prof. Ing. Karol Rástočný, PhD.
Katedra riadiacich a informačných systémov
Elektrotechnická fakulta, Žilinská univerzita v Žiline
Univerzitná 1 *Tel.: ++421/41/5133320*
01 026 Žilina *E-mail.: karol.rastocny@fel.uniza.sk*

Oponentský posudok doktorandskej dizertačnej práce

Názov dizertačnej práce: ***Analýza rizika aplikace systému ETCS***
Autor dizertačnej práce: ***Ing. Jakub Marek***

1. Aktuálnosť danej témy

V súčasnom období prebieha v rámci Európy rozsiahla modernizácia železničných zabezpečovacích systémov, ktorá je spojená aj s aplikáciou systému ETCS. Základnými cieľmi tejto modernizácie je zaistenie interoperability železničnej dopravy a zvýšenie bezpečnosti cestujúcich. Riziko, ktoré znáša cestujúci, by malo byť rovnaké a nezávislé od toho, v ktorej krajine sa nachádza. Objektivizácia analýzy rizika a s ňou súvisiace definovanie bezpečnostných požiadaviek na zabezpečovací systém je v súčasnosti veľmi problematická. Síce na európskej úrovni existujú bezpečnostné štandardy, ktoré určujú pravidlá, ako treba postupovať pri definovaní bezpečnostných funkcií a z nich vyplývajúcich bezpečnostných požiadaviek, ale tieto pravidlá sú definované len všeobecne. Cieľom tejto dizertačnej práce je navrhnúť a odporučiť postup, ktorý by uvedené nedostatky v čo najväčšej miere eliminoval. Preto tému tejto dizertačnej práce považujem za aktuálnu a vhodnú.

2. Splnenie cieľa práce

Doktorand ciele svojej dizertačnej práce sformuloval do štyroch bodov (I. až IV.). V bodoch I. až III. sú definované úlohy súvisiace s postupom pri analýze rizika, s výberom vhodných metód a ich prispôsobením na tento účel. Bod IV. súvisí so zovšeobecnením získaných výsledkov, tak aby sa dali použiť aj v iných bezpečnostne kritických aplikáciách. Cieľ práce je jasne definovaný a poskytuje dostatočný priestor na preukázanie vedeckých a odborných schopností doktoranda. Oprávnene možno očakávať, že splnenie vytýčeného cieľa bude mať prínos pre prax a pre ďalší rozvoj vedy a techniky.

Konštatujem, že uvedený cieľ bol splnený. Zdôvodnenie tohto tvrdenia je uvedené v 3. a 4. bode tohto posudku.

3. Zvolené metódy spracovania

V práci sú uvedené rôzne metódy a techniky (FTA, ETA, HAZOP, ...), ktoré doktorand považuje za vhodné na dosiahnutie stanovených cieľov. Ide všetko o metódy, ktoré sa bežne v praxi už dlhodobo používajú. Aby sa tieto metódy dali použiť pri analýze rizika, treba ich prispôsobiť špeciálne pre daný účel. Preto doktorand na základe hodnotenia pozitív aj negatív týchto metód a na základe požiadaviek analýzy rizika, prispôsobil metódy FTA, FMEA a FMECA, tak aby boli použiteľné pri analýze rizika (kap. 5.) – ide o splnenie jedného s cieľov práce.

4. Dosiahnuté výsledky

Treba poznamenať, že ciele vytýčené doktorandom sú veľmi ambiciózne a ich dôsledné splnenie by si vyžiadalo dlhodobú prácu väčšej skupiny ľudí. Tento fakt beriem do úvahy pri hodnotení dosiahnutých výsledkov.

Doktorand na základe podrobnej analýzy týchto v súčasnosti platných noriem, predpisov a smerníc pre železničné aplikácie (kap. 1.) dospel k záverom, že tieto dokumenty obsahujú nejednotnú terminológiu, v mnohých prípadoch aj nejednotný prístup k analýze

rizika a spravidla definujú „čo“ treba urobiť, ale nedávajú jasný návod „ako“ to treba urobiť. Tieto zistenia doložil aj citáciami z týchto dokumentov. Tu sa jasne preukázala schopnosť doktoranda formulovať svoje názory a aj ich podporiť vhodnou argumentáciou. Návod, ako sa s týmito nejednoznačnými požiadavkami noriem vyrovnať, dáva doktorand v kap. 4.1.3., kde prezentuje svoj vlastný prístup k analýze rizika, ktorý je podrobnejšie rozpracovaný v kap. 4.3. V kap. 6. doktorand sumarizuje čiastkové výsledky svojej práce uvedené v predchádzajúcich kapitolách a poskytuje komplexný návod na analýzu rizika, čo sa týka postupu a použitia navrhnutých metód v rámci analýzy rizika. Praktické použitie navrhnutej metodiky a ním upravených metód prezentoval na analýze rizika traťovej časti aplikácie systému ETCS (Príloha č. 5).

