 2003 a svou činnost zahájila okamžitě. [***WDI***] Při znalosti tohoto se nabízelo pokusit se při návrhu kritérií přijatelnosti rizik využít údajů z její databáze mimořádných událostí z posledních několika let. Ideálně z posledních ucelených 10 let (tj. od začátku její činnosti, tedy od roku 2003 do konce roku 2012). Původně byl záměr uvažovat i škody na životním prostředí v souladu s kategorizací následků uvedenou v normě [***126-1***] – poškození, ohrožení. Ovšem tyto ukazatele se ve zmíněné databázi nevyskytují, což je patrně dáno tím, že ani národní legislativa je přímo neuvádí (viz předchozí odstavec o závažnosti následků).

Drážní inspekce na základě zaslané žádosti poskytla údaje o mimořádných událostech od začátku roku 2008 do listopadu 2013 (viz přílohu č. 1). Uvážíme-li z těchto údajů pouze údaje týkající se období do konce roku 2012, můžeme hovořit o posledních pěti letech, které jsou ucelené a které současně představují čtvrtinu užitečného života železničního zabezpečovacího zařízení. Z těchto údajů byly postupem zachyceným v příloze č. 2 získány (po aproximaci na celý předpokládaný užitečný život elektronického železničního zabezpečovacího zařízení, během níž se mohou uvažovaná provozní rizika projevit a která činí 20 let) následující souhrnné údaje pro jednotlivé druhy (kategorie) mimořádných událostí – viz tab. 4.5.

Počet mimořádných událostí	Závažná nehoda	Nehoda	Ohrožení	
			O1	O2
V období za posledních ucelených 5 let (tj. od 1. 1. 2008 do 31. 12. 2012)	18	102	455	2 144
Po aproximaci na celý užitečný život ZZ (předpokládaných 20 let)	**72**	**408**	**1 820**	**8 576**

Tab. 4.5 – Počet mimořádných událostí jednotlivých kategorií za dané období

Pro získání údajů v tab. 4.5 bylo analyzováno a kategorizováno bezmála osm tisíc[17] mimořádných událostí evidovaných v drážní dopravě za posledních pět let (viz přílohy č. 1 až 3). Toto období považuji za mnohem vhodnější, než tvořit statistiku z údajů z posledních dvaceti let, což je obvyklá doba života elektronického železničního zabezpečovacího systému. Posledních ucelených pět let a následná aproximace na předpokládanou dobu života je dle mého názoru totiž reprezentativnější, neboť mnohem lépe vystihuje současný železniční provoz. Z těchto mimořádných událostí jsem dále uvažoval pouze železniční a takové, které lze eliminovat použitím evropského vlakového zabezpečovacího systému ETCS v součinnosti s klasickými zabezpečovacími zařízeními 3. kategorie dle TNŽ 34 2620 [***20***] (tj. srážka drážních vozidel, nedovolené projetí návěstidla zakazujícího další jízdu, vykolejení a některé ostatní). Neuvažoval jsem tudíž střety drážních vozidel se silničními vozidly, střety s osobou, požáry drážních vozidel a další zabezpečovacími systémy neovlivnitelné události.

Ohodnocení úrovní rizik plynoucích z nebezpečí navrhuji provádět v podmínkách se zohledněním národní legislativy a statistiky mimořádných (nehodových) událostí evidovaných Drážní inspekcí na základě tab. 4.6, která tedy v konečném důsledku uvádí stanovení přijatelnosti rizik jednotlivým úrovním rizika, která jsou dána kombinací četnosti a následků ohodnocovaného nebezpečí. Děje se tak na základě kritéria přijatelnosti rizika, které vychází ze zásady GAMAB („celkově nejméně tak dobré“) uvedené v normě [***126-1***] (též zde v kap. 1.2.1) a ze statistiky mimořádných událostí evidovaných na území ČR. Při stanovování přijatelnosti rizik zachycené v tab. 4.6 jsem vycházel z následující úvahy.

Máme-li respektovat výše zmíněnou zásadu GAMAB, pak počet nehodových událostí s danými následky představuje nepřípustný stav, který musíme aplikací nových zabezpečovacích systémů snížit. Z toho důvodu byla těmto kombinacím přiřazena kategorie „Nepřípustná“, což dle tab. 4.4 znamená, že tato rizika nejsou přijatelná a je nutno je v každém případě odstranit. Tutéž kategorii jsem přiřadil také všem úrovním rizik nad touto hranicí. Úrovním rizik v pásmu jedné kategorie četností pod touto úrovní jsem přiřadil kategorii „Nežádoucí“,

[17] Přesné číslo je 7 939 MU.

což dle tab. 4.4 znamená, že tato rizika téměř nejsou přijatelná. Úrovním rizik v pásmu dvou kategorií četností od kategorie rizika „Nežádoucí“ jsem přiřadil kategorii „Přípustná“, značící, že riziko lze přijmout při přiměřené kontrole a vždy se souhlasem provozovatele dráhy. Ostatní úrovně rizika mají kategorii rizika dle tab. 4.4 „Zanedbatelná“. Stejně jako všechny ostatní tabulky v této kapitole, které slouží pro návrh hodnocení rizika, i tato tabulka (tab. 4.6), stanovující přijatelnost jednotlivých úrovní rizik, by opět pro úplnost a dosažení co možná nejvyšší míry objektivity hodnocení měla být pro hodnocení rizik spojených se systémem ETCS odsouhlasena provozovatelem dráhy.

Výskyt\závažnost	Nevýznamné (Ohrož. O2)	Okrajové (Ohrož. O1)	Kritické (Nehoda)	Katastrofické (Závaž. neh.)
Častá více než 1 000 (> 1 000)	Nepřípustné	Nepřípustné	Nepřípustné	Nepřípustné
Pravděpodobná 100 až 1 000 (≤ 1 000)	Nežádoucí	Nežádoucí	Nepřípustné	Nepřípustné
Občasná 10 až 100 (≤ 100)	Přípustné	Přípustné	Nežádoucí	Nepřípustné
Malá 1 až 10 (≤ 10)	Přípustné	Přípustné	Přípustné	Nežádoucí
Nepravděpodobná 0,1 až 1 (≤ 1)	Zanedbatelné	Zanedbatelné	Přípustné	Přípustné
Vysoce nepravděpodobná (≤ 0,1)	Zanedbatelné	Zanedbatelné	Zanedbatelné	Přípustné
Počet MU dané kategorie	8 576	1 820	408	72
Kritérium přijatelnosti rizika (RAC) [h^{-1}]	10^{-6}	10^{-6}	10^{-7}	10^{-8}

Tab. 4.6 – Návrh přiřazení kategorií rizik jednotlivým úrovním rizik a stanovení RAC

Uvážíme-li dále, že rizika kategorie „Zanedbatelná“ je dle tab. 4.4 možno přijmout bez souhlasu provozovatele dráhy [pozn. tuto možnost připouští norma [***126-1***]], lze hranici mezi přípustným a zanedbatelným rizikem (viz její zvýraznění v tab. 4.6) považovat za mez přijatelnosti rizika a na základě tohoto principu pro každou kategorii závažnosti zkoumaného nebezpečí odvodit z charakteristik příslušných kategorií četností výskytů (viz tab. 4.2) kritérium přijatelnosti rizika RAC (Risk Acceptance Criterium). Výsledek tohoto procesu zachycuje poslední řádek v tab. 4.6. Takto získaná kritéria navrhuji používat pro vrcholová nebezpečí identifikovaná dle kapitoly 4.3.2.

Zajímavé je také porovnání těchto kritérií RAC odvozených pro jednotlivé kategorie závažnosti s obdobnými kritérii RAC, která byla stanovena Evropskou železniční agenturou ERA a která jsou používána pracovní skupinou UNISIG RAMS WP (viz např. [***ADSA***]). Toto porovnání zachycuje následující tabulka (viz tab. 4.7).

ID	Úroveň závažnosti	Následky pro cestujícího	RAC dle ERA	RAC dle tab. 4.6
S1	Nevýznamná	Možné lehké zranění	10^{-5}	10^{-6}
S2	Okrajová	Lehké zranění	10^{-5}	10^{-6}
S3	Kritická	Jednotlivé těžké zranění	10^{-7}	10^{-7}
S4	Katastrofická	Jednotlivé úmrtí a/nebo mnohočetná zranění	10^{-9}	10^{-8}

Tab. 4.7 – Porovnání kritérií přijatelnosti rizik RAC

Porovnáním kritérií RAC stanovených agenturou ERA a touto disertační prací (viz tab. 4.7) zjistíme [pozn. slovní popis závažností jsem ponechal, tak jak je uveden agenturou ERA[18]], že obě kritéria RAC mají obdobnou stoupající tendenci. Skutečnost, že se pro úroveň katastrofickou obě tato kritéria liší o řád, lze vysvětlit kupříkladu tak, že agentura ERA vzala pro jejich stanovení jinou (bezpečnější) referenční železnici, anebo tak, že vyšla ze společných bezpečnostních metod (CSM), které požadují u katastrofických následků prokázat plnění hodnoty intenzity výskytu maximálně do mezní hodnoty 10^{-9} h^{-1}. Pokud je tento kvantitativní cíl bezpečnosti nižší (přísnější) než tato mezní hodnota, není třeba jej dle CSM dále rozvíjet, tedy není třeba dále snižovat s ním související riziko (viz článek 2.5.4 směrnice 2013/402/EC [***402***]). Tyto dvě možnosti odůvodnění jsou ale pouze spekulacemi, neboť mi není znám způsob, na jehož základě byla tato RAC agenturou ERA stanovena.

4.3.4 Stanovení nápravných opatření

Nápravným opatřením se v kontextu řízení rizik myslí opatření, jímž se riziko snižuje na přijatelnou úroveň. Z pohledu zde navržené metodiky analýzy rizika, resp. řízení rizik železničních zabezpečovacích systémů je za nápravné opatření považováno:

[18] V této souvislosti bych si dovolil upozornit, že jednotlivé úrovně závažnosti jsou dle mého názoru definovány dosti zvláštně a navíc jsou definovány pouze pro jednoho cestujícího, nikoli pro cestující v množném čísle, což bych při této kategorizaci očekával.

I. opatření, které může mít formu stanovení tolerovatelné intenzity nebezpečí (THR), potažmo úrovně integrity bezpečnosti (SIL), potažmo bezpečnostního požadavku (SR), což se ve zde navržené metodice děje v rámci analýzy rizika;
II. opatření, které může mít v principu charakter administrativní nebo technický, což se ve zde navržené metodice děje v rámci záznamu o nebezpečí.

Kromě stanovení nápravného opatření je nutno taktéž zajistit, že nápravné opatření bude během životního cyklu daného systému zapracováno. K tomuto účelu je nutno ustanovit proces, který toto zajistí. Jako vhodný okamžik pro ustanovení tohoto procesu se mi jeví první nebo druhá etapa životního cyklu dle [***126-1***]. V rámci tohoto procesu doporučuji předepsat nutnost stanovit konkrétní odpovědnosti za provedení nápravného opatření již při jeho odvozování. Tedy stanovit odpovědnosti, včetně odpovědností za zajištění jeho implementace a provedení následného nového hodnocení rizika, které proběhne až po zapracování daného nápravného opatření.

Nápravná opatření můžeme kategorizovat následujícím způsobem. Každé nápravné opatření může být principiálně dvojího druhu. Nápravné opatření interní (například požadovaná modifikace funkčního chování analyzovaného technického systému), nápravné opatření externí (pravidlo – provozní, projekční apod.). Kromě toho u systému ETCS může navíc být každé nápravné opatření:

I. harmonizované – takové, které je součást evropských generických specifikací systému ETCS (viz definice systému ETCS v kap. 4.3.1);
II. neharmonizované – takové, které je až součást národních specifikací určité specifické aplikace systému ETCS (viz opět kap. 4.3.1).

Harmonizovaná nápravná opatření jak interní, tak externí, platná pro systém ETCS je potom možno nalézt v UNISIG Hazard Logu [***UHL***], popřípadě ve veřejné zprávě z tohoto Hazard Logu [***SS113***]. Další množinu harmonizovaných nápravných opatření pro systém ETCS je možno ve formě bezpečnostních požadavků nalézt v Subsetu-091 [***SS091***], zachycujícím bezpečnostní požadavky na tento systém. Jak vidno z předchozího, nápravná opatření představují de facto bezpečnostní požadavky na vyvíjený anebo již provozovaný systém nebo na jeho okolí /v tomto případě ve formě tzv. exportovaných[19] podmínek, což jsou požadavky

[19] někdy též aplikačních

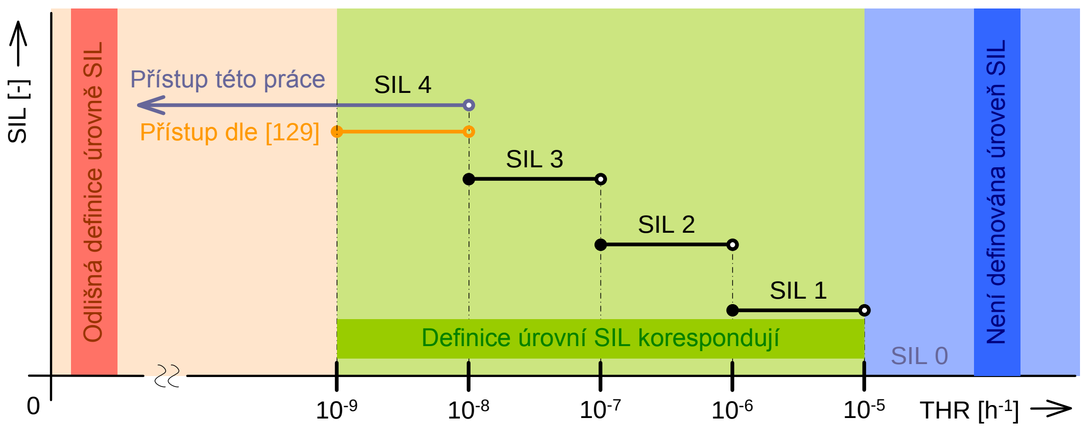
jednoho systému na systém jiný/. A právě o odvozování bezpečnostních požadavků na národní, neharmonizované úrovni pojednává následující kapitola (viz kap. 4.3.5).

4.3.5 Odvození bezpečnostních požadavků

Zde je třeba navázat na teprve níže popsané dělení tolerovatelných intenzit nebezpečí THR, tak jak je to navrženo v kapitole 5.3.4. Máme-li tedy k dispozici na základě ohodnocení rizik plynoucích z identifikovaných nebezpečí a dělení intenzit THR vrcholových událostí stromů FTA odvozeny intenzity THR jednotlivých základních událostí těchto stromů FTA, reprezentující zpravidla funkce analyzovaného systému. Je třeba stanovit proces, který zajistí, že se do příslušných požadavkových dokumentů přenesou jak tyto hodnoty intenzit THR pro jednotlivé funkce systému (reprezentující kvantitativní cíle bezpečnosti pro jednotlivé funkce systému), tak i od nich odvozené úrovně SIL (reprezentující kvantitativní cíle bezpečnosti pro jednotlivé funkce systému).

Úrovně SIL pro jednotlivé funkce, jejichž nejsnazší odvození je možno provést dle tabulky A.1 normy [***129***], které zachycuje obrázek na následující stránce (viz obr. 4.4), jsou důležité z toho důvodu, že na jejich základě se stanovují metody, které je třeba použít. Jejich použití (zejména ve smyslu řízení, a tedy i zajištění jakosti, potažmo bezpečnosti vyvíjeného systému) je vyžadováno jak dle téže normy při následném návrhu elektronického zabezpečovacího systému, tak dle normy [***128***] při návrhu bezpečného softwarového vybavení jakéhokoli počítačově-orientovaného zabezpečovacího systému, aby se adekvátně minimalizovalo riziko vložení systematických poruch do tohoto systému v rámci jeho vývoje.

Obrázek níže (viz obr. 4.4) zachycuje vazbu mezi úrovněmi SIL a intenzitami THR. Jinými slovy, zachycuje vztah mezi kvalitativními požadavky (SIL) a kvantitativními požadavky (THR) na jednotlivé funkce daného bezpečnostně-kritického systému.



Obr. 4.4 - Návrh (zkompletování) vztahu mezi intenzitami THR a úrovněmi SIL

Výše zmíněné dělení bezpečnostních požadavků na kvalitativní a kvantitativní umožňuje jejich částečné oddělení v oblastech, kde to dle obr. 4.4 dle normy [***129***] není definováno, tj. pro THR větší než nebo rovné 10^{-5} h^{-1}, respektive menší než 10^{-9} h^{-1}. Skutečnost, že se tato norma vůbec nezmiňuje o hodnotách THR větších než nebo rovných 10^{-5} h^{-1}, si lze – například v souladu s v této normě několikrát zopakovaným ustanovením, že „požadavky nevztahující se k bezpečnosti [pozn. tedy s úrovní SIL 0] jsou mimo rozsah platnosti této normy pro bezpečnost“ – vysvětlovat tak, že se nejedná o bezpečnostně-relevantní úroveň, tedy že se jedná o úroveň SIL 0. Norma [***129***] se však naopak snaží ošetřit hodnoty THR menší než 10^{-9} h^{-1}, u nichž navíc oproti splnění požadavků na SIL 4 [pozn. myšleno použití pro tuto úroveň definovaných adekvátních opatření a metod] dále požaduje – cituji:

„S funkcí, která má kvantitativní požadavky náročnější než 10^{-9} h^{-1}, je nutné zacházet jedním z následujících způsobů:

- *pokud je možné rozdělit funkci na funkčně nezávislé subfunkce, musí být THR mezi tyto subfunkce rozdělena a ke každé subfunkci přiřazena SIL;*
- *pokud nemůže být funkce rozdělena, musí být minimálně splněna opatření a metody požadované pro SIL 4 a funkce musí být použita v kombinaci s jinými technickými nebo provozními opatřeními, aby se dosáhlo nutné THR.“*[20]

S výše citovaným ošetřením hodnot THR menších než 10^{-9} h^{-1} bych si dovolil polemizovat. V této citaci nesdílím stejný názor na skutečnost, že by rozdělením funkce na funkčně nezávislé subfunkce došlo ke zvýšení /zmírnění/ hodnoty THR (první odrážka). Naopak jsem v souladu s dělením THR popsaném v kapitole 5.3.4 přesvědčen o tom, že rozdělením jedné funkce na více nezávislých subfunkcí dojde k dalšímu rozdělení THR, což následně způsobí pouze další snížení /zpřísnění/ této hodnoty.

Další výše citovaná odrážka požaduje pro případ, že daná funkce nemůže být rozdělena na subfunkce [pozn. myšleno, tak aby pro tyto subfunkce hodnota THR nepřevyšovala hodnotu 10^{-9} h^{-1}], což dle mého názoru nemůže být nikdy, aby byly splněny minimálně požadavky na SIL 4 a aby se použila další opatření. Dalším opatřením, které se celkem běžně používá světovými výrobci železničních zabezpečovacích systémů [pozn. což se projevuje např. při diskusích v pracovní skupině sdružení těchto výrobců UNISIG] a ke kterému se zde

[20] Norma ČSN EN 50129, příloha A, s. 47.

taktéž kloním, může být v této oblasti striktní dělení bezpečnostních požadavků na požadavky stanovující kvalitativní cíle bezpečnosti (SIL) a kvantitativní cíle bezpečnosti (THR).

Tento přístup umožňuje kupříkladu stanovení požadavku na SIL 4 spolu s požadavkem na THR = 10^{-11} h^{-1} pro jednu a tutéž funkci. Nadto je dle CSM, jejichž použití je dle směrnice o interoperabilitě [***57***] pro systém ETCS povinné, v některých případech (viz § 2.5.4 nařízení komise 2013/402/EC, o CSM, nahrazující původní nařízení 2009/352/EC) při požadavku na THR menší než 10^{-9} h^{-1} postačující prokázat, že dosažená hodnota THR je rovna právě této hodnotě, tedy 10^{-9} h^{-1}. Prokazování přísnější hodnoty není dle CSM nutno.

4.3.6 Ošetření nebezpečí identifikovaných mimo analýzu rizika

Je zřejmé, že obecně u každého bezpečnostně-kritického systému je nutno nebezpečí související s tímto systémem hledat v každé etapě jeho životního cyklu. Tedy nejen v rámci analýzy rizika, která je pro toto hledání přímo určena, ale také před i po jejím vykonání. Každé identifikované nebezpečí je třeba řídit a tento proces dokumentovat. O komplexním pohledu na řízení rizik plynoucích z identifikovaných nebezpečí pojednávají následující tři kapitoly (postupně kap. 4.4, kap. 4.5 a kap. 4.6).

4.4 Řízení rizik objevených v rámci analýzy rizika

Řízením rizik železničních zabezpečovacích systémů prostřednictvím analýzy rizika se zabývá větší část této práce. Ovšem jak je mimo jiné patrno z obrázku z kapitoly 4.6 (viz obr. 4.5), popisující komplexní pohled na řízení rizik těchto systémů, týká se tento způsob řízení rizik jen jedné konkrétní etapy životního cyklu, tak jak jej definuje norma [***126-1***]. Konkrétně jde o třetí etapu životního cyklu, tedy etapu velmi brzkou v rámci vývoje daného systému, kdy je pouze známa koncepce daného systému, jeho definice a podmínky použití. To je také důvod, proč se může analýza prováděná v tomto období zdát z určitého pohledu povrchní.

Ovšem, jak již bylo napsáno výše, rizika je třeba řídit během celého životního cyklu daného bezpečnostně-kritického systému. Tedy jak před třetí etapou, tak v etapách následných. Kdykoli je identifikováno nebezpečí související se systémem, je třeba riziko z něj plynoucí řídit. Jejich řízení v rámci analýzy rizika se věnuje celá tato práce, kromě kapitol 4.5 a 4.6, které se věnují jejich řízení také mimo tuto analýzu.

4.5 Řízení rizik objevených mimo analýzu rizika

V principu mohou nastat dva případy, kdy je riziko objeveno bez přímé vazby na analýzu rizika bezpečnostně-kritického systému:

I. riziko je objeveno ještě před vykonáním analýzy rizika, popřípadě během jejího vykonávání, tedy v první, druhé, popř. třetí etapě životního cyklu dle [***126-1***];
II. riziko je objeveno, když již analýza rizika byla dokončena, tedy v etapě čtvrté, páté nebo následné životního cyklu dle [***126-1***].

Pokud je nebezpečí nalezeno ještě před vykonáním analýzy rizika, popřípadě během jejího vykonávání, navrhuji riziko z něj plynoucí řídit prostřednictvím tzv. předzáznamů o nebezpečí (viz kap. 4.5.1). S každým takovým předzáznamem je seznámena osoba / skupina osob vykonávající analýzu rizika, takže mají možnost, je-li to vhodné, nebezpečí z předzáznamů zohlednit přímo při jejím vykonávání. Po vykonání analýzy rizika je třeba každý předzáznam posoudit, zda došlo k jeho zapracování v rámci analýzy rizika či nikoli. Pakliže došlo k jeho zapracování, je třeba o tom do patřičného pole předzáznamu o nebezpečí – viz návrh jeho šablony v tab. 4.8 – pořídit záznam a dále není nutno toto nebezpečí de facto celý předzáznam popisující toto nebezpečí v projektu uvažovat. V opačném případě (nebezpečí z předzáznamu nebylo zapracováno) je třeba, aby se z tohoto předzánamu o nebezpečí stal regulérní záznam o nebezpečí a došlo k řízení rizika mimo analýzu rizika.

Pokud je nebezpečí nalezeno po již vykonané analýze rizika, některé zdroje uvádějí, že se má analýza rizika znovu zopakovat (viz např. [***126-1***]). Osobně doporučuji řešit takové nebezpečí prostřednictvím záznamu o nebezpečí, jehož návrh šablony je v kapitole 4.5.2, neboť znalost systému po funkční, implementační i technické stránce a ostatních souvislostí je často nesrovnatelně mnohem dále, než byla v době vykonávání analýzy rizika. To by následně mohlo vést k radikálnímu přepracovávání analýzy rizika, což obvykle není cílem. Cílem je primárně vyřešit právě identifikované nebezpečí tím, že veškerou snahu vkládáme do nalezení vhodných nápravných opatření, aby došlo buď k jeho úplné eliminaci, či alespoň k jeho snížení na přijatelnou úroveň.

4.5.1 Návrh struktury předzáznamu o nebezpečí

Předzáznam o nebezpečí je zcela nový pojem, zavedený pro účely řízení rizika bezpečnostně-kritických systémů poprvé až v této disertační práci. Předzáznam, jak plyne z úvodu této kapitoly (viz kap. 4.5), vzniká, je-li identifikováno nebezpečí v etapě koncepce, definice systému a podmínek použití, či přímo v etapě analýzy rizika, avšak svým charakterem jej není vhodné přímo začlenit do právě vznikající analýzy rizika. Navrhuji, aby strukturou vycházel z klasického záznamu o nebezpečí, například tak jak je navržen v následující podkapitole (viz tab. 4.10), ovšem obsahoval jen označení, název, stručnou charakteristiku, odpovědnosti a navíc způsob uzavření, tak jak to uvádí tabulka níže (viz tab. 4.8).

Předzáznam o nebezpečí	*«Uvede se označení ve formátu: prHčččč, např. prH0024»*
Název nebezpečí	*«Uvede se název, stručně a výstižně charakterizující dané nebezpečí»*
Charakteristika nebezpečí	*«Uvede se bližší popis daného nebezpečí, umožňující posouzení, zda je třeba zakládat o tomto nebezpečí záznam, nebo zda bylo riziko plynoucí z tohoto nebezpečí ošetřeno v rámci analýzy rizika, což předpokládá, že před tímto posouzení již byla vykonána analýza rizika.* *Případně se též zde uvede vazba na jiný zdroj, ze kterého je popisované nebezpečí patrné, např. na konkrétní nebezpečí v UNISIG Hazard Logu [**UHL**]»*
Odpovědnosti	*«Uvedou se údaje, kdo nebezpečí identifikoval, kdo a do kdy provede uzavření daného předzáznamu o nebezpečí»*
Způsob uzavření	*«Uvede se, jakým způsobem byl daný předzáznam o nebezpečí uzavřen. Vždy s jednoznačným a přesným odkazem, prostřednictvím čeho je riziko plynoucí z daného nebezpečí řízeno – např. „Uzavřeno vytvořením záznamu o nebezpečí H0034.“, „Uzavřeno vytvořením události CH_{O515} v analýze rizika»*

Tab. 4.8 – Návrh šablony záznamu o nebezpečí

4.5.2 Návrh struktury záznamu o nebezpečí

Pojem záznam o nebezpečí je narozdíl od předzáznamu o nebezpečí běžně užívaný pojem v oblasti řízení rizik. Existují na něj v evropských normativech požadavky, a to zejména v [***126-1***] a [***129***]. Jeden z těchto požadavků stanovuje vypracování záznamů o nebezpečí i v rámci analýzy rizika, což při použití metodiky zde stanovené nepovažuji za nutné, neboť se domnívám, že jde pouze o způsob zajištění dokumentace v rámci analýzy rizika identifikovaných nebezpečí. To ovšem při dodržení zásad zde stanovené metodiky analýzy rizika je automaticky splněno, tudíž žádná další dokumentace není třeba. Další požadavky jsou dle [***126-1***] na položky, které musí záznamy o nebezpečí obsahovat. Jsou okomentovány v následující tabulce (viz tab. 4.9).

Požadovaná položka dle [*126-1*]	Komentář
cíl a účel záznamů o nebezpečí	dle mého názoru **není nutno**, aby bylo součástí každého záznamu o nebezpečí, tedy šablony pro záznamy o nebezpečí; doporučuji stanovit globálně, podobně jako je tomu např. výše v této kapitole (kap. 4.5)
všechny nebezpečné jevy a k nim přispívající složky	ideálně by mělo být **součástí popisu nebezpečí**, naleznou-li se všechny
pravděpodobné důsledky a četnosti sledu jevů spojených s každým nebezpečím	mělo by být **součástí hodnocení rizika**
riziko každého nebezpečí	mělo by být **součástí hodnocení rizika**
kritéria přípustnosti rizika pro zařízení	doporučuji stanovit globálně, podobně jako je tomu např. v kapitole 4.3.3
opatření učiněná pro snížení rizik na přípustnou úroveň nebo pro jejich odstranění pro každý nebezpečný jev	mělo by být **součástí nápravných opatření**
proces[21] přezkoumání účinnosti opatření ke snížení rizika	mělo by být **součástí následného hodnocení rizika**
proces[21] přezkoumání přípustnosti rizika	mělo by být **součástí následného hodnocení rizika**
proces[21] průběžného zaznamenávání rizik a nehod	mělo by být výsledkem záznamů o nebezpečí nebo analýzy rizika, tak jak je to popsáno např. v kap. 4.6 [pozn. v této kapitole je stanoven pouze proces průběžného zaznamenávání rizik; zaznamenáváním nehod (mimořádných událostí) je mimo jiného v podmínkách ČR pověřena Drážní inspekce, jakožto státní nezávislý vyšetřovací orgán]
proces[21] řízení záznamů o nebezpečí	doporučuji stanovit globálně, jako je tomu například částečně v této kapitole (kap. 4.5), částečně v kapitole následující (kap. 4.6)

[21] Procesy doporučuji popsat například v plánu bezpečnosti, který má dle [*126-1*] vzniknout ve druhé etapě životního cyklu daného systému. Mé komentáře se v této tabulce týkají pouze výsledků těchto procesů.

mezní hodnoty všech provedených analýz	je-li součástí popisu nebezpečí analýza, mělo by být **součástí popisu nebezpečí**
všechny předpoklady učiněné během analýzy	je-li součástí popisu nebezpečí analýza, mělo by být **součástí popisu nebezpečí**
všechny konfidenční meze platné pro data použitá při analýze	je-li součástí popisu nebezpečí analýza, mělo by být **součástí popisu nebezpečí**
použité metody, nástroje a techniky	je-li součástí popisu nebezpečí analýza, mělo by být **součástí popisu nebezpečí** [pozn. předpokládám, že jde o metody, nástroje a techniky použité k analýze – z textu normy [***126-1***] toto není zřejmé]
pracovníci podílející se na procesu a jejich kompetence	mělo by být **součástí odpovědností (za řízení rizika)**

Tab. 4.9 – Komentovaný seznam položek záznamů o nebezpečí

Dále uvádím návrh šablony pro záznamy o nebezpečí, který reflektuje mé dosavadní znalosti a zkušenosti a samozřejmě též požadavky dle tab. 4.9, doplněné o komentáře, z nichž jsou již patrné jednotlivé položky šablony záznamu o nebezpečí. Návrh této šablony je součástí následující tabulky (viz tab. 4.10).

Záznam o nebezpečí	*«Uvede se označení ve formátu: Hčččč, např. H0010»*
Název nebezpečí	*«Uvede se název, stručně a výstižně charakterizující dané nebezpečí»*
Popis nebezpečí	*«Uvede se bližší, detailní popis daného nebezpečí, umožňující jeho hodnocení z hlediska rizika, tj. včetně (pokud možno) všech k danému nebezpečí přispívajících složek [příčin].* *Je-li součástí popisu nebezpečí také analýza, uvedou se zde rovněž všechny uvažované předpoklady, použité mezní hodnoty, konfidenční meze atp.»*
Hodnocení rizika	*«Uvede se hodnocení nebezpečí z hlediska jeho četnosti výskytu, následků a rizika»*
Nápravná opatření	*«Uvedou se nápravná opatření zcela eliminující, či alespoň dostatečně snižující riziko plynoucí z daného nebezpečí»*
Odpovědnosti	*«Uvedou se údaje, kdo nebezpečí identifikoval, kdo jej hodnotil z hlediska rizika, kdo a do kdy provede implementaci nápravných opatření [pozn. zde uvedená osoba nemusí být nutně zaměstnancem právnické osoby vykonávající analýzu rizika – kupř. dodavatel systému vs. uživatel tohoto systému]»*

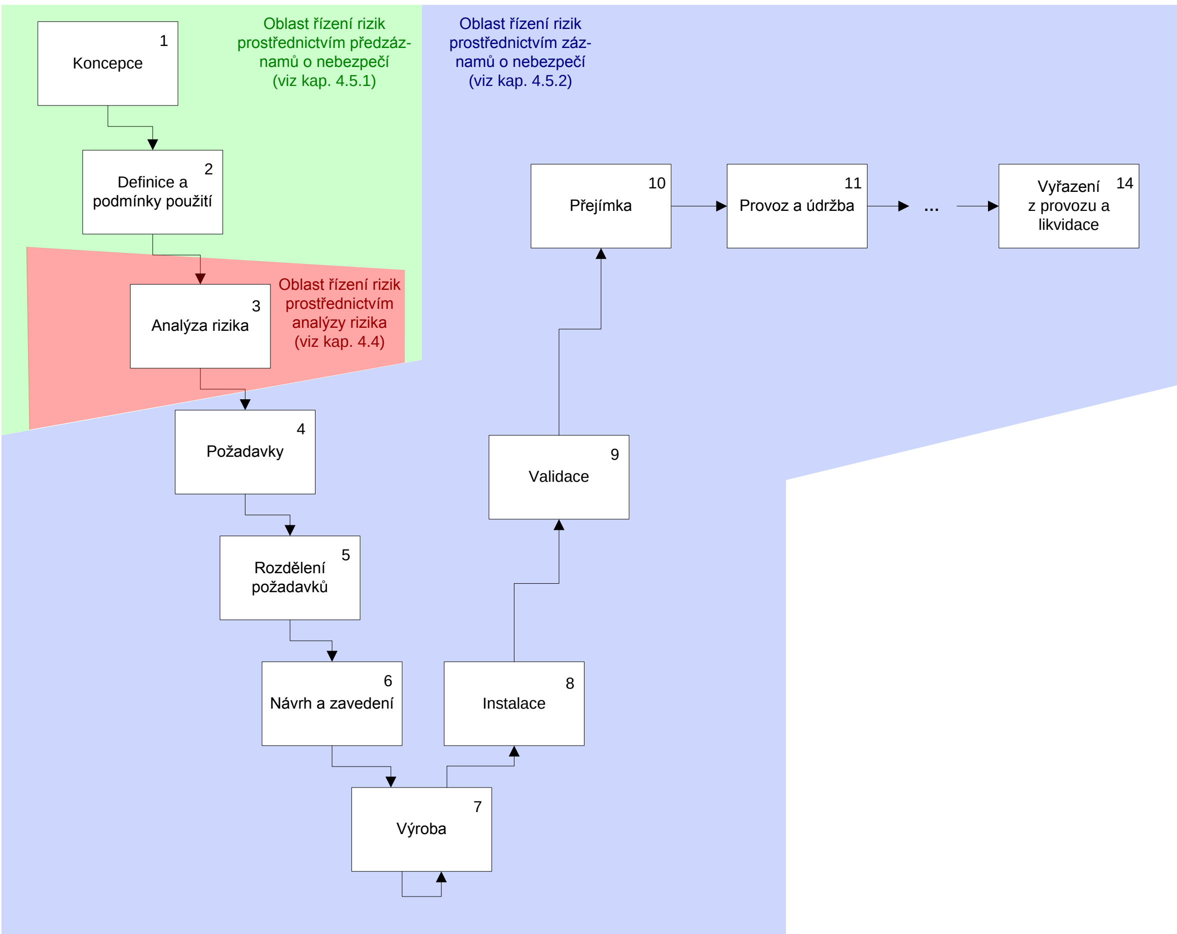
Následné hodnocení rizika	*«Uvede se hodnocení nebezpečí z hlediska jeho četnosti výskytu, následků a rizika reflektující již zapracovaná nápravná opatření»*

Tab. 4.10 – Návrh šablony záznamu o nebezpečí

Záznam o nebezpečí dle tab. 4.10 se založí a ponechá v hazard logu daného projektu aplikace systému ETCS, jen pokud existuje reziduální riziko plynoucí z jím popisovaného nebezpečí. V opačném případě pozbývá tento záznam o nebezpečí smyslu a je možno, mnou doporučováno, jej z hazard logu daného projektu odstranit.

4.6 Komplexní pohled na řízení rizik železničních zabezpečovacích systémů

Tato kapitola pouze shrnuje předchozí a názorně na obrázku založeném na V-diagramu dle [***126-1***] zachycuje v této práci navrhovaný způsob řízení rizik bezpečnostně-kritických systémů po celý jejich životní cyklus (viz obr. 4.5).



Obr. 4.5 – Navrhované způsoby řízení rizik po celý životní cyklus bezpečnostně-kritických systémů, potažmo dle zaměření této práce systémů železničních zabezpečovacích

Obrázek výše (viz obr. 4.5) zachycuje mimo jiné zde stanovený základní princip při řízení rizik bezpečnostně-kritických systémů, který spočívá v tom, že riziko plynoucí z každého identifikovaného nebezpečí je třeba řídit. Pokud k identifikaci nebezpečí dojde před třetí etapou životního cyklu dle [***126-1***], popřípadě během ní (viz překryv obou těchto oblastí na obr. 4.5) navrhuji řídit riziko z něj plynoucí prostřednictvím tzv. předzáznamů o nebezpečí, o nichž pojednává kapitola 4.5.1. Pokud k ní dojde po dokončené třetí etapě životního cyklu dle [***126-1***], navrhuji jej řídit prostřednictvím záznamu o nebezpečí, tak jak se o něm v souvislosti s průběžným managementem rizika zmiňuje například norma [***126-1***], či [***DisPpt***] a blíže jej specifikuje kapitola 4.5.2. O identifikaci a řízení rizik, které probíhá v rámci vykonávání analýzy rizika, pojednávají kapitoly 4, 5 a 6.

Z následující kapitoly (viz kap. 4.7) je patrné, že některá nebezpečí byla již identifikována na úrovni UNISIG/ERA. Jde o nebezpečí, která byla identifikována na úrovni generických technických specifikací systému ETCS. Tato nebezpečí jsou součástí UNISIG Hazard Logu [***UHL***], potažmo veřejně přístupné zprávy z tohoto hazard logu, tedy Subsetu-113 [***SS113***]. Tato nebezpečí, vzhledem k tomu, že povětšinou byla identifikována před vlastním vykonáním analýzy rizika konkrétní aplikace systému ETCS, popřípadě během jejího vypracovávání, navrhuji rizika z nich plynoucí řešit formou předzáznamů o nebezpečí (viz kap. 4.5.1), které se následně bezprostředně po vykonání této analýzy posoudí, zda byla zohledněna v rámci právě vykonané analýzy rizika či nikoli, a tedy je zapotřebí je řešit formou záznamů o nebezpečí (viz kap. 4.5.2), který se k tomuto účelu založí.

Následně po dokončení analýzy rizika doporučuji stále bedlivě sledovat prostřednictvím Subsetu-113 [***SS113***], čí lépe přímo prostřednictvím UNISIG Hazard Logu [***UHL***], je-li pro autory analýzy rizika dostupný, nově na této úrovni zakládané záznamy o nebezpečí. A ty poté, jsou-li shledány relevantními pro daný projekt, reflektovat založením odpovídajícího záznamu o nebezpečí [pozn. použití přímo UNISIG záznamů o nebezpečí v dokumentaci konkrétní aplikace systému ETCS v ČR na KP ETCS v úseku Břeclav–Kolín nedoporučuji z důvodu rozdílnosti šablon, tedy rozdílnosti požadovaných údajů o nebezpečí. Také by nepůsobilo dobrým dojmem mít část dokumentace v jazyce českém, část v jazyce anglickém].

Obecně lze říci, že téměř pro každý záznam o nebezpečí evidovaný na úrovni UNISIG/ERA, je-li pro daný projekt aplikace systému ETCS shledán relevantním, vznikne na úrovni tohoto projektu záznam o nebezpečí. Je to dáno skutečností, že záznamy o nebezpečí, jež jsou součástí [***UHL***], resp. [***SS113***], obsahují obvykle poměrně detailní provozní scénáře, při kterých daná nebezpečí nastávají. Nelze tedy předpokládat, že před analýzou rizika a v rámci jejího zpracovávání ve třetí etapě životního cyklu dle [***126-1***], kdy ještě zpravidla není znám konkrétní návrh systému a detailní popis funkčního chování, velmi pravděpodobně většinou nebudou ošetřena a bude potřeba je přenést z předzáznamů o nebezpečí daného projektu do záznamů o nebezpečí téhož projektu. Samozřejmě před jejich přenesením bude třeba posoudit, jestli k nim v dané aplikaci systému ETCS může dojít či nikoli.

Příkladem nebezpečí, pro které naopak nevznikne záznam o nebezpečí v projektu aplikace systému ETCS na KP ETCS v úseku Břeclav–Kolín, protože není pro tento projekt relevantní, je nebezpečí H0024 dle [***UHL***], resp. [***SS113***], ke kterému nemůže ve zmíněné aplikaci systému ETCS v ČR dojít, neboť se zde nevyužívá funkce zkracování MA ve spolupráci s palubní částí systému ETCS („Co-operative shortening of MA“ dle § 3.8.6 Subsetu-026 [***SS026***]). Konkrétněji se zmíněným UNISIG Hazard Logem, Subsetem-113 a souvisejícím procesním záležitostem věnuje následující kapitola 4.7, „Specifika související s řízením rizika systému ETCS“.

4.7 Specifika související s řízením rizika systému ETCS

Rizika související se systémem ETCS jsou částečně řízena na evropské úrovni. Tento proces je dokumentován v rámci mandatorních i volitelných Subsetů, které v rámci sdružení UNISIG vypracovává a je za ně zodpovědná pracovní skupina UNISIG RAMS WP, jejímž členem je též autor této práce. Tyto Subsety jsou následně přijímány a po odsouhlasení skupinou uživatelů ETCS (EUG) rovněž vydávány Evropskou železniční agenturou (ERA). Zezávazňovány jsou poté Evropskou komisí (EC) pro všechny členské státy Evropské unie (EU), které jsou povinni provést tzv. transpozici platných evropských směrnic do národní legislativy, je-li právní úprava v nich obsažená odlišná od té stávající [***Souš***].

Je tedy zřejmé, že pro komplexní pojetí řízení rizik souvisejících se systémem ETCS, což je hlavní záměr této práce, je třeba se také zabývat otázkou týkající se způsobu zapracování bezpečnostních analýz a požadavků provedených, respektive stanovených na evropské úrovni (tedy na úrovni UNISIG/ERA) do projektů konkrétních aplikací systému ETCS na úrovních národních. A právě možnými způsoby zohlednění závěrů bezpečnostních analýz a požadavků vzniknuvších v pracovní skupině UNISIG RAMS WP v národních projektech se zabývá tato kapitola. Dále tato kapitola blíže popisuje procesy související se záznamy o nebezpečí, jenž jsou součástí UNISIG Hazard Logu [***UHL***], který taktéž spravuje tato pracovní skupina (UNISIG RAMS WP).

Zde je třeba připomenout, že na systém ETCS lze pohlížet ve dvou rovinách: evropské a národní, a to nejen při řízení rizik (viz kapitoly 4.7.1 a 4.7.2), ale i při jeho definici, kdy požadavky na tento systém vznikají jak na jeho generickou část, tak i na jeho aplikační část (blíže viz kapitolu 4.3.1). Text následujících dvou kapitol byl autorem této práce již částečně publikován v [***ČBSB***], zde je rozšířen, doplněn.

4.7.1 Bezpečnostní analýzy vykonané na evropské úrovni

Tato kapitola rozebírá bezpečnostní analýzy vykonané skupinou UNISIG RAMS WP, vytváří seznam těchto analýz (včetně jejich stručného popisu) a navrhuje jejich zohlednění při řízení rizika konkrétní aplikace systému ETCS (v ČR). Tyto analýzy jsou obsaženy (dokumentovány) v následujících dokumentech:

Subset-088 (Safety Analysis /of the UNISIG ETCS Reference Architecture/)

- obsahuje systematickou analýzu nebezpečí systému ETCS
- odvozuje THR na jednotlivé komponenty ETCS (tzv. konstituenty interoperability)
- má čtyři části (Part 0 až Part 3)

Subset-088 Part 0 (Document Overview)

- úvodní, přehledový dokument
- definuje účel ETCS a tzv. základní nebezpečí (Core Hazard)

Subset-088 Part 1 (Functional Fault Tree)

- obsahuje strom FTA (analýza shora–dolů), který rozvíjí základní nebezpečí (tvořící zde vrcholovou událost stromu) do jednotlivých nebezpečí na rozhraních referenční architektury ETCS (viz kapitola 2 Subsetu-026 [***SS026***]) s definovaným vztahem k funkcím ETCS uvedeným v kapitole 4.5 Subsetu-026 „Modes and on-board function“ (tvořící zde základní události stromu), případně do selhání mimo systém ETCS (např. selhání lidského činitele – strojvedoucího)

Subset-088 Part 2 (Functional Analysis)

- detailněji analyzuje základní události stromu FTA ze Subsetu-088 Part 1, blíže je popisuje, kategorizuje (do následujících tří skupin: „safety critical“, „safety related“, či „not safety related“) a stanovuje jejich vztah k funkcím ETCS a nápravná opatření ve formě aplikačních podmínek

Subset-088 Part 3 (THR Apportionment)

- na základě předchozích částí (Part 1 a Part 2) odvozuje bezpečnostní požadavky na systém ETCS (THR na referenční architekturu ETCS)

Subset-078 (FMEA for the Interface to/from an Adjacent RBC)

- prostřednictvím analýzy FMEA systematicky zkoumá a dokumentuje nebezpečí hrozící na mandatorním rozhraní RBC/RBC dle referenční architektury ETCS, tak jak ji definuje Subset-026 [***SS026***] (viz obr. 4.6)

Subset-079 (FMEA for DMI-Subsystem)

- prostřednictvím analýzy FMEA systematicky zkoumá a dokumentuje nebezpečí hrozící na mandatorním rozhraní ke strojvedoucímu/strojvedoucí dle referenční architektury ETCS, tak jak ji definuje Subset-026 [***SS026***] (viz obr. 4.6)

Subset-080 (FMEA for TIU)

- prostřednictvím analýzy FMEA systematicky zkoumá a dokumentuje nebezpečí hrozící na mandatorním rozhraní k vozidlu dle referenční architektury ETCS, tak jak ji definuje Subset-026 [***SS026***] (viz obr. 4.6)

Subset-081 (FMEA for Transmission System)

- prostřednictvím analýzy FMEA systematicky zkoumá a dokumentuje nebezpečí hrozící na mandatorním rozhraní mezi traťovou a palubní částí ETCS dle referenční architektury ETCS, tak jak ji definuje Subset-026 [***SS026***] (viz obr. 4.6)

Subset-091 (Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2)

- z hlediska interoperability jde o mandatorní dokument
- obsahuje bezpečnostní požadavky na systém ETCS
- stanovuje THR na jednotlivé komponenty ETCS (konstituenty interoperability)
- vychází z ostatních výše citovaných analýz

Subset-077 (UNISIG Causal Analysis Process)

- stanovuje základní koncepci a pravidla platná pro bezpečnostní analýzy ETCS vykonávané skupinou UNISIG RAMS WP

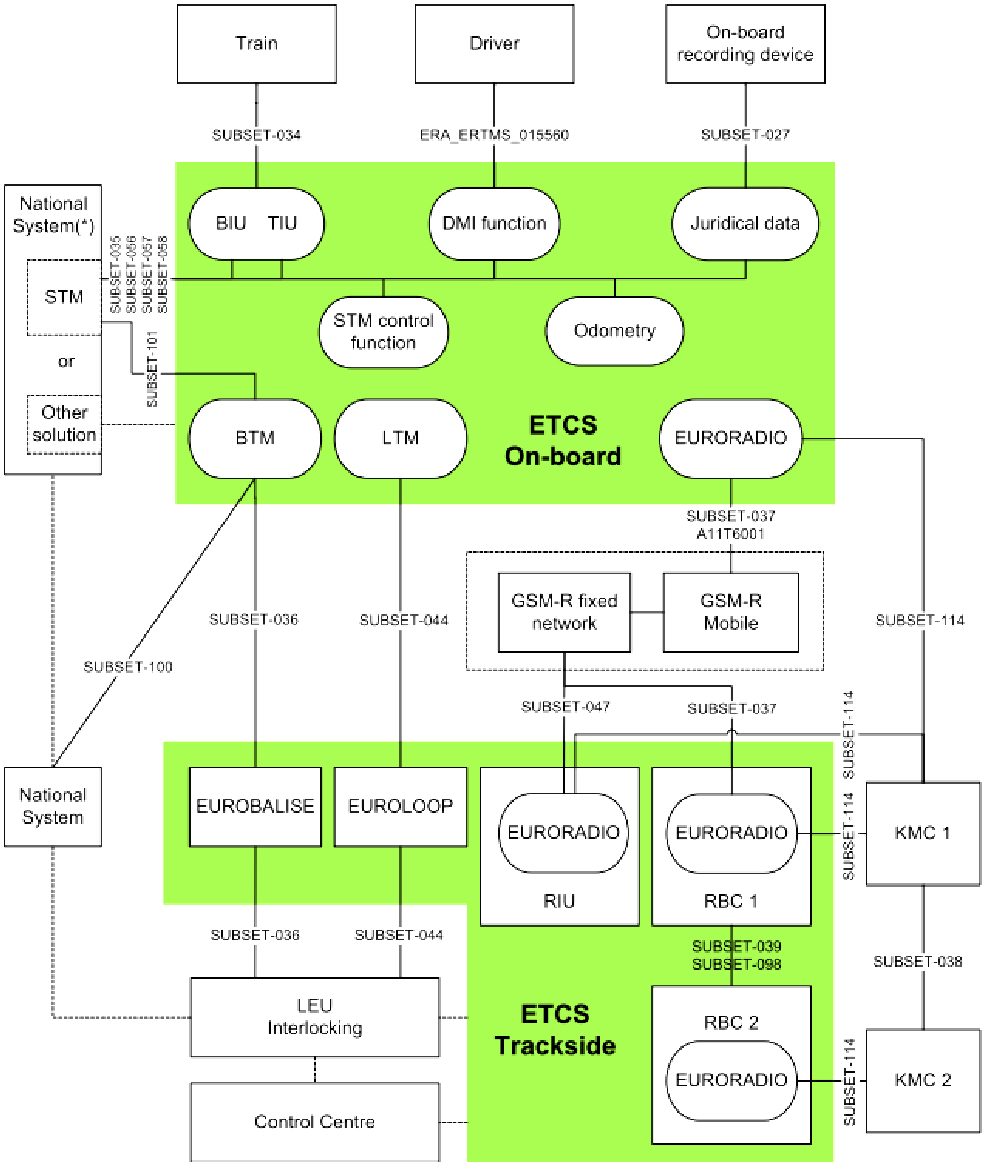
Na základě zde provedeného rozboru analýz zpracovaných a udržovaných skupinou UNISIG RAMS WP, jež jsou dokumentovány ve výše citovaných Subsetech, lze říci, že Subset-088 [***SS088***] stanovuje a systematicky analyzuje základní nebezpečí spojené se systémem ETCS („Exceedance of the safe speed or distance as advised to ETCS"), uvádí vztah tohoto nebezpečí k jednotlivým funkcím ETCS, resp. identifikuje posloupnosti událostí vedoucích k tomuto nebezpečí a na základě referenčního profilu mise ETCS vlaku odvozuje THR pro jednotlivé funkce ETCS, které jsou definované Subsetem-026. Takto odvozené THR přebírá mandatorní Subset-091 [***SS091***], který již je součástí přílohy A Technických specifikací pro interoperabilitu pro oblast řízení a zabezpečení TSI CCS [***TSI***].

Na základě výše zmíněného rozboru lze dále říci, že další skupina Subsetů, tj. Subset--078 [***SS078***], Subset-079 [***SS079***], Subset-080 [***SS080***], Subset-081 [***SS081***], detailněji analyzuje potenciální nebezpečí, která se mohou vyskytnout na mandatorních rozhraních systému ETCS dle jeho referenční architektury, tak jak ji definuje Subset-026 [***SS026***] (viz obr. 4.6). Analyzují se rozhraní k externím entitám, jako jsou:

I. vozidlo – Subset-080 [***SS080***],
II. strojvedoucí – Subset-079 [***SS079***],

stejně tak jako rozhraní mezi entitami interními, jako jsou:

I. RBC/RBC – Subset-079 [***SS079***],
II. BTM/Eurobalíza – Subset-081 [***SS081***],
III. LTM/Eurosmyčka – Subset-081 [***SS081***],
IV. Eurorádio (OBU) / Eurorádio (RBC nebo RIU) – Subset-081 [***SS081***].



*Obr. 4.6 – Referenční architektura ETCS [**SS026**]*

Výše uvedené analýzy, respektive jejich výsledky obsažené v Subsetu-091 [***SS091***] navrhuji zohlednit v rámci v této práci stanovené analýzy rizika aplikace systému ETCS při dělení THR vrcholové události stromu FTA (blíže viz kap. 5.3.4, resp. ukázkové provedení v příloze č. 5). Dále je z rozboru těchto analýz zřejmé, že se patrně záměrně neanalyzuje rozhraní k zabezpečovacímu zařízení (blok Interlocking[22] dle referenční architektury ETCS na obr. 4.6), jenž vlakovému zabezpečovači ETCS poskytuje nezbytné informace pro bezpečnou jízdu vlaku pod dohledem ETCS. Důvodem je podle mého názoru velmi pravděpodobně skutečnost, že toto rozhraní není harmonizované (ani jeho harmonizace není z hlediska dosažení

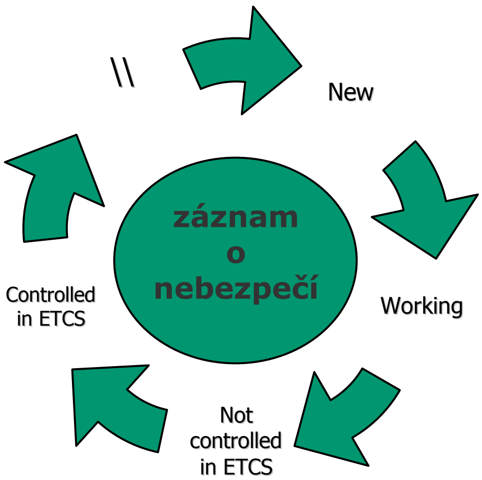
[22] U bloku „Interlocking“ v referenční architektuře ETCS je uvedená i jednotka LEU (Lineside Electronic Unit), což podle mého názoru není dobře – viz též můj komentář na konci kapitoly 4.3.1.

interoperability nutná). Z toho mi vyplývá, že právě na analýzu tohoto rozhraní se bude třeba blíže zaměřit při analýze rizika konkrétní aplikace systému ETCS (blíže viz kap. 4.3.2).

4.7.2 Nebezpečí identifikovaná na evropské úrovni

Pracovní skupina UNISIG RAMS WP vede hazard log obsahující nebezpečí identifikovaná na úrovni technických specifikací systému ETCS, zejména v souvislosti se systémovými požadavky na ETCS (tj. se Subsetem-026 [***SS026***]). Jedná se o nebezpečí, která byla identifikována dílem teoreticky (při výkladu technických specifikací ETCS), dílem experimentálně (při aplikaci systému ETCS v konkrétních projektech). Nejde tedy o úplný seznam nebezpečí spojených se systémem ETCS, ale o seznam získaný zpětnou vazbou z praxe.

Následující obrázek (viz obr. 4.7) ilustruje životní cyklus záznamu o nebezpečí, tak jak je používán [pozn. nikoli definován] v UNISIG Hazard Logu [***UHL***]. Následující text jej popisuje, a to včetně vazby na veřejně přístupnou zprávu z tohoto Hazard Logu, tedy na Subset-113 [***SS113***].



*Obr. 4.7 – Životní cyklus záznamu o nebezpečí v UNISIG Hazard Logu [**UHL**]*

Záznam o nebezpečí je oprávněn, ba dokonce povinen vytvořit každý člen pracovní skupiny UNISIG RAMS WP [***UHL***], jakmile identifikuje nebezpečí související se systémem ETCS, které spočívá v technických specifikacích tohoto systému. Vytvořením záznamu o nebezpečí je myšleno vyplnění předpřipravené šablony pro záznam o nebezpečí. Tím se záznam o nebezpečí dostává do stavu Nový (New). Jakmile se k danému záznamu o nebezpečí vyjádří celá skupina UNISIG RAMS WP přechází tento záznam do stavu Pracovní (Working). Tento záznam je dále postoupen diskusi s relevantními partnery, tj. zejména se Super Group (pracovní skupinou sdružení UNISIG definující záměr systému ETCS, tvořící a udržující Subset-026 [***SS026***]), dále s Evropskou železniční agenturou (ERA) a s uživateli systému ETCS (EUG, ERTMS Users' Group).

Po odsouhlasení navržených nápravných opatření přechází tento záznam o nebezpečí do stavu Neřízeno v systému ETCS (Not controlled in ETCS) a vytváří se záznam ve zprávě z UNISIG Hazard Logu (tj. v Subsetu-113 [***SS113***]). Navržená nápravná opatření mohou být v principu dvojího druhu:

I. nápravné opatření ve formě návrhu požadavku na změnu technických specifikací systému ETCS (CR, Change Request),
II. nápravné opatření ve formě návrhu projekčního či provozního pravidla.

V případě druhém zůstává záznam o nebezpečí nadále ve stavu Neřízeno v systému ETCS (Not controlled in ETCS), aby se prostřednictvím veřejně přístupného Subsetu-113 [***SS113***] dostalo toto nebezpečí a hlavně navržené nápravné opatření až k realizátorům konkrétních projektů systému ETCS. Takovéto záznamy je nutno přenést do konkrétního projektu aplikace systému ETCS, tak jak to již bylo popsáno v kapitole 4.6. V případě prvním se po přijetí požadavku na změnu technických specifikací systému ETCS dostává do stavu Řízeno v systému ETCS (Controlled in ETCS), kdy se záznam o nebezpečí maže v Subsetu-113. Po jeho smazání je zachováno jedinečné označení hazardu prázdné a do těla tohoto „záznamu" se zapíše následující formulace o tom, že dané nebezpečí již není relevantní pro jakoukoli Baseline systému ETCS: „*Intentionally left empty. The hazard has not been considered as relevant for any ETCS baseline. No action by application projects is required.*"

Z hlediska řízení rizika systému ETCS bude třeba posoudit každé nebezpečí obsažené v záznamech o nebezpečí UNISIG Hazard Logu [***UHL***], respektive ve veřejné zprávě z tohoto Hazard Logu (tedy Subsetu-113 [***SS113***]) jsou pro danou aplikaci systému ETCS relevantní, tj. že jeho nastání je vyloučeno použitým řešením (návrhem), což je ovšem možno ověřit až při dostatečně podrobné znalosti tohoto řešení (návrhu). Z tohoto důvodu navrhuji nebezpečí obsažená v těchto záznamech hodnotit až v rámci záznamů o nebezpečí dané aplikace systému ETCS, prostřednictvím nichž se dle kapitoly 4.6 řídí rizika až po již vykonané analýze rizika, kdy je úroveň znalosti navrhovaného řešení dle mého názoru zpravidla nedostatečná (jde o třetí etapu životního cyklu železničního zabezpečovacího systému dle [***126-1***]).

5 PŘIZPŮSOBENÍ METOD VHODNÝCH KE ZDE STANOVENÉ METODICE ANALÝZY RIZIKA

5.1 Popis a výběr metod k navrženému přístupu analýzy rizika

5.1.1 Výběr metod vhodných pro dané použití

Metody vybrané v kapitole 3.3 lze z hlediska možností jejich použití rozdělit do dvou základních skupin – primární a sekundární. Primární metody budou v navržené metodice použity jako základní. Sekundární metody mohou tyto základní metody v některých specifických případech vhodně doplňovat. Dříve popsané metody (viz kap. 3) jsem do těchto skupin rozděleny následovně:

I. primární (základní): FTA, FME(C)A;
II. sekundární (doplňkové): PHA, HAZOP, MD.

Důvody výběru primárních metod jsou zřejmé z kapitoly 4.2. Důvody výběru sekundárních metod jsou stručně shrnuty zde:

- Možné využití PHA spatřuji při rozhodování o významnosti změny systému dle směrnice [***49***].
- Studii HAZOP lze uplatnit až při detailnější znalosti celého systému/procesu, může být použita například při opakované analýze rizika, nikoli však při analýze rizika ve 3. etapě životního cyklu zabezpečovacího systému dle [***126-1***], kdy ještě tak detailní znalost neexistuje.
- Nelze opomenout metodu MD, která může v komplikovanějších případech, kdy prostřednictvím svého silného matematického aparátu může ostatní výše uvedené metody vhodně doplňovat. Typicky kupříkladu v oblasti železničních zabezpečovacích systémů při simulaci horké či studené zálohy, umožňuje například – na rozdíl od metody FTA – zachytit též obnovu systému pracujícího v bezpečnostně-spolehlivostní architektuře 2 ze 3 (tj. zejména její opětovný přechod z architektury 2 ze 2 na 2 ze 3). Integraci metody MD do metody FTA lze provést například tak, že výsledky MD se použití jako vstupní hodnoty pro určitou událost, respektive události stromu FTA.

Zde je výběru těchto metod (jak primárních, tak sekundárních) věnována větší pozornost, zejména s ohledem na již nabytou znalost celkového kontextu navrhované metodiky. Dále je provedena jejich modifikace z hlediska jejich využitelnosti v jednotlivých krocích přístupu k tvorbě analýzy rizika, tak jak jej stanovuje kapitola 4.

5.2 Detailnější popis metody využívající analýzu FME(C)A

5.2.1 Popis analýz FMEA a FMECA

FMEA je analýza druhů a důsledků poruch (Failure Mode and Effect Analysis), která byla – a v ostatních oborech stále je – primárně určena k tomu, aby umožňovala zkoumat projevy různých druhů poruch. Rozšíříme-li tuto analýzu ještě o hodnocení kritičnosti důsledků těchto poruch, pak se takto rozšířená analýza označuje jako analýza FMECA (Failure Mode, Effect, and Criticality Analysis). Jak analýza FMEA, tak analýza FMECA jsou použitelné v oblasti železniční zabezpečovací techniky. Velmi vhodné a praxí ověřené je například použití analýzy FMEA při rozboru bezpečnosti poruch (RBP), při kterém se prokazuje a hodnotí bezpečnost zabezpečovacích systémů pracujících na principu vnitřní bezpečnosti. Tímto způsobem lze totiž relativně snadno a systematicky prokázat splnění požadavků na technickou bezpečnost těchto systémů, tj. jejich bezpečnost při poruše.

Porucha			Důsledek poruchy			Hodnocení (poruchy)	Poznámka
číslo	součást	druh	chyba	selhání	výstup		

*Obr. 5.1 – Příklad předpřipraveného formuláře FMEA pro účely RBP [**AFME**]*

Při rozboru bezpečnosti poruch zabezpečovacích systémů či součástí založených na principu vnitřní bezpečnosti je vhodné vyjít z katalogu uvažovaných poruch uvedených v příloze C normy ČSN EN 50129 [***129***] a využít předpřipravenou tabulku (formulář analýzy FMEA), jejíž jedna možná varianta je uvedena na obr. 5.1. Podobný formulář byl použit v závěrečné práci autora z předmětu Syntéza bezpečných elektronických obvodů na ZČU v Plzni při rozboru bezpečnosti dohlížecího obvodu SMN-01, který je určen pro bezpečnou detekci napěťové úrovně vstupního analogového signálu a je používán v mnoha aplikacích v železniční zabezpečovací technice [***RBP***].

5.2.2 Přizpůsobení metody FME(C)A s ohledem na použití v analýze rizika

Jak již bylo naznačeno v kapitole 4.2, slouží v této práci navržené metodice analýzy rizika analýza FME(C)A k dalšímu podrobnějšímu zkoumání nebezpečí identifikovaných na určité úrovni. Může tedy sloužit nejen k analýze poruch, k čemuž byla původně určena, ale též k analýze nebezpečí, tak jak je to například navrženo zde. Tedy k požadovanému hledání posloupností událostí (příčin a následků), četností a kritičností (rizik) důsledků těchto nebezpečí. Jak jsem uváděl v kapitole 4.2, toto se dle návrhu metodiky analýzy rizika v této práci děje v několika úrovních. První úroveň představují nebezpečí nalezená v oblastech definovaných v kapitole 4.3.2. K jejich analýze je postačující využít analýzu FMEA, neboť zde není třeba uvažovat dělení THR (bližší souvislosti k dělení THR obsahuje kapitola 5.3.1). Návrh k tomuto účelu vhodného formuláře je na obrázku níže (viz obr. 5.2).

Charakteristika nebezpečí			Důsledky nebezpečí			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	

Obr. 5.2 – Metoda využívající analýzu FMEA: Návrh formuláře FMEA

Následující úrovně představují nebezpečí uvedená v předcházejícím kroku jako příčiny daného nebezpečí. Zde už dělení THR je požadováno, tudíž se k tomuto účelu použije analýza FMECA, která již hodnotí daná nebezpečí i z hlediska rizika. Návrh k tomuto účelu vhodného formuláře je na obrázku níže (viz obr. 5.3).

Charakteristika nebezpečí			Důsledky nebezpečí			Hodnocení nebezpečí			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	závažnost	četnost	riziko	

Obr. 5.3 – Metoda využívající analýzu FMECA: Návrh formuláře FMECA

Stručné vysvětlení významu jednotlivých sloupců formulářů FME(C)A je následující:

III. Charakteristika nebezpečí, obsahující identifikaci a charakteristiku daného nebezpečí

   a) *číslo (nebezpečí)* – obsahuje jedinečné identifikační číslo daného nebezpečí, které má být jedinečné v rámci celého životního cyklu analyzovaného systému
   b) *projev (nebezpečí)* – obsahuje sice stručný, zato výstižný popis projevu nebezpečí, zpravidla na úrovni významových informací
   c) *druh (nebezpečí)* – obsahuje jeden z následujících druhů:

      i. poškození = změna hodnoty (např. určitého parametru)
      ii. selhání = selhání určité funkce
      iii. ovlivnění = negativní vzájemné působení dvou a více zařízení (ať už funkční, či fyzické)
      iv. zranění = poranění
      v. znečištění = kontaminování (např. životního prostředí)

IV. Důsledky nebezpečí, obsahující popis důsledků nebezpečí na vyšších úrovních

   a) *na výstupu traťové části ETCS* – obsahuje popis projevu nebezpečí na výstupu z prvků traťové části ETCS (tj. na výstupu BG, RBC, …)
   b) *na výstupu palubní části ETCS* – obsahuje popis projevu nebezpečí na výstupu z prvků traťové části ETCS (tj. na výstupu OBU)
   c) *koncový* – obsahuje popis projevu nebezpečí na úrovni železničního systému (provozu) s ohledem na systém ETCS

V. Hodnocení nebezpečí, obsahující hodnocení nebezpečí z hlediska rizika dle kapitoly 4.3.3

   a) *závažnost (následků nebezpečí)* – pro popis hodnocení viz tab. 4.3
   b) *četnost (výskytu nebezpečí)* – pro popis hodnocení viz tab. 4.2
   c) *riziko* – dáno kombinací četnosti a závažnosti dle tab. 4.6

VI. Příčina/příčiny nebezpečí, obsahující popis možných příčin daného nebezpečí (na základě takto stanovených příčin dochází k následnému dělení základních událostí v další úrovni stromu FTA – více viz kap. 6.3)

Poznámka: Pokud existuje více stavů analyzované informace, doporučuji v analýze FMECA uvažovat jejich nejnepříznivější (nejkritičtější) kombinaci (např. informace o stavu VC může nabývat jedné z pěti významových hodnot, přičemž v analýze FMECA je uvažována pouze jejich nejkritičtější kombinace, tj. namísto hodnoty „Neaktivní“ je přenášena hodnota „Postavená s dovolující návěstí“).

Obdobné formuláře FMEA a FMECA byly již autorem této práce použity v praxi, například při analýze rizika bezpečného elektronického rozhraní mezi SZZ a RBC ETCS na Pilotním projektu ETCS v ČR (IRI, Interlocking–RBC Interface) [***RAIRI***].

5.3 Detailnější popis metody využívající analýzu FTA

5.3.1 Metoda využívající analýzu FTA (HTA)

Analýzu stromu poruchových stavů (Fault Tree Analysis), jak již bylo uvedeno v kapitole 3.2.3, ve které lze nelézt i další obecný popis této analýzy, lze úspěšně použít k identifikaci a analýze událostí, které vedou k nežádoucí vrcholové události nacházející se na vrcholu stromu (poruchových stavů). Toto představuje standardní použití této analýzy, kdy se nejprve kvalitativně přístupem od shora dolů (tj. postupem identifikace vrcholové události → následná postupná identifikace základních událostí stromu) analyzuje například funkčnost daného systému, a to od jeho základní funkce až po požadovanou úroveň jeho subfunkcí.

Poté se standardně kvantitativně, tedy za pomoci matematického aparátu, stručně popsaného v kapitole 5.3.3, analyzuje pravděpodobnost/četnost výskytu vrcholové události na základě znalosti (odhadu) pravděpodobností/četností výskytů jednotlivých základních událostí stromu. Toto je ale při analýze rizika v třetí etapě životního cyklu dle [***126-1***], kdy neznáme pravděpodobnosti/četnosti základních událostí stromu, nepoužitelné. Proto autor této práce navrhl použití nové, opačné, při němž se ze znalosti požadované pravděpodobnosti/četnosti výskytu vrcholové události stromu na základě váhování odvozují od pravděpodobnosti/četnosti výskytů jednotlivých základních událostí. Stanovení tohoto v této práci stanoveného přístupu je součástí kapitoly 5.3.4.

*Terminologická poznámka: Při analýze rizika představují jednotlivé události stromu (vrcholová, přechodové i základní – viz symboly používané při tvorbě stromu FTA zachycené na obr. 3.3) nebezpečí související s analyzovaným systémem, tedy strom by se neměl nazývat stromem poruchových stavů FTA (Fault Tree Analysis), ale strom hazardních stavů HTA (Hazard Tree Analysis). Zde se tedy kloním spíše k terminologii použité v [**ZAZS**]. Nicméně v této* *práci budu nadále používat označení FTA, a to zejména pro jeho široké v teorii i praxi již zažité užívání.*

5.3.2 Kvalitativní část analýzy FTA

Kvalitativní část analýzy FTA umožňuje vytvořením stromu poruchových stavů, respektive při analýze rizika ve třetí etapě životního cyklu dle [***126-1***] stromu selhání funkcí/subfunkcí analyzovaného systému, zachycení logických vazeb mezi jednotlivými selháními – událostmi stromu. O tom, jaké symboly, pojmy a postupy se k této kvalitativní části analýzy FTA používají, pojednává kapitola 3.2.3.

5.3.3 Kvantitativní část analýzy FTA

Analýza FTA umožňuje, vedle kvalitativní části analýzy popsané výše, též provedení kvantitativní analýzy pro výpočet kvantitativních parametrů (např. intenzit, pravděpodobností) směrem zdola nahoru. Výpočet kvantitativních parametrů směrem zdola nahoru, tj. výpočet parametrů vrcholové události při znalosti parametrů základních událostí, představuje standardní použití analýzy FTA, tak jak jej popisuje dostupná literatura o této analýze (viz např. [***FTH***]). Poněvadž informace o parametrech základních událostí, na rozdíl od informace o parametrech vrcholové události stromu FTA, obvykle není ve třetí etapě životního cyklu dle [***126-1***] dostupná. Autor této práce přišel s myšlenkou pokusit se při analýze rizika využít vhodně upravený matematický aparát pro výpočet kvantitativních parametrů jednotlivých základních událostí ze znalosti parametrů vrcholové události (blíže viz kap. 5.3.4).

Parametrem vrcholové události, meziudálosti i základní události může být v jednom stromu buď pravděpodobnost výskytu dané události, nebo intenzita výskytu této události. Záleží na účelu použití daného stromu. Pro spolehlivostní výpočty se obvykle používá pravděpodobnost. Pro bezpečnostní výpočty je předpoklad, že se budou používat intenzity výskytů jednotlivých událostí, neboť výsledkem kvantitativní části analýzy rizika má být stanovení THR, čili mezních intenzit výskytů nebezpečných událostí (Tolerable Hazard Rate). Zde je třeba zdůraznit ne příliš známou skutečnost, že při práci s intenzitami je třeba věnovat zvýšenou pozornost při kombinování různých událostí na hradle typu AND (tj. rovněž PRIORITY AND). Blíže se matematickým přístupům při výpočtech různých parametrů věnuje text na následující straně.

1. Výpočet pravděpodobnosti vrcholové události

Pro výpočet pravděpodobnosti průniku a sjednocení více (obecně závislých a slučitelných) jevů platí následující vzorce:

a) pro pravděpodobnost sjednocení výskytu *n* (slučitelných) jevů A_i:

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i) - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} P(A_i \cap A_j) + \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1}\sum_{k=j+1}^{n} P(A_i \cap A_j \cap A_k) + \ldots$$
$$\ldots + (-1)^{n-1} P\left(\bigcap_{i=1}^{n} A_i\right) \quad (5.1)$$

b) pro pravděpodobnost průniku výskytu *m* (závislých) jevů A_i:

$$P\left(\bigcap_{i=1}^{m} A_i\right) = P(A_1).P(A_2|A_1).P(A_3|A_1.A_2)\ldots.P(A_m|A_1.A_2.A_3\ldots.A_{m-1}), \quad (5.2)$$

kde $P(A_i|A_j) = \dfrac{P(A_i \cap A_j)}{P(A_j)}$, přičemž $P(A_j) \neq 0$ (5.3)

2. Výpočet intenzity vrcholové události

Pro výpočet intenzit platí obdobná pravidla (vzorce), které jsou uvedeny výše. Hlavní rozdíl spočívá v tom, že zatímco pravděpodobnost je bezrozměrná veličina, intenzita rozměr má. Proto v případě sčítání a násobení intenzit musíme toto respektovat, a to zejména při násobení, kdy násobit dvě intenzity z tohoto důvodu nelze. Je pouze přípustné sčítat dvě a více intenzit a násobit intenzitu s pravděpodobností (naznačuje to mimo jiné též norma [***159***] ve své informativní příloze D). Intenzitu v případě analýzy rizika železničních zabezpečovacích systémů představuje THR, čili v každém rozvětvení stromu FTA, které končí na hradle AND se může vyskytovat pouze jedna událost charakterizovaná intenzitou svého nastání.

Připomeňme zde ještě, že při standardním způsobu použití analýzy FTA je nejprve třeba pro každou základní událost stromu určit tzv. model poruchových stavů. Tedy určit pravidla, za kterých selhání dané události nastane. Použít lze modely známé z teorie spolehlivosti (konstantní model /výskyt je konstantní/, četnostní model /četnost výskytu i četnost obnovy je konstantní/, MTTF-model /podobný jako četnostní, ale zadány jsou přímo parametry MTTF (Mean Time To Failure) a MTTR (Mean Time To Repair))/, binomický model a další). Blíže o těchto modelech pojednává například [***Isogr***].

5.3.4 Přizpůsobení metody FTA s ohledem na použití v analýze rizika

V této kapitole je autorem navržen nový přístup k používání metody FTA a dále je zde popsán nový matematický aparát, který byl navržen tak, aby jím bylo možno určovat intenzity THR jednotlivých funkcí systému. Určení intenzit THR pro funkce systému má být totiž dle normy [***129***] také výsledkem analýzy rizika (viz krok 5 dle přístupu na obr. 4.1).

Standardní použití metody FTA vychází ze znalosti parametrů (pravděpodobností nebo intenzit) výskytu základních událostí, z nichž se postupem naznačením v předcházející kapitole (viz kap. 5.3.3) vypočítává parametr nastání vrcholové události. Vzhledem k tomu, že analýza rizika, pro níž je v této práci metoda FTA přizpůsobována, je vykonávána ve třetí etapě životního cyklu analyzovaného systému dle [***126-1***], nejsou zpravidla tyto parametry základních událostí dostupné. Autor této práce přišel s myšlenkou pokusit se upravit matematický aparát metody FTA, tak aby vyhověl pro výpočet neznámých kvantitativních parametrů jednotlivých základních událostí, a to ze znalosti parametrů vrcholové události. Tato hypotéza (možnost úpravy matematického aparátu) je v následujícím textu dále rozvíjena.

Základním předpokladem, který si autor této práce stanovil pro odvození vhodného matematického aparátu, je předchozí znalost, popřípadě vhodné stanovení kvantitativních parametrů nežádoucí vrcholové události (dále jen intenzity jejího nastání, neboť v analýze rizika jde zejména o určení tolerovatelných intenzit nebezpečí THR pro jednotlivé funkce analyzovaného systému). Dalším předpokladem je zachování standardního kvalitativního postupu tvorby stromu FTA, při němž se nejprve stanoví nežádoucí vrcholová událost a následně se v několika úrovních (fázích tvorby stromu) stanovují (rozvíjí) jednotlivé větve stromu, až se dojde na požadovanou úroveň podrobnosti (více o požadované podrobnosti viz kap. 5.4). Vyjde se tedy z intenzity vrcholové události a po provedení každé následující fáze tvorby stromu se tato intenzita vhodně rozdělí dle níže navrženého vzorce (5.7).

Navrhuji dělit intenzity výskytu událostí stromu identifikovaných v jedné fázi tvorby stromu FTA (dále jen stromu) mezi intenzity výskytu událostí stromu identifikovaných v bezprostředně následující fázi tvorby tohoto stromu založit na tzv. váhování. Váhování znamená, že každé události následující fáze tvorby stromu se přiřadí přirozené číslo, jehož hodnota je odvozena od hodnocení úrovně rizika dané události. Omezme zde řešení pouze na události, jež jsou kombinovány na hradle OR, neboť kombinace intenzit, jak bylo odůvodněno v předcházející kapitole 5.3.3, na hradle AND není možná. Pro správné rozdělení intenzity THR je nutno, aby součet intenzit THR jednotlivých událostí dal intenzitu THR události na nejbližší vyšší úrovni vzniknuvší v předcházející fázi tvorby stromu. Navíc z důvodu usnadnění používání zde navržené metodiky navrhuji používat absolutní váhy, tak aby analytik nemusel být zatěžován, z nichž se dle vzorce (5.4) vypočítá tzv. normovaná váha, která se následně využije pro vlastní dělení THR (5.6).

Na základně získaných zkušeností stanovuji pro určení matematického aparátu pro dělení intenzit THR následující výchozí předpoklady:

I. Mezi přiřazenou váhou a hodnotou intenzity THR dané události musí platit nepřímá úměra – čím vyšší je riziko (úroveň rizika) plynoucí z konkrétního nebezpečí, tím vyšší je váha tohoto nebezpečí, tím přísnější jsou požadavky na bezpečnost funkce, jejíž selhání může toto nebezpečí způsobit, a tím nižší je pro tuto funkci požadovaná intenzita THR.
II. Součet všech vah, podle nichž se dělí intenzita THR události na předcházejí úrovni, všech událostí dané úrovně stromu je roven 1 – při součtu intenzit THR jednotlivých větví je celková intenzita THR rovna intenzitě THR události na předcházející úrovni.
III. Vstupní hodnotami do výpočtu dělení intenzit THR jsou absolutní váhy jednotlivých událostí dané úrovně stanovené analytikem.

Následující tabulka (viz tab. 5.1) přibližuje postup váhování a dělení intenzity THR j-té úrovně stromu [pozn. proměnné jsou v tabulce znázorněny kurzívou]:

ID_{TOPj}	«Popis nebezpečí na vyšší úrovni stromu»				THR_{TOPj}
ID	Popis nebezpečí (nebezpečné události)	Abs. váha	Rel. váha	Norm. váha	THR $[h^{-1}]$
ID_{B1}	«Popis nebezpečí na nižší úrovni stromu»	v_{absB1}	v_{relB1}	$v_{n\text{-}relB1}$	THR_{B1}
⋮					
ID_{Bi-1}	«Popis nebezpečí na nižší úrovni stromu»	$v_{absBi-1}$	$v_{relBi-1}$	$v_{n\text{-}relBi-1}$	THR_{Bi-1}
ID_{Bi}	«Popis nebezpečí na nižší úrovni stromu»	v_{absBi}	v_{relBi}	$v_{n\text{-}relBi}$	THR_{Bi}
ID_{Bi+1}	«Popis nebezpečí na nižší úrovni stromu»	$v_{absBi+1}$	$v_{relBi+1}$	$v_{n\text{-}relBi+1}$	THR_{Bi+1}
⋮					
ID_{Bnj}	«Popis nebezpečí na nižší úrovni stromu»	v_{absBnj}	v_{relBnj}	$v_{n\text{-}relBnj}$	THR_{Bnj}

Tab. 5.1 – Parametry navržené metody dělení intenzit THR ve stromu FTA

Z předchozí tabulky (viz tab. 5.1) jsou patrné následující skutečnosti ohledně vstupních hodnot, mezihodnot a výstupních hodnot:

I. Vstupní hodnoty (podbarveny žlutě) jsou dvojího druhu:

A) hodnota intenzity THR_{TOPj}, což je hodnota pro danou úroveň „vrcholové“ události, jež se převezme z předcházející fáze tvorby stromu;

B) hodnoty absolutních vah v_{absBi} jednotlivých událostí na právě tvořené úrovně stromu, které stanoví analytik.

II. Mezihodnoty (podbarveny modře) jsou taktéž dvojího druhu:

A) hodnoty relativních vah v_{relBi}, které se ze vstupních hodnot absolutních vah v_{absBi} vypočítají dle vzorce (5.4);

B) hodnoty normovaných vah $v_{n\text{-}relBi}$, které se z mezihodnot v_{relBi} vypočítají dle vzorce (5.6).

III. Výstupní hodnoty (podbarveny zeleně) představují intenzity THR_{Bi}, které se z mezihodnot vypočítají dle vzorce (5.7).

Následující text uvádí konkrétní vzorce, včetně postupu, kterým se ze vstupních hodnot (THR_{TOPj}, v_{absBi}) získají hodnoty výstupní (THR_{Bi}). Vstupní hodnoty absolutních vah v_{absBi} se zadávají v závislosti na úrovni rizika souvisejícího s konkrétním nebezpečím, respektive lépe (pokud to lze) v závislosti na počtu výskytů jednotlivých prvků v referenčním traťovém úseku. Ze vstupních hodnot absolutních vah v_{absBi} je vypočítávána relativní váha v_{relBi} dle následujícího vzorce:

$$v_{relBi} = \begin{cases} \text{pro}\, v_{absBi} \neq 0 \wedge n_j > 1:\ 1 - \dfrac{v_{absBi}}{\sum_{i=1}^{n_j} v_{absBi}}, \\ \text{pro}\, v_{absBi} = 0 \wedge n_j > 1:\ 0, \\ \text{pro}\, v_{absBi} \neq 0 \wedge n_j = 1:\ 1, \end{cases} \tag{5.7}$$

kde n_j je počet základních událostí j-té úrovně stromu.

Z relativních vah (v_{relBi}) se následně vypočítá normovaná relativní váha ($v_{n\text{-}relBi}$), která je charakteristická tím, že pro ni platí:

$$\sum_{i=1}^{n} v_{n-relBi} = 1, \tag{5.5}$$

kde n_j je počet základních událostí j-té úrovně stromu.

Výpočet normovaných relativních vah ($v_{n\text{-}relBi}$) ze znalosti příslušných relativních vah (v_{relBi}) je proveden na základě vzorce:

$$v_{n-relBi} = \begin{cases} v_{relBi} \neq 0 : \dfrac{v_{relBi}}{\sum_{i=1}^{n_j} v_{relBi}}, \\ v_{relBi} = 0 : 1 \end{cases} \tag{5.6}$$

kde n_j je počet základních událostí j-té úrovně stromu.

Intenzity THR základních událostí (THR_{Bi}) se získají postupným vynásobením intenzity THR pro j-tou úroveň bezprostředně předcházející události (THR_{TOPj}) normovanou pro i--tou základní událost dané úrovně stromu dle vzorce:

$$THR_{Bi} = THR_{TOPj} . v_{n-relBi}, \tag{5.7}$$

kde THR_{TOPj} je tolerovatelná intenzita nebezpečí „vrcholové“ události j-té úrovně stromu, respektive tolerovatelná intenzita nebezpečí příslušné události (j-1)-ní úrovně stromu.

Poznámka 1: V případě, že vrcholová událost má pouze jedinou základní událost, výše uvedený matematický aparát není třeba používat a THR základní události THR_{Bi} je rovna THR vrcholové události THR_{TOPj}. Viz podmínka $n_j > 1$ ve vzorci (5.4).

Poznámka 2: Vyskytne-li se jedna a tatáž událost v různých větvích stromu dané úrovně s různými požadavky na intenzitu THR, považuji za z hlediska bezpečnosti vhodné aplikovat pro všechny její výskyty její nejpřísnější požadavek na intenzitu THR, tj. použití nejnižší hodnoty intenzity THR.

Poznámka 3: Navrhuji stanovovat absolutní váhy pro dělení THR z hodnocení úrovní rizik daného nebezpečí. Úroveň rizika je dána kombinací četnosti výskytu nebezpečí a závažnosti jeho následků. Každé úrovni rizika je přiřazena buď váha (jedno přirozené číslo) nebo množina vah (množina přirozených čísel). Tento způsob váhování umožní rozlišit různé úrovně rizika, a to i v případě, kdy je těmto úrovním dle tab. 4.6 přiřazena stejná kategorie rizika. Použití množiny vah doporučuji použít v případech, kdy to lze a kdy je to racionálně opodstatněné, například v situaci, kdy RBC ETCS během jednoho výpočetního cyklu (EC) zpraco-

vává informace o stavech všech relevantních prvků v kolejišti/stavědle, lze jako váhy použít přímo počty těchto prvků. Tyto počty se vezmou buď přímo z celého danou aplikací analyzovaného zabezpečovacího systému dotčeného traťového úseku, je-li předem znám, nebo z vhodně vybraného referenčního traťového úseku [pozn. ovšem pouze za předpokladu, že je tento úsek dostatečně reprezentativní]. Tento druhý způsob stanovování vah (množina vah pro každou úroveň rizika) umožní ještě preciznější dělení THR.

5.4 Popis metodiky kombinující analýzy FMEA, FMECA a FTA

Pro každou oblast dle kap. 4.3.2 je identifikováno nebezpečí, pro každé takovéto nebezpečí vznikne jeden strom FTA. Toto nebezpečí je v prvním kroku zakresleno jako vcholová událost tohoto stromu FTA. Následně je podrobeno analýze FMEA. Při ní se toto nebezpečí podrobněji analyzuje, zejména se najdou jeho příčiny. Tyto příčiny se v dalším kroku tvorby stromu FTA použijí jako základní události dané úrovně tvorby tohoto stromu. Tyto základní události se podrobí analýze FMECA. Při ní se tato nebezpečí (základní události) podrobněji analyzují, zejména se ohodnotí z hlediska rizika a najdou se jejich příčiny. Ohodnocení z hlediska rizik se využije při dělení THR, příčiny se využijí v dalším kroku tvorby stromu FTA. Tímto způsobem se pokračuje v dekompozici systému až na požadovanou úroveň podrobnosti, zpravidla na úroveň funkcí, jimž je požadováno odvodit bezpečnostní požadavky (THR, SIL apod.). Názornější a o něco podrobnější popis výše nastíněného postupu je v kapitole 6.3 „Navržená metodika analýzy rizika“, popřípadě v příloze č. 5 „Ukázka použití navržené metodiky analýzy rizika aplikace systému ETCS v ČR“.

5.5 Shrnutí vhodných metod přizpůsobených k navrženému přístupu k analýze rizika

Pro jednotlivé kroky analýzy rizika, které jsou uvedeny v kapitole 4.1.3, jsou použity následující metody – viz tab. 5.2.

Požadovaný krok analýzy rizika	Použitá metoda/technika	Reference/poznámka
Identifikace nebezpečí spojených s analyzovaným systémem / jeho okolím (krok I dle kap. 4.1.3)	úvaha provedená systematicky ve všech doporučovaných oblastech	viz kap. 4.3.2
Identifikace posloupností událostí vedoucích k identifikovaným nebezpečím (krok I dle kap. 4.1.3)	kombinace pro tento účel přizpůsobených metod FTA a FMECA	viz kap. 6.3
Ohodnocení rizik plynoucích pro systém z jednotlivých nebezpečí (krok II dle kap. 4.1.3)	expertní odhad v rámci přizpůsobené metody FMECA	viz kap. 5.2.2; toto ohodnocování navrhuji provádět bez uvážení nápravných opatření, zde je dále třeba uvážit nejhorší možné následky (např. může-li dojít ke srážce vlaků, je třeba uvažovat s tím, že došlo ke srážce dvou plně obsazených vlaků osobní dopravy)
Určení přijatelnosti rizik plynoucích pro systém z jednotlivých nebezpečí (krok III dle kap. 4.1.3)	provádí se na základě předem stanovených kritérií RAC pro jednotlivé kategorie následků, jež musí být pro dané použití odsouhlaseny provozovatelem dráhy	pro návrh jejich odvození viz kap. 4.3.3
Odvození kvantitativních bezpečnostních požadavků (krok IV dle kap. 4.1.3)	odvození intenzit THR (dělením) v rámci upravené metody FTA	viz kap. 5.3.4
Odvození kvalitativních bezpečnostních požadavků (krok IV dle kap. 4.1.3)	odvození metod pro vyvarování se vložení systematických chyb při návrhu daného systému na základě úrovní SIL, odvozených od odvozených intenzit THR	viz kap. 4.3.5
Ošetření nebezpečí identifikovaných mimo analýzu rizika (krok V dle dle kap. 4.1.3)	vypracování předzáznamů nebo záznamů o nebezpečí	viz kap. 4.5

Tab. 5.2 – Metody použité ve zde navržené metodice analýzy rizika železničních zabezpečovacích systémů

5.6 Softwarové nástroje podporující zvolené metody

Metoda využívající analýzu FMEA, či FMECA je poměrně nenáročná na softwarové nástroje. Je možno si vystačit například s dnes již běžně používaným textovým editorem MS Word. Metoda využívající analýzu FTA je z tohoto pohledu o něco náročnější. U ní je však třeba rozlišovat její kvantitativní a kvalitativní část. Pro kvalitativní část analýzy FTA, vyjadřující tvarem stromu logické závislosti mezi jednotlivými událostmi, lze využít v podstatě libovolný kreslící nástroj, například MS Malování nebo MS Visio. Tyto nástroje však nepodporují tvorbu stromů FTA, čímž přináší do jejich tvorby jistý diskomfort a odvádí tak pozornost od vlastní tvorby stromu (vymýšlení logických vazeb) k formální tvorbě stromu (vymýšlení grafické podoby stromu), což není žádoucí. Lze tedy i pro kvalitativní část tvorby stromu doporučit použití vhodného softwarového nástroje. Pro kvalitativní část analýzy FTA, při níž se provádějí nejčastěji výpočty pravděpodobnosti nastání vrcholové události (obecně lze říci matematická analýza stromu), je použití vhodného softwarového nástroje téměř nezbytností. I zde jsou však k dispozici různé nástroje, například nástroj Isograph Fault Tree+, jenž je používán v rámci pracovní skupiny UNISIG RAMS WP, která provádí bezpečnostní analýzy ETCS (viz kupř. Subset-088 [***SS088***]), nebo dostupnější nástroj OpenFTA, jenž je volně dostupný na internetu (např. na [***OFT***]).

Pro účely této disertační práce bude dále pro analýzu FME(C)A používán textový editor MS Word. Pro analýzu FTA pak volně dostupný nástroj OpenFTA, a to jak pro její kvalitativní, tak i pro její kvantitativní část. Nástroj OpenFTA je otevřený software (open source), který pomocí intuitivního rozraní umožňuje uživateli vytvářet, upravovat a matematicky analyzovat strom poruchových stavů (více např. na [***OFT***]).

6 CELKOVÉ SHRNUTÍ, POPIS NAVRŽENÉ METODIKY ANALÝZY RIZIKA

Tato kapitola vychází z poznatků předcházejících kapitol, shrnuje je a jasně definuje v této práci navrženou metodiku analýzy rizika železničních zabezpečovacích systémů, se zaměřením na aplikaci systému ETCS v ČR. V této kapitole již můžeme hovořit o kompletní metodice, neboť již známe nejen přístup k tvorbě analýzy rizika (viz jeho návrh v kap. 4), ale také metody, které se v jednotlivých krocích tohoto přístupu budou využívat (viz jejich výběr a přizpůsobení danému účelu v kap. 5), a také to, jakým způsobem se při tom budou používat (viz konkrétní návrh způsobu jejich použití v podkap. 4.2).

Jinými slovy, tato kapitola reflektuje poznatky předcházejících kapitol. Sumarizuje je a vyvozuje z nich závěry vedoucí k navržení metodiky analýzy rizika aplikace systému ETCS, což má představovat hlavní jádro této disertační práce.

6.1 Návrh postupu při vykonávání analýzy rizika

Vhodný přístup k analýze rizika železničních zabezpečovacích systémů byl stanoven v kapitole 4.1.3. Pro splnění zde jmenovaných kroků a zajištění systematičnosti provádění analýzy rizika navrhuji následující iterativní postup při jejím vykonávání:

I. identifikace základního a všech ostatních nebezpečí souvisejících se systémem
II. analýza těchto nebezpečí, tj. identifikace jejich příčin (neboli nebezpečí na bezprostředně předcházející úrovni podrobnosti)
III. současná analýza rizika těchto nebezpečí, se zohledněním jejich příčin a následků
IV. stanovení bezpečnostních požadavků na systém – odvození THR pro jednotlivé funkce systému

Z rozboru provedeného v kapitole 4.1 také plyne, že tento přístup splňuje všechny požadavky, kladené na analýzu rizika relevantními evropskými normativy.

6.2 Předpoklady navržené metodiky analýzy rizika

I. Definice systému v požadované míře podrobnosti proběhne před vlastní analýzou rizika. Tento předpoklad je automaticky splněn, pokud se při vývoji zabezpečovacího systému postupuje dle životního cyklu stanoveného v ČSN EN 50126-1 [***126-***

-1], popřípadě dle vlastního životního cyklu, kde definice systému předchází analýze rizika, tak jak je v tomto předpokladu požadováno.

II. Navržená kritéria pro hodnocení četností, následků a rizik plynoucích z nebezpečí je odsouhlaseno uživatelem systému, tj. například u traťové části systému ETCS provozovatelem dráhy (v ČR tedy u drah celostátních, na nichž se předpokládá nasazení tohoto systému, státní organizací SŽDC).

III. Předpokládá se nezávislost jednotlivých nebezpečí, respektive jejich příčin identifikovaných v rámci analýzy FMECA, což jsou vlastně opět nebezpečí, ovšem na následující úrovni dekompozice analyzovaného systému. Tento předpoklad není striktní, avšak jeho uvažování velmi usnadní následné matematické úvahy a výpočty.

6.3 Navržená metodika analýzy rizika

Následující body stručně shrnují návrh autora této disertační práce pro systematické provádění analýzy rizika bezpečnostně-kritických systémů, a to včetně návrhu metod k tomu uplatnitelných. Odvození této metodiky je součástí předcházejících kapitol této práce.

Metodika analýzy rizika železničních zabezpečovacích systémů:

1. Identifikuje se základní nebezpečí související s analyzovaným systémem
    - Základní nebezpečí u železničních zabezpečovacích systémů, jak je již uvedeno v kapitolách 4.3.2 a 4.3.3, souvisí s procesem řízení železniční dopravy, neboť tyto specifické bezpečnostně-kritické systémy slouží právě k řízení tohoto technologického procesu (železniční dopravy).
    - Identifikuje se tedy základní nebezpečí:

$$\boxed{H_{zákl.}}, \tag{6.1}$$

    - Pro takto identifikované nebezpečí se stanoví dle kritérií přijatelnosti rizik odvozených v kapitole 4.3.3 požadovaná hodnota intenzity THR:

$$\boxed{THR_{Hzákl.}}, \tag{6.2}$$

2. Identifikují se ostatní nebezpečí související s analyzovaným systémem

   - Ostatní nebezpečí se hledají v oblastech uvedených a popsaných v kapitole 4.3.2, čímž dostaneme následující vektor nebezpečí:

$$\boxed{\vec{H}_O = \left(H_{O1}, H_{O2}, \ldots, H_{Ox}\right)}, \tag{6.3}$$

     kde *x* je počet oblastí, v nichž jsou tato nebezpečí hledána.

   - Pro takto identifikovaná nebezpečí se stanoví dle kritérií přijatelnosti rizik odvozených v kapitole 4.3.3 požadované hodnoty intenzit THR:

$$\boxed{\overrightarrow{THR}_O = \left(THR_{O1}, THR_{O2}, \ldots, THR_{Ox}\right)}, \tag{6.4}$$

     kde x je počet oblastí, v nichž jsou tato nebezpečí hledána.

   - Přičemž samozřejmě může platit, že:

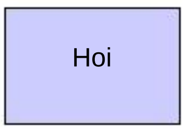
$$H_{zákl.} = H_{Oi}. \tag{6.5}$$

   - Z oblastí uvedených v kapitole 4.3.2 jsou technicky zajímavé a měly by podle mého názoru tudíž být nejvíce rozpracovány dvě oblasti: oblast rozhraní (funkce a vliv jejich selhání na rozhraní systému) a oblast funkčnosti (elektromagnetická kompatibilita /EMC/, tedy jak odolnost daného systému vůči rušení EMS, tak okolních systémů EMI)

3. Analyzují se jednotlivá nebezpečí H_{Oi} dle zde navrženého iterativního postupu kombinujícího analýzu FMEA, resp. FMECA a upravenou analýzu FTA

   - Pro každé jedno nebezpečí H_{Oi} vznikne jeden strom FTA, jehož vrcholovou událostí je právě toto nebezpečí, dle následujících bodů:

   I. Provede se kvalitativní část analýzy FTA /tvorba stromu/:

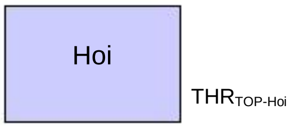


II. Provede se analýza FMEA nebezpečí H_{Oi} (vrcholové události stromu FTA) s použitím formuláře dle kapitoly 5.2.2, v rámci níž se dané nebezpečí analyzuje, zejména se určí jeho bezprostřední příčiny:

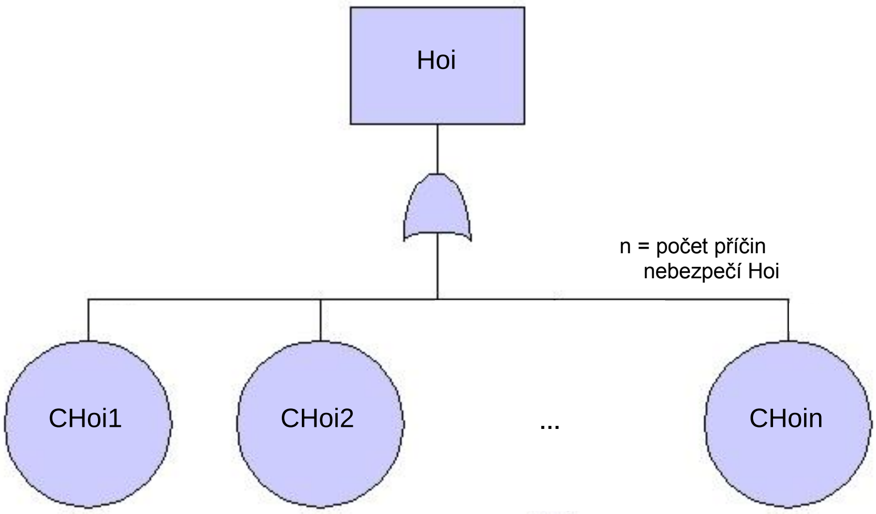
Charakteristika nebezpečí			Důsledky nebezpečí			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	
H_{Oi}	*«doplní se textový popis projevu nebezpečí»*	*«doplní se druh nebezpečí a jeho textový popis»*	*«doplní se textový popis důsledku nebezpečí na výstupu traťové části ETCS »*	*«doplní se textový popis důsledku nebezpečí na výstupu palubní části ETCS»*	*«doplní se textový popis koncového důsledku nebezpečí»*	CH_{Oi1}, CH_{Oi2}, …, CH_{Oin}

III. Provede se dělení THR /počátek kvantitativní části analýzy FTA/, v této počáteční fázi omezené pouze na stanovení THR vrcholové události H_{Oi} (tj. $THR_{TOP\text{-}HOi}$).

IV. Provede se kvantitativní část analýzy FTA, zohlednění dělení THR (dle kroku III) do kvalitativní části analýzy FTA (z kroku I):



V. Provede se kvalitativní část analýzy FTA /tvorba stromu/ další úrovně – – využije se přitom příčin identifikovaných v rámci analýzy FMECA z bodu 0:



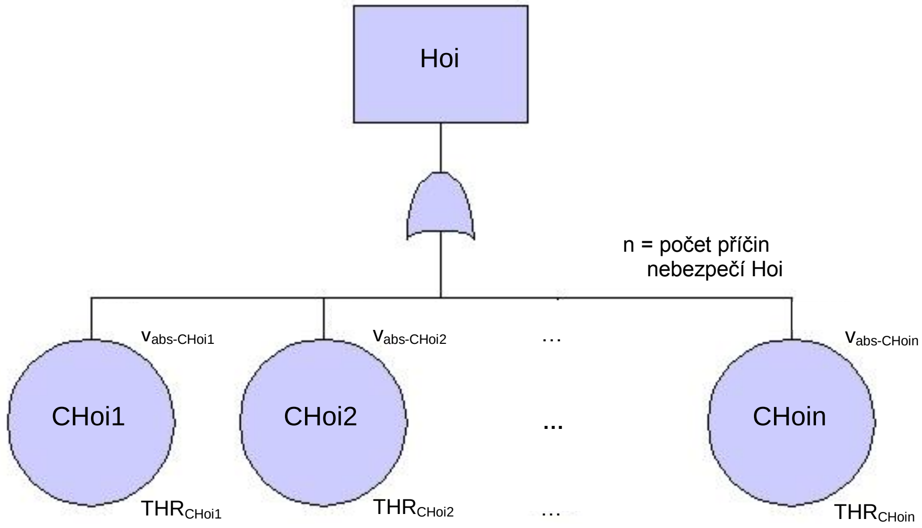
VI. Provede se analýza FMECA jednotlivých nebezpečí CH_{Oi} (základních událostí stromu FTA) s použitím formuláře dle kapitoly 5.2.2, v rámci níž se daná nebezpečí analyzují, zejména se určí jejich bezprostřední příčiny:

Charakteristika nebezpečí			Důsledky nebezpečí			Hodnocení nebezpečí			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	závažnost	četnost	riziko	
CH_{Oi1}	*«doplní se textový popis projevu nebezpečí»*	*«doplní se druhu nebezpečí a jeho textový popis »*	*«doplní se textový popis důsledku nebezpečí na výstupu traťové části ETCS»*	*«doplní se textový popis důsledku nebezpečí na výstupu palubní části ETCS»*	*«doplní se textový popis koncového důsledku nebezpečí»*	*«doplní se závažnost dle tab. 4.3»*	*«doplní se četnost dle tab. 4.2»*	*«doplní se hodnocení rizika dle tab. 4.6, resp. kap. 4.3.3»*	CH_{Oi11}, CH_{Oi12}, …, CH_{Oi1m}
CH_{Oi2}	…	…	…	…	…	⋮	⋮	⋮	CH_{Oi21}, CH_{Oi22}, …, CH_{Oi2n}
…									
CH_{Oij}	…	…	…	…	…	⋮	⋮	⋮	CH_{Oij1}, CH_{Oij2}, …, CH_{Oijo}
...									

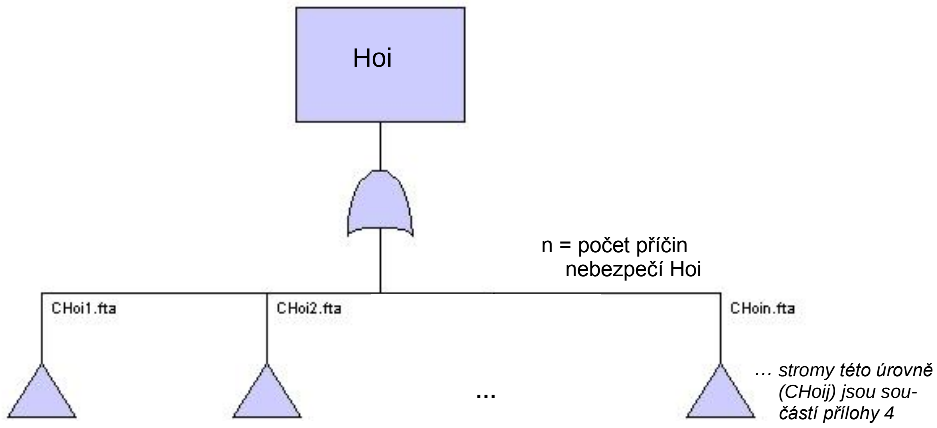
VII. Provede se dělení THR /počátek kvantitativní části analýzy FTA/, čili se provede přiřazení absolutních vah $v_{absCHOik}$ jednotlivým pro danou úroveň základním událostem CH_{Oijk} a výpočet $THR_{TOP-CHOi}$ mezi tyto události CH_{Oij} (kde $j \in \{1;...;n\}$, kde n je počet příčin nebezpečí Hoi) stromu FTA dle postupu uvedeného v kapitole 5.3.4, čímž se získají THR_{CHOik} jednotlivých základních událostí.

VIII. Provede se kvantitativní část analýzy FTA – zohlednění dělení THR (dle kroku 0) do kvalitativní části analýzy FTA (z kroku I):

- pozn. obr. je na následující straně



IX. Provede se kvalitativní část analýzy FTA další úrovně – využije se přitom příčin identifikovaných v rámci analýzy FMECA z bodu VI:



X. Opakují se kroky VI až 0, dokud se nedosáhne požadované úrovně podrobnosti dekompozice daného systému.

4. Stanoví se dle bodu 3 odvozené bezpečnostní požadavky:

$$\overrightarrow{THR}_{funkce} = (THR_{funkce\text{-}1}, THR_{funkce\text{-}2}, \ldots, THR_{funkce\text{-}n})$$

$$\Downarrow$$

$$\overrightarrow{SIL}_{funkce} = (SIL_{funkce\text{-}1}, SIL_{funkce\text{-}2}, \ldots, SIL_{funkce\text{-}n})$$

$$\Downarrow$$

$$\overrightarrow{SR}_{funkce} = (SR_{funkce\text{-}1}, SR_{funkce\text{-}2}, \ldots, SR_{funkce\text{-}n})$$

Doplňme, že jeden bezpečnostní požadavek $SR_{funkce\text{-}i}$ může obsahovat jeden nebo více bezpečnostních požadavků současně. V následujících etapách životního cyklu je třeba respektovat takto odvozené bezpečnostní požadavky a prokázat jejich naplnění (viz kap. 4.3.5).

ZÁVĚR

Předkládaná disertační práce se zabývá oblastí analýzy rizika aplikace evropského vlakového zabezpečovacího systému ETCS (European Train Control System), jehož traťová část se v dnešních dnech instaluje na traťovém úseku prvního národního tranzitního železničního koridoru Břeclav–Kolín. Na základě zvážení rizik spojených se systémem, což se děje právě v rámci analýzy rizika, se stanovují bezpečnostní požadavky na obecný bezpečnostně-kritický systém. Pro aplikaci systému ETCS, obecně pro aplikaci jakéhokoli železničního zabezpečovacího systému jsou v našich podmínkách závazné evropské normy řady ČSN EN 50126-1:2007, ČSN EN 50129:2003, ČSN EN 50159:2011, ČSN EN 50128:2012, které pro tuto oblast zcela nahrazují evropskou normu ČSN EN 61508:2011, která je jinak obecně platná pro bezpečnostně-kritické systémy.

Všechny tyto normy požadují vykonání analýzy rizika a stanovují požadavky s tím související. Ovšem tyto požadavky jsou velmi obecné, leckdy nedostatečné a navíc ne vždy napříč všemi uvedenými normami jednotné. Jeden z možných výkladů vysoké míry obecnosti a z našeho pohledu nedostatečnosti je například ten, že tyto normy ponechávají jistou volnost, aby vyhověly i případně již existující národní postupy a metody související s vykonáváním analýzy rizika železničních zabezpečovacích systémů. Výše uvedené normy tedy v podstatě stanovují pouze přístup k analýze rizika jako takové a její začlenění do životního cyklu konkrétního železničního systému. Stanovení metodiky analýzy rizika je ponecháno na národní úroveň. Tímto rozborem současného stavu poznání se se zohledněním evropské směrnice 2004/49/EC, respektive se zohledněním různých doporučení vydaných v souvislosti s touto směrnicí podrobněji zabývá kapitola 1 předkládané disertační práce.

Kromě stanovení vhodného přístupu k analýze rizika tak, aby ideálně ideově vyhověl požadavkům všem výše uvedených relevantních evropských norem, což je provedeno v kapitole 4 této disertační práce, je třeba vybrat vhodné metody, jež lze k tomuto přístupu upravit a využít. Výběru těchto metod se věnuje kapitola 3, která analyzuje metody původně normou ČSN EN 50129:2003 určené pro analýzu poruch a nebezpečí. Tato norma, respektive její příloha E ovšem uvádí jen názvy těchto metod, což není zdaleka dostačující, ba leckdy i zavádějící. Zejména u těch názvů, jenž jsou sdíleny více různými metodami. Proto byl jejich seznam v této práci rozšířen o poznámky s odkazy na zdroje obsahující popisy, o nichž se lze domnívat, že nejlépe odpovídají požadovanému účelu. Následně byl doplněn jejich stručný, komentovaný popis vzhledem k možnostem jejich použití v rámci analýzy rizika.

Z těchto metod byly následně vybrány ty metody, o kterých se bylo možno domnívat, že nejlépe poslouží požadovanému účelu, tedy účelu přístupu k tvorbě analýzy rizika železničních zabezpečovacích systémů, který byl stanoven v kapitole 4 této disertační práce. V kapitole 5 této disertační práce byly vybrány dvě metody primární (FMECA a FTA) a několik metod podpůrných, sekundárních (PHA, HAZOP a Markovovy diagramy). Dále se tato kapitola zaměřuje pouze na tyto primární metody a způsob jejich použití ve zde navržené metodice analýzy rizika, včetně jejich přizpůsobení k tomuto záměru. Obě primární metody se sice již používají, hojně například v pracovní skupině UNISIG RAMS WP, jíž je autor této práce členem. Ovšem používají se zde poněkud odlišným způsobem, což je patrné z kapitoly 4.7.1. Jejich použití (použití jejich kombinace) navržené v této práci je zcela nové.

Toto jejich použití spočívá v tom, že ve zde navržené metodice analýzy rizika je navrženo používat kombinaci těchto metod tak, že se v každém iterativním kroku této analýzy [pozn. přičemž každý tento krok obsahuje jak analýzu nebezpečí (kvalitativní část), tak následnou analýzu rizika (kvantitativní část) – viz kap. 6] použije při analýze nebezpečí pro bližší popis a hodnocení nebezpečí analýza FMECA, při následné analýze rizika se pro dělení tolerovatelných intenzit nebezpečí THR použije modifikovaná analýza FTA. Její modifikace spočívá v odlišném použití její kvantitativní části, při němž se ze znalosti intenzity THR vrcholové události postupným dělením dostáváme k intenzitám THR jednotlivých funkcí analyzovaného systému na potřebné úrovni podrobnosti (což je u kvantitativní části analýzy FTA zcela opačný přístup, než je přístup běžně používaný), a v použití odlišného matematického aparátu, který je odvozen v kapitole 5.3.4 této disertační práce.

Domnívám se, že v této disertační práci byl stanoven obecný proces řízení rizik železničních zabezpečovacích systémů, a to jak formou analýzy rizika, tak formou záznamů o nebezpečí (vč. odvození kritérií přijatelnosti rizik na základě statistik nehodových událostí evidovaných v ČR (kap. 4.3.3), stanovení šablony pro záznamy o nebezpečí (kap. 4.5.2) a zavedení tzv. předzáznamu o nebezpečí (viz kap. 4.5.1). Byl zde stanoven a popsán přístup k analýze rizika železničních systémů s důrazem na to, aby byl v souladu se všemi požadavky relevantních norem a doporučení. Dále byly navrženy (vybrány a danému účelu použití přizpůsobeny) metody, které je vhodné v rámci analýzy rizika použít a byl popsán způsob jejich použití. Zde odvozená, rozšířená metodika analýzy rizika byla již v praxi autorem této práce v méně propracované formě použita při vývoji bezpečného rozhraní mezi klasickým zabezpečovacím zařízením a radioblokovou centrálou systému ETCS L2 (komponenty IRI).

POUŽITÁ LITERATURA

[050] IEC 60050-191:1990 / A1:1999 / A2:2002. *International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*. Geneve: CEI, 1990. 149 p.

[126-1] ČSN EN 50126-1. *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)*. Část 1: Základní požadavky a generický proces. Praha: Český normalizační institut, 2007. 72 s.

[128] ČSN EN 50128 ed. 2. *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy*. Edice 2. Praha: Český normalizační institut, 2012. 108 s.

[129] ČSN EN 50129. *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy*. Praha: Český normalizační institut, 2003. 60 s. ČSN EN 50129. *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy*. Praha: Český normalizační institut, 2003. 104 s.

[159] ČSN EN 50159. *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Komunikace v přenosových zabezpečovacích systémech*. Praha: Český normalizační institut, 2011. 60 s.

[191] ČSN IEC 50(191):1993 / Z1:2003 / Z2:2003. *Medzinárodný elektrotechnický slovník: Kapitola 191: Spoľahlivosť a akosť služieb*. Bratislava: Československý inštitút technickej normalizácie a akosti, 1990. 149 s.

[20] TNŽ 34 2620. *Železniční zabezpečovací zařízení: Staniční a traťové zabezpečovací zařízení*. Praha: Generální ředitelství ČD, 2002. 82 s.

[34] SŽDC. *Směrnice pro uvádění do provozu výrobků, které jsou součástí sdělovacích a zabezpečovacích zařízení a zařízení elektrotechniky a energetiky, na železniční dopravní cestě ve vlastnictví státu státní organizace Správa železniční dopravní cesty*. Zpracoval Ing. Marcel Klega. Praha: Správa železniční dopravní cesty, 2007. 47 s.

[402] European Committee. *CSM Directive (2013/402/EC)*. Brusel: EC, 2013. 18 s.

[49] European Committee. *Safety Directive (2004/49/EC)*. Brusel: EC, 2004. 33 s.

[508] ČSN EN 61508 ed. 2. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností*. Edice 2. Praha: Český normalizační institut, 2010. 7 částí. 632 s.

[508-7] IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures.* Brussels: CENELEC, 2000. 553 p.

[57] European Committee. *Interoperability Directive (2008/57/EC)*. Brusel: EC, 2008. 45 s.

[882] IEC 61882. *Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití*. Praha: Český normalizační institut, 2002. 56 s.

[ADSA] RIBBING, Dag – LITZÉN, Björn – RYDING, Carl. *Functional Safety Analysis of ETCS DMI for Hazards other than the ETCS Core Hazard*. Draft version 1.0. Stockholm: Bombardier, 2012. 232 s.

[AFME] MAREK, Jakub. Aplikace analýzy FMEA v oblasti železniční zabezpečovací techniky. In *Elektrotechnická zařízení v dopravě*. Pardubice: KEEZ DFJP UPa, 2011. 5 s. ISBN 978-80-7395-366-9.

[AnA] European Railway Agency (ERA). *Recommendation on updating the Annex A of the TSI Control Command and Signalling (ERA/REC/03-2012/ERTMS)*. Brussels: ERA, 2012.

[ARSP] LESO, Martin – BRANDEJSKÝ, Tomáš. Analýza rizika ve schvalovacím procesu železničních zabezpečovacích zařízení z pohledu hodnotitele bezpečnosti. In *17. medzinárodné simpózium EURO-Žel 2009*. Žilina, 2009. s. 185–192. ISBN 978-80-554-0023-5.

[BMZS] HLOUŠEK, Petr. Bezpečnost moderních zabezpečovacích systémů. *Nová železniční technika*. 2008, č. 1. s. 31–34. ISSN 1210-3942.

[BŽZS] ZAHRADNÍK, Jiří – RÁSTOČNÝ, Karol – KUNHART, Milan. *Bezpečnost železničných zabezpečovacích systémov*. 1. vyd. Žilina: EDIS, 2004. 276 s. ISBN 80-8070-296-9.

[CSM] European Railway Agency (ERA). *Recommendation on the 1st set of Common Safety Methods*. Brussels: ERA, 2007. 20 p.

[CsmArt] BREYNE, Thierry – JOVICIC, Dragan. *Common Safety Method (CSM) on risk evaluation and assessment*. France: ERA, 2012. 4 p. Issued by ERA: Safety Unit – Safety Assessment Sector.

[CsmRep] ERA Safety Unit – CSM Team. *Report on the development of the first set of CSM*. Version 1.0. Brussels: ERA, 2007. 12 p.

[ČBSB] MAREK, Jakub. Činnost a výstupy pracovní skupiny UNISIG RAMS WP . In *6. konference – Zabezpečovací a telekomunikační systémy na železnici: Spolehlivostí k vyšší bezpečnosti*. České Budějovice, 2013. s. 46–49. ISBN 978-80-905200-5-9.

[DissPpt] DAVIES, Karen – DUQUENNE, Nathalie – ANTOVA, Maria – BREYNE, Thierry –CASSIR, Christophe – JOVICIC, Dragan. *Dissemination of the Commission Regulation on Common Safety Methods (CSM) on Risk Evaluation and Risk Assessment*. Presentation from CSM on Risk Assessment Dissemination Workshop. 2010. 174 p.

[Dp17] SŽDC Dp17. *Předpis pro hlášení a šetření mimořádných událostí*. Praha: Správa železniční dopravní cesty, 2008. 40 s.

[Dp17-1] SŽDC Dp17-1. *Prováděcí opatření k předpisu pro hlášení a šetření mimořádných událostí*. Praha: Správa železniční dopravní cesty, 2008. 40 s.

[DPN] ZAHRÁDKA Petr. *DesignTech.cz: otevřený publikační portál věnovaný nejen CA technologiím* [online]. 2006 [cit. 2011-04-03]. Diagram příčin a následků. Dostupné z WWW: <http://www.designtech.cz/c/caq/diagram-pricin-nasledku.htm>.

[E128] MARIANESCHI, Massimo. *UNIFE support for the extension of validity of the EN 50128:2001*. Official letter to CEN-CENELEC (especially TCX9) from General Manager of UNIFE, The European Rail Industry. Brussels: UNIFE, 2013. 3 p.

[ECE] European Commission (EC). *ERTMS – European Rail Traffic Management System*. 2009. Dostupné z WWW: <http://ec.europa.eu/transport/rail/interoperability/ertms/ertms_en.htm>.

[EČR] VARADINOV, Petr. Informace o vývoji ERTMS v České republice. In *K aktuálním problémům zabezpečovací techniky v dopravě V*. ZČU v Plzni, 2010. Dostupný též z WWW: <http://www.fel.zcu.cz/Data/documents/sem_de_2010/08_Varadinov_10.pdf>.

[EDP] European Commission (EC). *ERTMS – European Deployment Plan and National Deployment Plans*. 2009. Dostupné z WWW: <http://ec.europa.eu/transport/rail/interoperability/ertms/edp_map_en.htm>.

[ERA] European Railway Agency. Available from WWW: <http://www.era.europa.eu>.

[ETAT] CLEMENS, Pat. *Event tree analysis: a minitutorial*. 2nd Edition. 1990. 13 p. (***ETAT***)

[EWC] Union of Railways (UIC). *UIC ERTMS World Conference, Stockholm 2012: ERTMS Global Dimensions*. 2012. Dostupné též z WWW: <http://www.uic.org/cdrom/2012/10_ERTMS-Conference2012/index.html>.

[FTAW] Fault tree analysis. In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 11th August 2002, last modified on 21st February 2011 [cit. 2011-04-02]. Available from WWW: <http://en.wikipedia.org/wiki/ Fault_tree_analysis>.

[FTH] U. S. Nuclear Regulatory Commission. *Fault Tree Handbook (NUREG-0492).* Washington, D. C. 20555: Office of Nuclear Regulatory Research, 1981. 209 p.

[GTS] European Commission (EC). *TSI Application Guide (Guide for the Application of the TSI for the CCS)*. EC: Brusel, 2012. s. 26.

[HAZOP] LIHOU, Mike. *LihouTech Web site* [online]. 6.0. 2011 [cit. 2011-04-02]. Hazard & Operability Studies (HAZOPs). Dostupné z WWW: <http://www.lihoutech.com/ /hzp1frm.htm>.

[HFTA] ERICSON, Clifton II. Fault Tree Analysis – A History. In *The 17th International System Safety Conference*. Orlando, 1999. 9 p.

[HLIRI] MAREK, Jakub. *IRI – Seznam nebezpečí*. Praha, , 2011. 7 s. (bez příloh, vlastních záznamů o nebezpečí). AŽD Praha s.r.o. Závod Technika. Výzkum a vývoj. Interní dokument zastřešující jednotlivé záznamy o nebezpečí.

[InfSp] European Railway Agency (ERA). *List of Informative Specifications* [online]. 2009. [cit. 2010-12-30]. Dostupné z WWW: <http://www.era.europa.eu/Core-Activities/ ERTMS/Pages/ListOfInformativeSpecifications.aspx>.

[Isogr] Isograph. *User Guide for FaultTree+: Reliability Workbench*. Version 11.1. Warrington (UK): Isograph Ltd, 2013. 557 p.

[José] Osobní rozhovor s panem José Figueiredem, zástupcem společnosti Bombardier. Berlín, 2011.

[ManSp] European Railway Agency (ERA). *List of Mandatory Specifications* [online]. 2009. [cit. 2010-12-30]. Dostupné z WWW: <http://www.era.europa.eu/Core-Activities/ ERTMS/Pages/ListOfMandatorySpecifications.aspx>.

[MKha] KUNHART, Milan. *Systémový návrh aplikace ERTMS/ETCS L2 v ČR.* Pardubice, 2005. 102 s. Univerzita Pardubice. Dopravní fakulta Jana Pernera. Katedra elektrotechniky, elektroniky a zabezpečovací techniky v dopravě. Habilitační práce.

[MRA] MAREK, Jakub. Dílčí metody analýzy rizika železničních zabezpečovacích systémů. In *Elektrotechnická zařízení v dopravě*. Pardubice: KEEZ DFJP UPa, 2012. 11 s. ISBN 978-80-7395-466-6.

[NIP] Ministerstvo dopravy ČR. *Národní implementační plán ERTMS*. Praha: MD ČR, 2007. 29 s.

[ODP] MAREK, Jakub. *Analýza rizika aplikace systému ETCS*. 2011. 41 s. Univerzita Pardubice. Dopravní fakulta Jana Pernera. Katedra elektrotechniky, elektroniky a zabezpečovací techniky v dopravě. Odborná práce ke státní doktorské zkoušce.

[OFT] Auvation: Advanced Software solutiuons. *OpenFTA website*. Dostupné z WWW: <http://www.openfta.com/>.

[Polo] POLO, Alice. *Legal framework: Authorisation Process following the interoperability Directive 2008/57/EC*. Brusel: UNIFE, 2013. 16 s. Prezentace zástupkyně UNIFE pro členy pracovní skupiny UNISIG RAMS WP.

[PUP] MAREK, Jakub. Případy užití a problematika jejich použití v praxi. In *Seminář Elektrotechnika a elektronika v dopravě.* Pardubice, 24. 9. 2009. 5 s. ISBN 978-80-7395-194-8.

[PZH] PALEČEK, Miloš a kol. *Postupy a metodiky analýz a hodnocení rizik pro účely zákona o prevenci závažných havárií*. 1. aktualiz. vyd. Praha: VÚBP, 2005. 221 s.

[RAIRI] MAREK, Jakub. *IRI – Analýza rizika*. Praha, 2011. 48 s. (bez příloh, stromů ohrožení). AŽD Praha s.r.o. Závod Technika. Výzkum a vývoj. Interní dokument.

[RBP] MAREK, Jakub. *Rozbor bezpečnosti dohlížecího obvodu SMN-01*. 2009. 36 s. ZČU v Plzni. Fakulta elektrotechnická. Katedra aplikované elektroniky a telekomunikací. Závěrečná práce z předmětu Závěrečná práce k předmětu Syntéza bezpečných elektronických drážních zabezpečovacích systémů (KAE/XSBES).

[RHOP] Manufacturing Technology Committee – Risk Management Working Group. *Hazard & Operability Analysis (HAZOP): Risk Management Training Guide*. 2009. 9 p.

[RusKonf] Международная железнодорожная конференция по вопросам систем управления и безопасности, используемых на железнодорожном транспорте 4–6 марта 2009. Прага, Чехия.

[ŘČB] ŘÍHA, Vladimír. Zkušenosti z Pilotního projektu ETCS. In *6. konference – Zabezpečovací a telekomunikační systémy na železnici: Spolehlivostí k vyšší bezpečnosti*. České Budějovice, 2013. s. 21–26. ISBN 978-80-905200-5-9.

[SCS] Department of Trade and Industry and Engineering and Physical Sciences Research Council. *Results and Achievements from the DTI/EPSRC R&D Programme: Advances in Safety Critical Systems*. Compiled and Edited by M. Falla. 1997. 292 p.

[SDMI] Lloyd’s Register Rail BV & UK. *Functional Safety Analysis of ETCS DMI: Final Safety Analysis Report (for European Railway Agency)*. Issue 04. Compiled by Nick Brierley. 2009. 169 p.

[Souš] SOUŠEK, Jaroslav. *Zapojení České republiky do právního systému EU v působnosti železniční dopray.* Příspěvek z konference „Moderní zabezpečovací, řídicí a telekomunikační technika na tratích ČR jako součást evropského železničního systému“. České Budějovice, 2007. 5 s.

[SRS] KUNHART, Michal – KMEŤ, Vladimír. *RBC ETCS – Specifikace systémových požadavků na traťovou část ETCS L2*. 224 s. AŽD Praha s.r.o. Závod Technika. Výzkum a vývoj. Interní dokument.

[SRT] RAUSAND, Marvin – HØYLAND Arnljot. *System Reliability Theory: Models, Statistical Methods, and Applications*. 2nd ed. Wiley, 2004. 36 p. ISBN 978-0-471-47133-2.

[SS026] UNISIG (SG). *ERTMS/ETCS – ERTMS/ETCS – System Requirements Specification*. Subset-026. Issue 3.3.0. Brussels: ERA, 2012. 583 p.

[SS040] UNSIG. *ERTMS/ETCS – Dimensioning and Engineering rules*. Issue 3.2.0. Brussels: ERA, 2012. 47 p.

[SS078] UNSIG (RAMS WP). *ERTMS/ETCS – FMEA for the Interface to/from an Adjacent RBC*. Subset-078. Issue 3.3.0. Brussels: ERA, 2012. 49 p.

[SS079] UNSIG (RAMS WP). *ERTMS/ETCS – FMEA for DMI-Subsystem*. Subset-079. Issue 3.9.0. Brussels: ERA, 2012. 183 p.

[SS080] UNSIG (RAMS WP). *ERTMS/ETCS – FMEA for TIU in Application Level 1 and Level 2*. Subset-080. Issue 2.2.2. Brussels: ERA, 2012. 103 p.

[SS081] UNSIG (RAMS WP). *ERTMS/ETCS – FMEA for Transmission System*. Subset-081. Issue 3.3.0. Brussels: ERA, 2012. 44 p.

[SS088] UNSIG (RAMS WP). *ERTMS/ETCS – ETCS Application Levels 1 & 2 – Safety Analysis*. Subset-088. Issue 3.5.0. Brussels: ERA, 2012. 308 p.

[SS091] UNSIG (RAMS WP). *ERTMS/ETCS – Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2*. Subset-091. Issue 3.2.0. Brussels: ERA, 2012. 49 p.

[SS113] UNISIG (RAMS WP). *ERTMS/ETCS – Report from UNISIG Hazard Log*. Subset--113. Issue 1.1.28. Brussels: ERA, 2012. 98 p.

[TI] SEIFFERT, Rolf (ITC of IRSE). Train integrity, making ETCS L3 happen. *Signal + + Draht*. 2010, č. 9. s. 49–50. ISSN 0037-4997.

[TP] SŽDC. *Technické požadavky pro implementaci ERTMS/ETCS L2 na české části Koridoru E*. Verze 1.0.0. Praha: Správa železniční dopravní cesty, 2010. 54 s.

[TSI] European Commission (EC). *TSI CCS (Technical Specification for Interoperability for Control-Command and Signalling Subsystem)*. EC: Brusel, 2012. s. 65. (***TSI***)

[UHL] UNISIG (RAMS WP). *ERTMS/ETCS – UNISIG Hazard Log*. HAZLOG. Issue 1.1.28. Brussels: ERA, 2012. 124 p. UNISIG Internal document.

[UNIFE] UNIFE. *ERTMS Levels: Different ERTMS/ETCS application levels to match customers' needs*. ERTMS Factsheets. 2009. 2 s.

[VAR] VINCK, Karel. *Annual activity report of coordinator Karel Vinck – ERTMS project*. Brusel, 2007, 10 s. Dostupná též na WWW: <http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/tran20081103_rapp07-08vinck_/TRAN20081103_Rapp07-08Vinck_en.pdf>.

[VHAZ] TABAS, Marek – BABINEC, František – LÁSKOVÁ, Andrea. Význam analýzy metodou HAZOP při tvorbě bezpečnostní dokumentace. *Automa* [online]. 2006, č. 11 [cit. 2010-03-30]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=31467>. ISSN 1210-9592.

[VZDI] Drážní inspekce ČR. *Výroční zpráva 2012*. Praha: DI ČR, 2013. Výroční zpráva o činnosti národního vyšetřovacího orgánu pro nezávislé šetření mimořádných událostí na dráhách.

[WDI] Drážní inspekce. *Drážní inspekce: Nezávislý národní orgán pro odborné šetření příčin mimořádných událostí v drážní dopravě* [online]. 2008 [cit. 2013-11-22]. O Drážní inspekci. Dostupné z WWW: <http://www.dicr.cz/o-drazni-inspekci>.

[ZAZS] RAPKO, Július. *Teoretické základy analýzy zabezpečovacích systémov*. 1. vyd. Žilina: EDIS, 2001. 107 s. ISBN 80-7100-822-21.

[ŽEL11] MAREK, Jakub. Assessment of ETCS-definition in term of its formalisation. In *19th International symposium EURO – Žel 2011*. Žilina, 8th June 2011. pp. 161–166. ISBN 978-80-263-0003-8.

[ŽZT] CHUDÁČEK, Václav a kol. *Železniční zabezpečovací technika*. 2. přeprac. a doplň. vyd. Praha: VÚŽ, 2005. 145 s.

VLASTNÍ PUBLIKACE AUTORA

STRUČNÉ CURRICULUM VITAE – ING. JAKUB MAREK

Jakub Marek (nar. 1984) se ve své odborné činnosti zaměřuje na železniční zabezpečovací techniku, specializuje se především na otázky týkající se vlakového zabezpečovacího systému ETCS a na analýzu rizika železničních systémů. Vystudoval obor dopravní prostředky a infrastruktura – elektrotechnická zařízení v dopravě na DFJP UPa. V letech 2008/2009 zde působil na katedře elektrotechniky, elektroniky a zabezpečovací techniky v dopravě jako interní doktorand, od té doby také na UPa vyučuje odborné předměty z oblasti svého zaměření. Od roku 2009 se na úseku výzkumu a vývoje AŽD Praha s.r.o. zabývá aplikací systému ETCS na národní úrovni, v podmínkách ČR (nyní instalací traťové části systému ETCS v úseku Břeclav–Kolín). Od roku 2011 je členem mezinárodní pracovní skupiny UNISIG RAMS WP, jež primárně provádí generické bezpečnostní analýzy systému ETCS a stanovuje bezpečnostní a spolehlivostní požadavky na tento systém na evropské úrovni (výsledky této skupiny tvoří součást technických specifikací pro interoperabilitu TSI CCS).

[1] MAREK, Jakub. Činnost a výstupy pracovní skupiny UNISIG RAMS WP[23]. In *6. konference – Zabezpečovací a telekomunikační systémy na železnici: Spolehlivostí k vyšší bezpečnosti*. České Budějovice, 13. 11. 2013. s. 46–49. ISBN 978-80-905200-5-9.

[2] MAREK, Jakub. Dílčí metody analýzy rizika železničních zabezpečovacích systémů. In *Elektrotechnická zařízení v dopravě*. Pardubice, 28. 2. 2012, 11 s., ISBN 978-80-7395-466-6.

[3] MAREK, Jakub. Assessment of ETCS-definition in term of its formalisation. In *19. Inter-national symposium EURO – Žel 2011*. Žilina, 8th June 2011. pp. 161–166. ISBN 978-80-263-0003-8.

[4] MAREK, Jakub. Aplikace analýzy FMEA v oblasti železniční zabezpečovací techniky. In *Elektrotechnická zařízení v dopravě*. Pardubice, 25. 2. 2011, 5 s., ISBN 978-80-7395-366-9.

[5] MAREK, Jakub. Possible methods of train approach warning time of level crossing system equalization using ETCS. In *18. medzinárodné sympózium EURO – Žel 2010*. Žilina, 26. 5. 2010. s. 81–88, ISBN 978-80-554-0198-0.

[6] MAREK, Jakub. Možnosti spolupráce systému ETCS s přejezdovými zabezpečovacími zařízeními. In *Seminář Elektrotechnická zařízení v dopravě*. Pardubice, 12. 2. 2010, 8 s. ISBN 978-80-7395-237-2.

[23] Název příspěvku publikovaný ve sborníku: Pracovní skupina WP RAMS.

[7] KUNHART, Michal – MAREK, Jakub – OUŘEDNÍČEK, Jan. Use cases as a semi-formal way of description of the ETCS functional behaviour. In *5th International Scientific Conference Theoretical and Practical Issues in Transport*. Pardubice, 11th – 12th February 2010, pp. 79–86. ISBN 978-80-7395-245-7.

[8] MAREK, Jakub. Případy užití a problematika jejich použití v praxi. In *Elektrotechnika a elektronika v dopravě.* Pardubice, 24. 9. 2009. 5 s. ISBN 978-80-7395-194-8.

[9] KUNHART, Michal – MAREK, Jakub – OUŘEDNÍČEK, Jan. Případy užití jako první krok specifikace funkčních požadavků na aplikaci ETCS. In *EURO – Žel 2009*. Žilina, 3. 6. 2009, s. 279–289, ISBN 978-80-554-0023-5.

[10] KUNHART, Milan – MAREK, Jakub. Popis prací na projektu interface IRI. In *K aktuálním problémům zabezpečovací techniky v dopravě IV*. Plzeň, 27. 5. 2009.

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

ALARP	As Low As Reasonable Practicable	Tak malé (riziko), jak je to jen rozumně proveditelné
AŽD	-	Automatizace železniční dopravy
BTM	Balise Transmission Module	Přenosový modul pro balízy (ETCS)
CCD	Cause-Consequence Diagrams	Diagramy „příčina–následek“
CCS	Control-Command and Signalling Subsystem	Řídicí a zabezpečovací subsystém
CSM	Common Safety Method	Společná bezpečnostní metoda
ČR	-	Česká republika
DFJP	-	Dopravní fakulta Jana Pernera
DMI	Driver Machine Interface	Rozhraní (OBU) ke strojvedoucímu
DÚ	-	Drážní úřad
EC	European Commission // Elaboration Cycle //	Evropská komise // Výpočetní cyklus //
ERA	European Railway Agency	Evropská železniční agentura
ERTMS	European Rail Traffic Management System	Evropské systém řízení železničního provozu
ETA	Event Tree Analysis	Analýza stromu událostí
ETCS	European Train Control System	Evropský vlakový zabezpečovací systém
ETCS L2	European Train Control System Level 2	Evropský vlakový zabezpečovací systém 2. úrovně
EU	European Union	Evropská unie
EUG	ERTMS Users' Group	Skupina uživatelů
FMEA	Failure Modes and Effects Analysis	Analýza druhů a důsledků poruch
FMECA	Failure Modes, Effects and Criticality Analysis	Analýza druhů, důsledků a kritičnosti poruch
FTA	Fault Tree Analysis	Analýza stromu poruchových stavů
GAMAB	Globalement Au Moins Aussi Bon	Celkově nejméně tak dobré (jako to předchozí)

GSM-R	Global System for Mobile Communications for Railways	Globální systém pro mobilní komunikace pro železniční aplikace
H	Hazard	Nebezpečí
HAZOP	HAZard and OPerability Study	Studie nebezpečí a provozuschopnosti
HR	Hazard Rate	Četnost/intenzita nebezpečí
HTA	Hazard Tree Analysis	Analýza stromu nebezpečí
CH	Cause of Hazard	Příčina nebezpečí
IRI	Interlocking–RBC Interface	Rozhraní mezi RBC a ZZ
JRU	Juridical Recordable Unit	Záznamová jednotka (ETCS)
KMC	Key Management Centre	Centrum správy klíčů
LC	Life Cycle	Životní cyklus
LEU	Lineside Electronic Unit	Traťová elektronická jednotka (ETCS)
MD	Markovov diagrams	Markovovy diagramy
MEM	Minimum Endogenous Mortality	Minimální endogenní úmrtnost
MTTF	Mean Time To Failure	Střední doba do poruchy
MTTR	Mean Time To Repair	Střední doba do opravy
OBU	On-Board Unit	Mobilní/palubní jednotka (ETCS)
P&ID	Piping and Instrumentation Diagram	-
PHA	Preliminary Hazard Analysis	Předběžná analýza nebezpečí
PU	-	Případy užutí
R	Requirement	Požadavek
RAC	Risk Acceptation Criteria	Kritéria přijatelnosti rizika
RAMS	Reliability, Availability, Maintainability, and Safety	Bezporuchovost, pohotovost, udržovatelnost a bezpečnost
RBC	Radioblock Centre	Radiobloková centrála
RBP	-	Rozbor bezpečnosti poruch
SIL	Safety Integrity Level	Úroveň integrity bezpečnosti
SR	Safety Requirement	Bezpečnostní požadavek
SS	Subset	Podmnožina (technických specifikací ETCS)
STA	Success Tree Analysis	Analýza stromu úspěchů
STM	Specific Transmission Module	Specifické přenosový modul (pro národní VZ) (ETCS)

SZZ	-	Staniční zabezpečovací zařízení
SŽDC	-	Správa železniční dopravní cesty
SG	Super Group	-
THR	Tolerable Hazard Rate	Tolerovatelná četnost/intenzita nebez-pečí
TSI	Technical Specifications for Interope-rability	Technické specifikace interoperability
UNISIG	UNIon of SIGnalling	Sdružení výrobců železničních zabez-pečovacích systémů
UPa	-	Univerzita Pardubice
WP	Work Packet	Pracovní balíček/skupina
ZČU	-	Západočeská univerzita
ZZ	-	Zabezpečovací zařízení
ŽU	-	Žilinská univerzita

SEZNAM PŘÍLOH

Příloha č. 1: Údaje z databáze Drážní inspekce ČR (www.dicr.cz) o mimořádných událostech
Příloha č. 2: Dokumentovaný postup zpracování údajů o mimořádných událostech
Příloha č. 3: Výsledky zpracování (statistika) údajů o mimořádných událostech
Příloha č. 4: Dílčí stromy CHoi1 až CHoin z kapitoly 6.3
Příloha č. 5: Ukázka použití navržené metodiky analýzy rizika aplikace systému ETCS v ČR

Příloha č. 1 Údaje z databáze Drážní inspekce ČR (www.dicr.cz) o mimořádných událostech

Na základě žádosti autora této disertační práce poskytla Drážní inspekce, státní instituce, která odborně zjišťuje příčiny nehodových (mimořádných) událostí a vykonává státní dozor na dráhách, potřebné údaje z databáze mimořádných událostí z let 2008 až 2013 (resp. od 1. 1. 2008 do 18. 11. 2013). Tato data obsahuje přiložený CD-ROM.

Příloha č. 2 Dokumentovaný postup zpracování údajů o mimořádných událostech (dále jen MU)

MU druhu Srážka drážních vozidel

I. Výběr dat za ucelené období od 1. 1. 2008 do 31. 12. 2012 (tj. zohledněno posledních ucelených 5 let, údaje za kalendářní rok 2013 nebyly v době zpracovávání této disertační práce úplné)

II. Omezení dat pouze na dráhy celostátní, regionální a vlečky (tedy vyjmutí dat za dráhy tramvajové a trolejbusové)

III. Omezení dat pouze na ta data, která vyhovují [pozn. sloveso „vyhovují“ zní v tomto kontextu poněkud zvláštně, ovšem z hlediska statistického je jeho použití správné] tím, že součet usmrcených a zraněných osob je roven nebo vyšší než 5: splňuje 7 MU * katastr. / závažná nehoda

IV. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je vyšší než 5 mil. Kč: splňují 4 MU * katastr. / závažná nehoda

V. Omezení dat pouze na ta data, která vyhovují tím, že došlo k jednomu nebo více úmrtí a současně součet usmrcených a zraněných osob je menší než 5: splňuje 0 MU * kritick. / nehoda

VI. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že součet usmrcených a zraněných osob je menší než 5: splňuje 20 MU * kritick. / nehoda

VII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je v rozmezí od 0,5 mil. Kč (včetně) do 5 mil. Kč (mimo): splňuje 23 MU * kritick. / nehoda

VIII. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je v rozmezí od 50 tis. Kč (včetně) do 0,5 mil. Kč (mimo): splňuje 57 MU * kritick. / ohrožení

IX. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je do 50 tis. Kč (mimo): splňuje 63 MU * kritick. / ohrožení

MU druhu vykolejení DV taková, k nimž došlo vinou překročení povolené rychlosti (*v konečné statistice se předpokládá, že jde o 75 % ze všech evidovaných*)

I. Výběr dat za ucelené období od 1. 1. 2008 do 31. 12. 2012 (tj. zohledněno posledních ucelených 5 let, údaje za kalendářní rok 2013 nebyly v době zpracovávání této disertační práce úplné)
II. Omezení dat pouze na dráhy celostátní, regionální a vlečky (tedy vyjmutí dat za dráhy tramvajové a trolejbusové)
III. Omezení dat pouze na ta data, která vyhovují tím, že součet usmrcených a zraněných osob je roven nebo vyšší než 5: splňuje 1 MU * katastr. / závažná nehoda
IV. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je vyšší než 5 mil. Kč: splňuje 8 MU * katastr. / závažná nehoda
V. Omezení dat pouze na ta data, která vyhovují tím, že došlo k jednomu nebo více úmrtí a současně součet usmrcených a zraněných osob je menší než 5: splňuje 0 MU * kritick. / nehoda
VI. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že součet usmrcených a zraněných osob je menší než 5: splňuje 0 MU * kritick. / nehoda
VII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je v rozmezí od 0,5 mil. Kč (včetně) do 5 mil. Kč (mimo): splňuje 38 MU * kritick. / nehoda
VIII. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je v rozmezí od 50 tis. Kč (včetně) do 0,5 mil. Kč (mimo): splňuje 194 MU kritick. / ohrožení
IX. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je do 50 tis. Kč (mimo): splňuje 620 MU kritick. / ohrožení

MU druhu Nedovolené projetí návěstidla zakazujícího jízdu

I. Výběr dat za ucelené období od 1. 1. 2008 do 31. 12. 2012 (tj. zohledněno posledních ucelených 5 let, údaje za kalendářní rok 2013 nebyly v době zpracovávání této disertační práce úplné)
II. Omezení dat pouze na dráhy celostátní, regionální a vlečky (tedy vyjmutí dat za dráhy tramvajové a trolejbusové)

III. Omezení dat pouze na data týkající se projetí návěstidel vlaky, nikoli posunujícími díly, přičemž současně nejde o projetí návěstidla v důsledku náhlé změny návěsti před vlakem

IV. Omezení dat pouze na ta data, která vyhovují tím, že součet usmrcených a zraněných osob je roven nebo vyšší než 5: splňuje 0 MU * katastr. / závažná nehoda

V. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je vyšší než 5 mil. Kč: splňuje 0 MU * katastr. / závažná nehoda

VI. Omezení dat pouze na ta data, která vyhovují tím, že došlo k jednomu nebo více úmrtí a současně součet usmrcených a zraněných osob je menší než 5: splňuje 0 MU * kritick. / nehoda

VII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že součet usmrcených a zraněných osob je menší než 5: splňuje 0 MU * kritick. / nehoda

VIII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je v rozmezí od 0,5 mil. Kč (včetně) do 5 mil. Kč (mimo): splňuje 0 MU * kritick. / nehoda

IX. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je v rozmezí od 50 tis. Kč (včetně) do 0,5 mil. Kč (mimo): splňuje 12 MU * kritick. / ohrožení

X. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je do 50 tis. Kč (mimo): splňuje 223 MU kritick. / ohrožení

MU druhu Ostatní

I. Výběr dat za ucelené období od 1. 1. 2008 do 31. 12. 2012 (tj. zohledněno posledních ucelených 5 let, údaje za kalendářní rok 2013 nebyly v době zpracovávání této disertační práce úplné)

II. Omezení dat pouze na dráhy celostátní, regionální a vlečky (tedy vyjmutí dat za dráhy tramvajové a trolejbusové)

III. Omezení dat pouze na data týkající se pouze následujících poddruhů: lomu kolejnice, selhání návěstních/zabezpečovacích systémů, jiné MU

IV. Omezení dat pouze na ta data, která vyhovují tím, že součet usmrcených a zraněných osob je roven nebo vyšší než 5: splňuje 0 MU * katastr. / závažná nehoda

V. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je vyšší než 5 mil. Kč: splňuje 0 MU * katastr. / závažná nehoda

VI. Omezení dat pouze na ta data, která vyhovují tím, že došlo k jednomu nebo více úmrtí a současně součet usmrcených a zraněných osob je menší než 5: splňuje 0 (2008), 0 (2009), 1 (2010), 3 (2011), 1 (2012) MU * kritick. / nehoda

VII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že součet usmrcených a zraněných osob je menší než 5: splňují 3 (2008), 2 (2009), 3 (2010), 3 (2011), 4 (2012) MU * kritick. / nehoda

VIII. Omezení dat pouze na ta data, která nevyhovují dle bodu předchozího, avšak vyhovují tím, že celková vzniknuvší škoda je v rozmezí od 0,5 mil. Kč (včetně) do 5 mil. Kč (mimo): splňuje 3 (2008), 0 (2009), 3 (2010), 2 (2011), 2 (2012) MU * kritick. / nehoda

IX. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je v rozmezí od 50 tis. Kč (včetně) do 0,5 mil. Kč (mimo): splňuje 38 (2008), 38 (2009), 42 (2010), 59 (2011), 63 (2012) MU * kritick. / ohrožení

X. Omezení dat pouze na ta data, která vyhovují tím, že u nich nedošlo k žádnému úmrtí ani zranění, avšak celková vzniknuvší škoda je do 50 tis. Kč (mimo): splňuje 212 (2008), 236 (2009), 279 (2010), 294 (2011), 372 (2012) MU * kritick. / ohrožení

Příloha č. 3 Výsledky zpracování (statistika) údajů o mimořádných událostech

Na základě výše popsaného postupu (Příloha č. 2) vznikly statistiky, kterou zachycují následující dvě tabulky:

1. Základní dělení vybraných kategorií MU

Druh MU	Počet MU za posledních 5 let (2008–2012) kategorie		
	závažná nehoda	nehoda	ohrožení
srážka DV	11	43	120
vykolejení DV taková, k nimž došlo vinou překročení povolené rychlosti (75 %)	7 (9*)	29 (38*)	611 (814*)
projetí návěstidla v poloze zakazující jízdu	0	0	235
lom kolejnice (pozn. je součástí kategorie ostatní MU)	*nejsou dostupné informace*	*nejsou dostupné informace*	*nejsou dostupné informace*
ostatní MU	0	30	1 633
celkové počty pro všechny druhy MU	**18**	**102**	**2 599**
po aproximaci na celý užitečný život ZZ[24]	**72**	**408**	**10 396**

**) Z dostupných údajů (viz přílohu č. 1) nebyla patrná příčina vykolejení: Jedná se tedy o číslo získané dle kritérií v příloze č. 2 ze všech evidovaných vykolejení dle přílohy č. 1. Před závorkou je toto číslo redukováno na předpokládaný počet vykolejení, k nimž došlo vinou překročení rychlosti (předpokládám, že jich bylo 75 % z celkového počtu).*

Pozn. Pro tabulku s podrobnějším dělení vybraných kategorií MU viz následující stranu.

[24] Pro definici ne příliš rozšířeného pojmu „užitečný život“ viz normu ČSN IEC 50(191):1993 / Z1:2003 / Z2:2003 [***191***], která je českou verzí normy IEC 60050-191:1990 / A1:1999 / A2:2002 [***050***]. Počátkem tohoto časového intervalu (užitečného života), který není ve výše citovaných normách explicitně uveden, rozumím okamžik, kdy je systém uveden do provozu (tj. např. ve vazbě na normu [***126-1***] je úspěšně ukončena etapa 10 dle této normy definovaného životního cyklu).

2. Podrobnější dělení vybraných kategorií MU

Druh MU	Počet MU za posledních 5 let (2008–2012) kategorie			
	závažná nehoda	nehoda	ohrožení	
			O1	O2
srážka DV	11	43	57	63
vykolejení DV taková, k nimž došlo vinou překročení povolené rychlosti (75 %)	7 (9*)	29 (38*)	146 (194*)	465 (620*)
projetí návěstidla v poloze zakazující jízdu	0	0	12	223
lom kolejnice (pozn. je součástí kategorie ostatní MU)	*nejsou dostupné informace*	*nejsou dostupné informace*	*nejsou dostupné informace*	*nejsou dostupné informace*
ostatní MU	0	30	240	1 393
celkové počty pro všechny druhy MU	**18**	**102**	**455**	**2 144**
po aproximaci na celý užitečný život ZZ	**72**	**408**	**1 820**	**8 576**

Legenda:

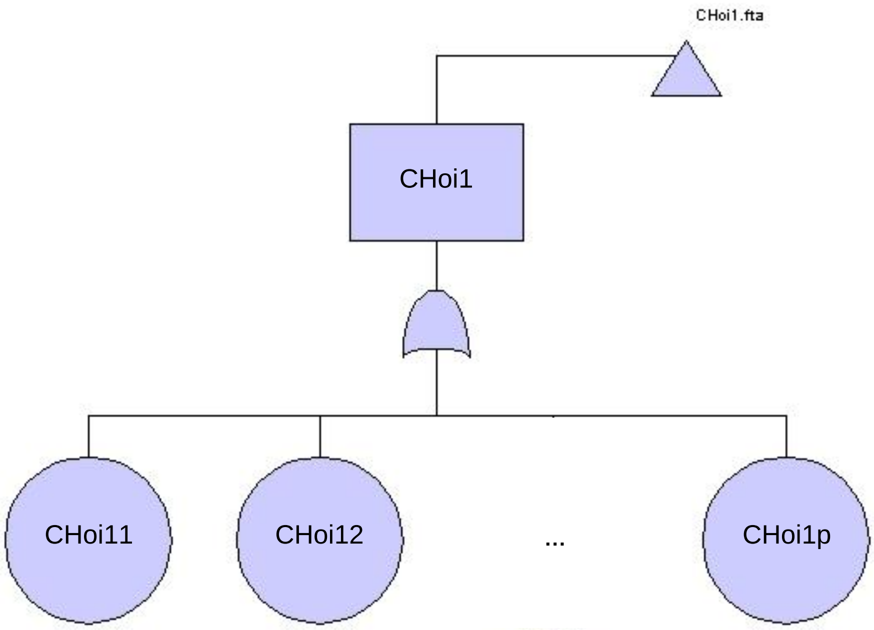
Kategorie MU (závažná nehoda, nehoda, ohrožení) jsou kategorie MU, tak jak jsou uvedeny v zákonu o dráhách a definovány ve Výroční zprávě 2012.

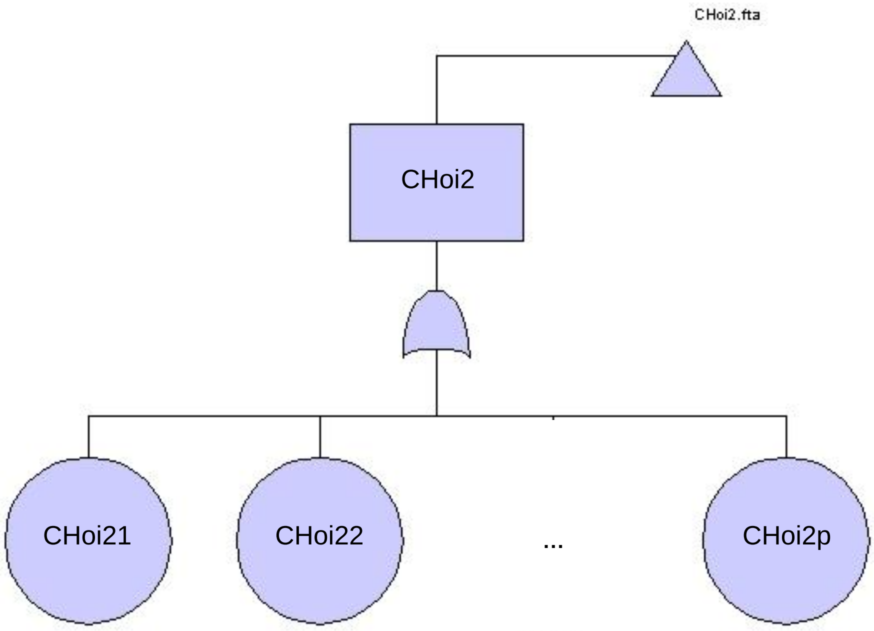
Kategorie MU (závažná nehoda, nehoda, ohrožení) jsou kategorie MU, tak jak jsou uvedeny v zákonu o dráhách a definovány ve Výroční zprávě 2012.

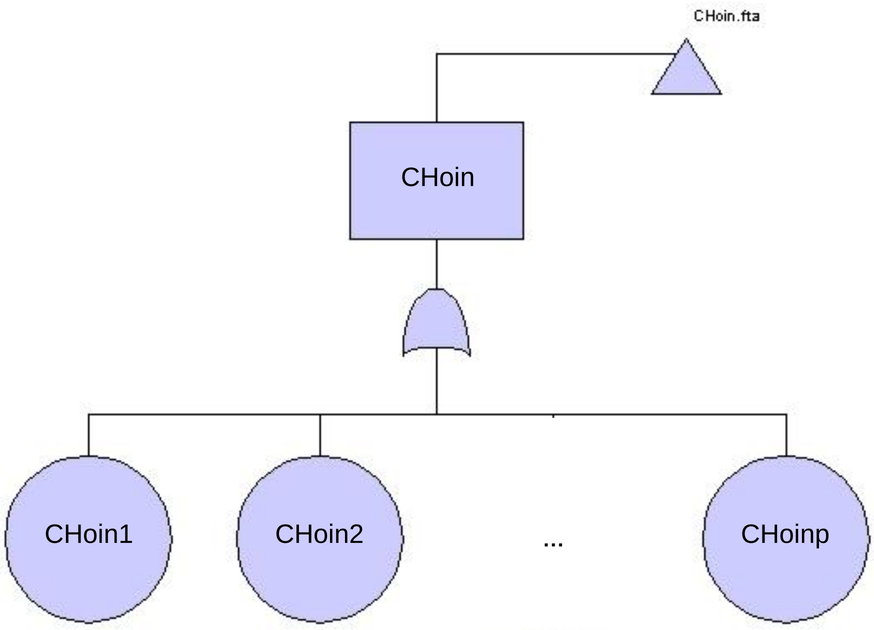
Podkategorie MU kategorie ohrožení (O1 a O2) jsem odlišil dle hmotné škody, která při nich vznikla (jestli škoda byla ve smyslu zákona č. 140/1961 Sb., trestního zákona, větší nebo nikoli). Vznikla-li škoda větší (tj. škoda převyšující částku 50 tis. Kč) jde o podkategorii O1, v opačném případě o podkategorii O2.

Text „nejsou dostupné informace“ značí, že tento druh MU není v databázi Drážní inspekce ČR explicitně uvedený. Je zahrnut v kategorii jiné (např. ostatní MU).

Příloha č. 4 Dílčí stromy CHoi1 až CHoin z kapitoly 6.3






CHoin.fta
CHoin
CHoin1
CHoin2
...
CHoinp

Příloha č. 5 Ukázka použití navržené metodiky analýzy rizika aplikace systému ETCS v ČR

Tato ukázka má sloužit pouze pro ilustrativní přiblížení použití navržené metodiky na příkladu aplikace systému ETCS, respektive na aplikaci jeho traťové části na Komerčním projektu ETCS v ČR na úseku Břeclav–Kolín. Neklade si za cíl být zcela vyčerpávající a kompletní. Vychází z postupu naznačeného v kapitole 6, čemuž koresponduje i použité číslování.

1. Identifikuje se základní nebezpečí související s analyzovaným systémem

   - Základní nebezpečí související s evropským vlakovým zabezpečovacím systémem ETCS, jakožto vlakovým zabezpečovačem s kontrolou rychlosti vlaku, je definováno v § 4.2.1.8 Subsetu-091 [***SS091***] jako:

překročení povolené rychlosti/vzdálenosti

   - *Poznámka: V původní definici je v [**SS091**] navíc dovětek: „[...] as advised to ETCS“, což zde, kde již hovoříme o konkrétní aplikaci tohoto systému, není nutno, ba dokonce ani žádoucí, neboť je třeba analyzovat též rizika související s chybnými vstupními informacemi, jejichž dostupnost a správnost se očekává.*
   - Pro nebezpečí související s traťovou částí systému ETCS stanovuje obrázek 3 Subsetu-091 [***SS091***] tolerovatelnou intenzitu nebezpečí takto:

     $$\boxed{THR_{trackside} = 1.10^{-9}\ h^{-1}}$$

   - Omezíme-li se pouze na traťovou část systému ETCS, která bude dále analyzována, lze základní nebezpečí formulovat jako:

vydání více povolující informace

   - Intenzitu THR pro takto definované základní nebezpečí související s traťovou částí systému ETCS lze převzít tak, jak ji stanovuje Subset-091 [***SS091***]. Její hodnota totiž neodporuje kritériu pro katastrofickou závažnost následků dle tab. 4.6 (hodnota přebíraná ze Subsetu je přísnější), tedy:

     $$\boxed{THR_{\text{základní nebezpečí}} = 1.10^{-9}\ h^{-1}}$$

2. Identifikují se ostatní nebezpečí související s analyzovaným systémem

   - Ostatní nebezpečí se hledají při uvažování všech normálních okolností v oblastech uvedených a blíže specifikovaných v kapitole 4.3.2:

a) Nebezpečí plynoucí z normálního provozu traťové části ETCS (H_{O1})

   - Z hlediska projevu je toto nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
   - Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho1} = THR_{\text{základní nebezpečí}} = 10^{-9}\ h^{-1}}$$

b) Nebezpečí plynoucí z nouzového provozu traťové části ETCS (H_{O2})

   - Nouzový provoz ETCS je provoz s určitými omezeními, např. jsou dostupné jen vybrané funkce. U analyzované aplikace ETCS však tento druh provozu není definován, tudíž tato oblast nebude pro účely analýzy rizika dále uvažována.
   - Intenzita THR nebyla v důsledku neuvažování nebezpečí stanovena.

c) Nebezpečí plynoucí z poruchových stavů traťové části ETCS (H_{O3})

   - Z hlediska projevu je toto nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
   - Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho3} = THR_{\text{základní nebezpečí}} = 10^{-9}\ h^{-1}}$$

d) Nebezpečí plynoucí z chybného použití traťové části ETCS (H_{O4})

   - Nebezpečí plyne z chybného stanovení podmínek použití jednotlivých komponent traťové části ETCS, nebo z nedodržení správně stanovených podmínek použití.
   - Z hlediska projevu je toto nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
   - Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho4} = THR_{\text{základní nebezpečí}} = 10^{-9}\ h^{-1}}$$

e) Nebezpečí plynoucí z rozhraní traťové části ETCS (H_{O5})

- Nebezpečí spočívá v možnosti nežádoucího vydání nebo přijetí chybné informace vedoucí k vydání více povolující informace.
- Z hlediska projevu je toto nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho5} = THR_{\text{základní nebezpečí}} = 10^{-9}\ h^{-1}}.$$

f) Nebezpečí plynoucí z funkčnosti traťové části ETCS (H_{O6})

- Nebezpečí spočívá buď v možnosti nežádoucího ovlivňování jednotlivých komponent traťové části ETCS sousedními zařízeními, anebo v možnosti nežádoucího ovlivňování sousedních zařízení těmito komponentami (toto ovlivňování může být jak logické, tak fyzické).
- Nebezpečí spočívá v možnosti nežádoucího ovlivňování dvou a více zařízení a z hlediska svého projevu je v nekritičtějším uvažovaném případě shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho6} = THR_{\text{základní nebezpečí}} = 10^{-9}\ h^{-1}}.$$

g) Nebezpečí plynoucí z otázek provozu, údržby a podpory traťové části ETCS (H_{O7})

- Oblast souvisí s běžným komerčním provozem traťové části ETCS (zde přichází do úvahy pouze případné opravy jednotlivých jejích komponent), s údržbou a podporou těchto komponent (tj. s jejich konfigurací, diagnostikou apod.).
- Nebezpečí spočívá v možnosti zranění údržbáře/ky nebo opraváře/ky při provozu nebo údržbě ETCS. V případě chybné podpory (např. nahrání nových, ale chybných konfiguračních dat) lze u tohoto nebezpečí odkázat na nebezpečí plynoucí z rozhraní traťové části ETCS.
- Následky tohoto nebezpečí jsou kritické (v nejhorším uvažovaném případě hrozí újma na zdraví nepředpokládám více než 5 osob současně), proto volím:

$$\underline{THR_{Ho7} = THR_{RAC\text{-}kritick\acute{e}} = 10^{-7}\ h^{-1}}.$$

h) Nebezpečí plynoucí z úvah o likvidaci traťové části ETCS (H_{O8})

- Oblast souvisí s ekologickou likvidací traťové části ETCS, tj. s činnostmi prováděnými po jejím vypnutí a odstavení z provozu.
- Nebezpečí spočívá v možnosti zranění pracovníka provádějícího likvidaci, či poškození životního prostředí při likvidaci.
- Následky tohoto nebezpečí jsou okrajové[25] (v nejhorším uvažovaném případě hrozí ohrožení životního prostředí), proto volím:

$$\underline{THR_{Ho8} = THR_{RAC\text{-}okrajov\acute{e}} = 10^{-6}\ h^{-1}}.$$

i) Nebezpečí plynoucí z lidského činitele (H_{O9})

- Oblast zahrnuje vliv lidského činitele na vývoj, návrh, projekci, výrobu, montáž, provoz a údržbu jednotlivých komponent traťové části ETCS.
- Z hlediska projevu je nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$$\underline{THR_{Ho9} = THR_{z\acute{a}kladn\acute{i}\ nebezpe\check{c}\acute{i}} = 10^{-9}\ h^{-1}}.$$

j) Nebezpečí plynoucí z problémů nemocí z povolání (H_{O10})

- Vzhledem ke skutečnosti, že traťová část ETCS má definováno rozhraní k obsluze (v analyzované aplikaci ETCS L2 jde o komponentu RBC), s nímž je udržující, ale zejména obsluhující pracovník/pracovnice při výkonu služby v kontaktu, může nebezpečí spočívající v možnosti vzniku nemoci z povolání nastat.
- Předpokládá se, že dle směnového plánu se u obslužného pracoviště RBC ETCS bude střídat celkově 5 pracovníků obsluhy; údržba je občasná, tudíž ohrožení pracovníků údržby, resp. servisu do tohoto nebezpečí nezahrnuji.
- Následky tohoto nebezpečí jsou tedy kritické (v nejhorším uvažovaném případě hrozí újma na zdraví nepředpokládám více než 5 osob současně – dle směnového plánu), proto volím:

[25] A to i přesto, že to tab. 4.3 explicitně neuvádí, je to zřejmé z tabulky 3 normy [***126-1***], z níž tato vychází.

$\underline{THR_{Ho10} = THR_{RAC\text{-}kritick\acute{e}} = 10^{-7}\ h^{-1}}$.

k) Nebezpečí plynoucí z mechanických vlivů prostředí (H_{O11})

- Z hlediska projevu je nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$\underline{THR_{Ho11} = THR_{z\acute{a}kladn\acute{i}\ nebezpe\check{c}\acute{i}} = 10^{-9}\ h^{-1}}$.

l) Nebezpečí plynoucí z elektrických vlivů prostředí (H_{O12})

- Z hlediska projevu je nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$\underline{THR_{Ho12} = THR_{z\acute{a}kladn\acute{i}\ nebezpe\check{c}\acute{i}} = 10^{-9}\ h^{-1}}$.

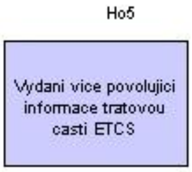
m) Nebezpečí plynoucí z venkovních (klimatických) vlivů prostředí (H_{O13})

- Z hlediska projevu je nebezpečí shodné se základním nebezpečím, tj. vydání více povolující informace, vedoucí k překročení dovolené rychlosti/vzdálenosti.
- Následky tohoto nebezpečí jsou tedy katastrofické (v nejhorším uvažovaném případě hrozí srážka vlaků osobní dopravy), proto:

$\underline{THR_{Ho13} = THR_{z\acute{a}kladn\acute{i}\ nebezpe\check{c}\acute{i}} = 10^{-9}\ h^{-1}}$.

3. Analyzují se jednotlivá výše identifikovaná nebezpečí dle iterativního postupu kombinujícího analýzu FMEA, resp. FMECA a upravenou analýzu FTA [pozn. pro účely této ukázky bude analyzováno pouze jedno vybrané nebezpečí, a to nebezpečí identifikované v oblasti rozhraní traťové části ETCS (viz bod e) – H_{O5})]

I. Provede se kvalitativní část analýzy FTA /tvorba stromu/:

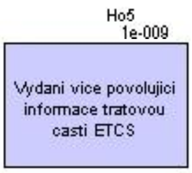


II. Provede se analýza FMEA nebezpečí H_{Oi} (vrcholové události stromu FTA) s použitím formuláře dle kapitoly 5.2.2, v rámci níž se dané nebezpečí analyzuje, zejména se určí jeho bezprostřední příčiny:

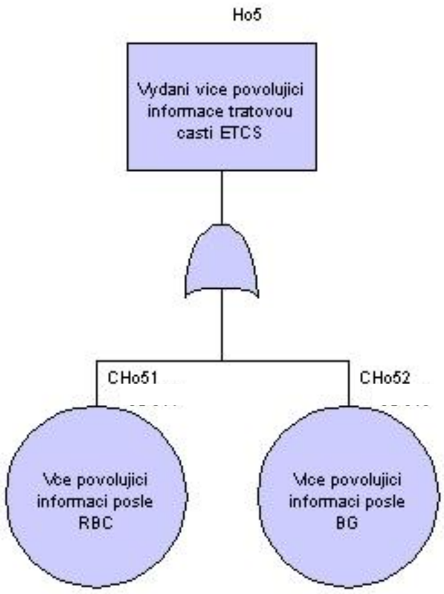
Charakteristika nebezpečí			Důsledky nebezpečí			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	
H_{O5}	Vydání více povolující informace traťovou částí ETCS	poškození: Výstupní zprávy z traťové části ETCS	Traťová část ETCS posílá mobilní části ETCS více povolující informace, než odpovídá reálné situaci na trati	Mobilní část ETCS dohlíží rychlost jízdy vlaku dle více povolující informace	*hazard:* Vlak pod dohledem ETCS může překročit povolenou rychlost a/nebo vzdálenost	Více povolující informaci pošle buď radiobloková centrála ETCS (CH_{O51}) nebo balízová skupina ETCS (CH_{O52})

III. Provede se dělení THR /počátek kvantitativní části analýzy FTA/, které je v této počáteční fázi omezené pouze na stanovení THR vrcholové události H_{O5} (tj. $THR_{TOP-Ho5}$), což bylo již provedeno za použití kritérií RAC z tab. 4.7 v kroku předcházejícím, tedy $THR_{TOP-Ho5} = 10^{-9}\ h^{-1}$.

IV. Provede se kvantitativní část analýzy FTA, zohlednění dělení THR (dle kroku III) do kvalitativní části analýzy FTA (z kroku I):



V. Provede se kvalitativní část analýzy FTA /tvorba stromu/ další úrovně – – využije se přitom příčin identifikovaných v rámci analýzy FMECA z bodu II:



VI. Provede se analýza FMECA jednotlivých nebezpečí CH_{Oi} (základních událostí stromu FTA) s použitím formuláře dle kapitoly 5.2.2, v rámci níž se daná nebezpečí analyzují, zejména se určí jejich bezprostřední příčiny:

Charakteristika nebezpečí			Důsledky nebezpečí			Hodnocení nebezpečí[26]			Příčina/příčiny nebezpečí
číslo	projev	druh	na výstupu traťové části ETCS	na výstupu palubní části ETCS	koncový	závažnost	četnost	riziko	
CH_{O51}	Více povolující informaci pošle RBC	poškození: Funkce RBC generující výstupní informaci (zprávu)	RBC posílá mobilní části ETCS více povolující informace, než odpovídá reálné situaci na trati	Mobilní část ETCS dohlíží rychlost jízdy vlaku dle více povolujících informací	*hazard:* Vlak pod dohledem ETCS může překročit povolenou rychlost a/nebo vzdálenost	katastrofická	častá	nepřípustné	Selže část funkčních algoritmů RBC generující oprávnění k jízdě /msg3/ (CH_{O511}) nebo SR autorizaci /msg2/ (CH_{O512}) nebo příkaz k podmíněnému nouzovému zastavení /msg15/ (CH_{O513}) nebo příkaz k nepodmíněnému nouzovému zastave-

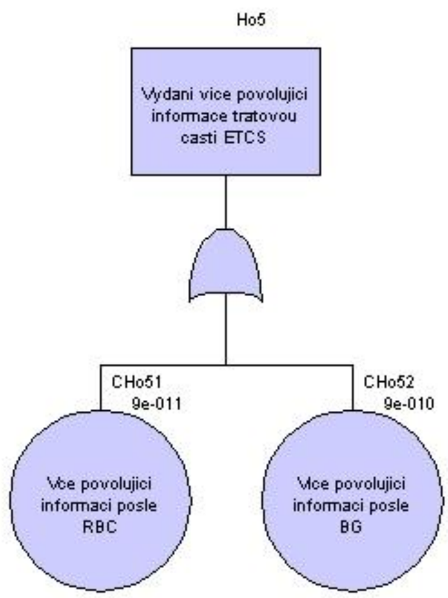
[26] Hodnocení závažnosti a četnosti je zde provedeno, aniž by byla uvažována jakákoli bezpečnostní opatření, jako je použití metod dle [***129***] pro odstranění systematických poruch z návrhu systému, implementované principy technické bezpečnosti apod., s tím, že se uvažuje nejhorší uvažovaný případ. Hodnocení rizik se následně děje dle tab. 4.6.

									ní /msg16/ (CH_{O514}) nebo odvolání příkazu k nouzovému zastavení /msg18/ (CH_{O515})
CH_{O52}	Více povolující informaci pošle BG	poškození: Funkce BG generující výstupní informaci (zprávu)	BG posílá mobilní části ETCS více povolující informace, než odpovídá reálné situaci na trati	Mobilní část ETCS dohlíží rychlost jízdy vlaku dle více povolujících informací	*hazard:* Vlak pod dohledem ETCS může překročit povolenou rychlost a/nebo vzdálenost	katastrofická	častá	nepřípustné	Selže část funkčních algoritmů BG zajišťující přenos zprávy obsahující národní hodnoty /pkt3/ (CH_{O521}) nebo posun zakázán /pkt132/ (CH_{O522})

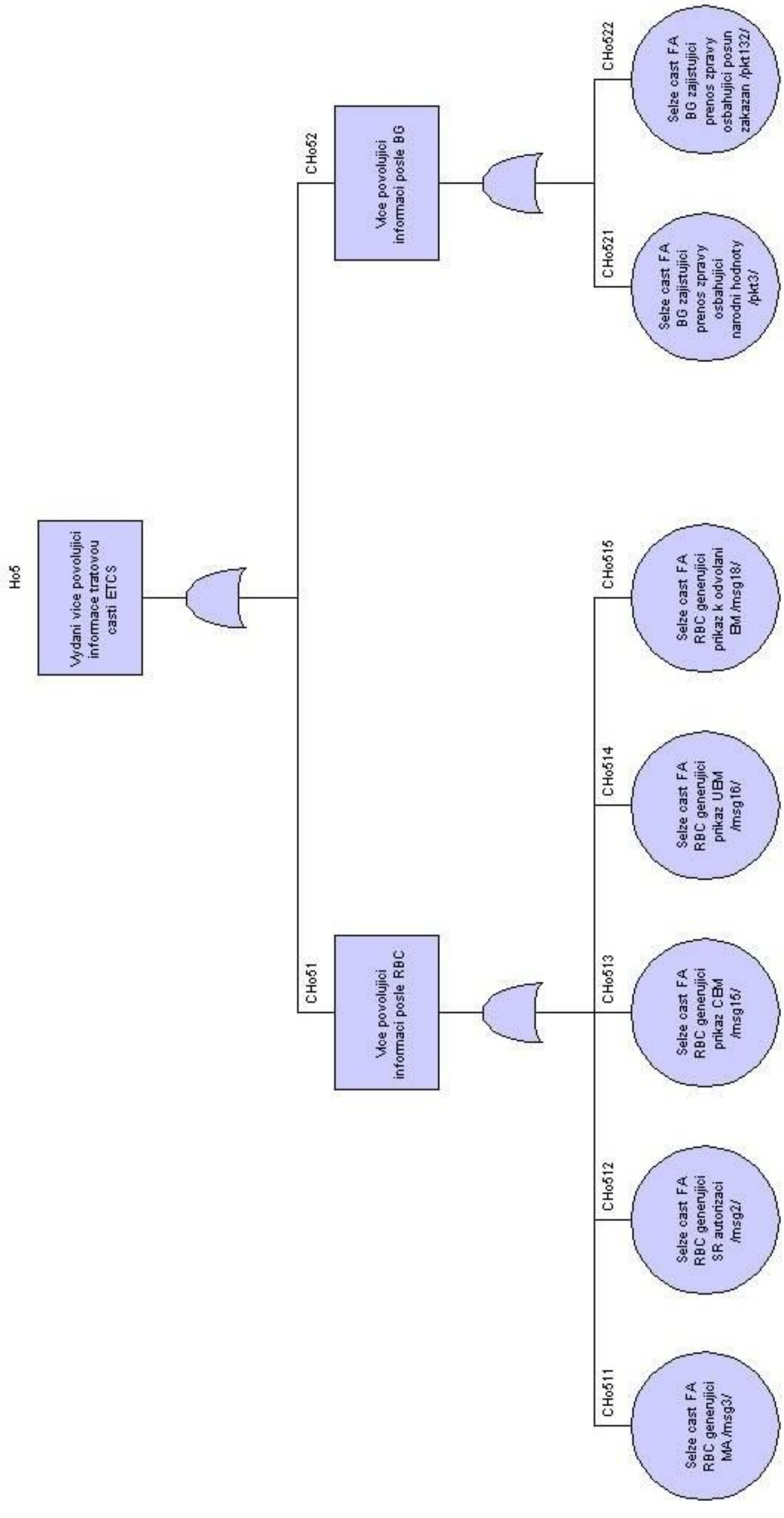
VII. Provede se dělení THR /počátek kvantitativní části analýzy FTA/, čili se provede přiřazení absolutních vah $v_{absCHOik}$ jednotlivým pro danou úroveň základním událostem CH_{Oijk} a výpočet $THR_{TOP\text{-}CHOi}$ mezi tyto události CH_{Oij} (kde $j \in \{1;...;n\}$, kde n je počet příčin nebezpečí Hoi) stromu FTA dle postupu uvedeného v kapitole 5.3.4, čímž se získají THR_{CHOik} jednotlivých základních událostí.

H_{O5}	Vydání více povolující informace traťovou částí ETCS				10^{-9}
ID	Popis nebezpečí (nebezpečné události)	Abs. váha	Rel. váha	Norm. váha	THR [h^{-1}]
CH_{O51}	Více povolující informaci pošle RBC	10	0,09	0,09	9.10^{-11}
CH_{O51}	Více povolující informaci pošle BG	1	0,91	0,91	9.10^{-10}

VIII. Provede se kvantitativní část analýzy FTA – zohlednění dělení THR (dle kroku 0) do kvalitativní části analýzy FTA (z kroku I):



IX. Provede se kvalitativní část analýzy FTA další úrovně – využije se přitom příčin identifikovaných v rámci analýzy FMECA z bodu VI:



X. Opakují se kroky VI až IX, dokud se nedosáhne požadované úrovně podrobnosti dekompozice daného systému.

4. Stanoví se dle bodu 3 odvozené bezpečnostní požadavky:
Z analýzy rizika traťové části ETCS provedené pro 3. etapu životního cyklu dle [***126-1***] výše vyplynuly následující bezpečnostní požadavky na funkce a vstupní informace:

1) Bezpečnostní požadavky na funkce traťové části ETCS

Funkce traťové části ETCS	Požadavek na		Plyne z nebezpečí
	THR	SIL	
Část funkčních algoritmů RBC generující oprávnění k jízdě /msg3/	$1{,}09.10^{-11}$	SIL 4	CH_{O511}
Část funkčních algoritmů RBC generující SR autorizaci /msg2/	$1{,}89.10^{-11}$	SIL 4	CH_{O512}
Část funkčních algoritmů RBC generující příkaz k podmíněnému nouzovému zastavení /msg15/	$2{,}01.10^{-11}$	SIL 4	CH_{O513}
Část funkčních algoritmů RBC generující příkaz k nepodmíněnému nouzovému zastavení /msg16/	$2{,}13.10^{-11}$	SIL 4	CH_{O514}
Část funkčních algoritmů RBC generující odvolání příkazu k nouzovému zastavení /msg18/	$1{,}89.10^{-11}$	SIL 4	CH_{O515}
Část funkčních algoritmů BG zajišťující přenos zprávy obsahující národní hodnoty /pkt3/	$8{,}71.10^{-10}$	SIL 4	CH_{O521}
Selže část funkčních algoritmů BG zajišťující přenos zprávy obsahující posun zakázán /pkt132/	$2{,}9.10^{-11}$	SIL 4	CH_{O522}

Poznámka: Při dělení THR, jímž jsem došel k hodnotám výše, jsem předpokládal následující vektory absolutních vah: $\overrightarrow{v_{absB2CHo51}} = (10, 3, 2, 1, 3)$ *a* $\overrightarrow{v_{absB2CHo52}} = (1, 30)$.

2) Bezpečnostní požadavky na vstupní informace traťové části ETCS

Vstupní informace IRI	Požadavek na		Plyne z nebezpečí
	THR	SIL	
V tomto ilustrativním příkladě nebylo analyzováno	*NR*	*NR*	*NR*

Poznámka: Bezpečnostní požadavky na vstupní informace traťové části ETCS by představovaly exportované požadavky částečně na zabezpečení přenosu těchto informací, částečně na funkční vlastnosti zabezpečovacích systémů, jenž tyto informace vytvářejí.