Výsledky svojej práce doktorand publikoval v zborníkoch z vedeckých konferencií, resp. sympózií (10). Rozsah jeho publikačnej činnosti považujem za primeraný.

5. Prínos pre prax a pre ďalší rozvoj vedy a techniky

Dizertačná práca svojim zameraním, cieľmi a spôsobom riešenia je priamo predurčená na použitie pri vývoji zabezpečovacích zariadení. Fakt, že autor práce je členom riešiteľského tímu spoločnosti AŽD Praha s. r. o., ktorý sa zaoberá vývojom komponentov ETCS, sa pozitívne odrazil na kvalite práce a vytvára veľmi dobré predpoklady na prenos dosiahnutých výsledkov do praxe.

Ide o pomerne rozsiahlu, veľmi zaujímavú a užitočnú prácu nie len pre prax, ale aj pre ďalšie vedecké bádanie. Bolo by vhodné, aby táto práca bola podrobená prísnej kritike (v dobrom slova zmysle) a na jej základoch bola vypracovaná nová (vylepšená) metodika na analýzu rizika.

6. Pripomienky k práci a otázky na autora práce

Práca svojim rozsahom riešených problémov evokuje k veľkému množstvu otázok, námetov do diskusie, resp. pripomienok. V tejto časti uvádzam len tie podstatné.

1. Doktorand sa pri riešení zadaných úloh snažil o striktné dodržiavanie noriem, predpisov a smerníc, ktoré sa viažu na železničné aplikácie. Jeho prístup chápem, pretože chcel, aby navrhnutá metodika bola nie len dobrá, ale aj praxou akceptovaná a v praxi použiteľná (takýto prístup je priamo podporovaný aj názvom práce). Ale tiež treba brať do úvahy aj fakt, že analýza rizika nie je špecifická záležitosť len pre železnice a že je predmetom záujmu aj v iných aplikačných oblastiach s bezpečnostne kritickými procesmi. Tým sa „ochudobnil“ o rôzne ďalšie podnetné nápady. Typickým príkladom toho je fakt, že doktorand sa pri analýze rizika zameral na také rizikové faktory ako je početnosť výskytu nebezpečenstiev a ich následky (úplne v zhode s uvažovanými normami; str. 10, vzťah (1.1)), ale nebral do úvahy ďalšie faktory ovplyvňujúce veľkosť rizika, napríklad čas trvania nebezpečenstva.
2. Analýzu rizika možno realizovať na dvoch úrovniach. Buď sa analyzuje len riziko súvisiace s riadeným procesom (ešte nie sú aplikované opatrenia na zníženie rizika; cieľom je definovanie bezpečnostných funkcií a bezpečnostných požiadaviek; ide o 3. etapu životného cyklu v zmysle normy EN 50126-1) alebo sa analyzuje riziko sústavy riadiaci (zabezpečovací) systém – riadený systém (už sú aplikované opatrenia na zníženie rizika; cieľom je kontrola dostatočnosti aplikovaných opatrení; ide o etapy nasledujúce po 3. etape životného cyklu v zmysle normy EN 50126-1). Navrhnutá metodika medzi týmto prístupmi k analýze rizika nerozlišuje.

3. Kap. 3. obsahuje metódy, ktoré sa dajú použiť na analýzu nebezpečenstiev, prípadne na určenie ich početnosti výskytu a ich následkov. Na výpočet (odhad rizika) treba použiť iné metódy (nie sú uvedené).
4. Str. 72 – úvahy doktoranda formulované v komentári považujem za diskutabilné. Podľa môjho názoru je situovanie traťovej elektronickej jednotky (LEU) mimo súčasť ETCS (obr. 4.6.), z pohľadu analýzy rizika, správne.
5. Kap. 4.3.3. – prečo pri určovaní intenzity výskytu nebezpečenstva sa uvažuje s časom 20 rokov? Môžu sa nebezpečenstvá vyskytovať aj počas vývoja systému?
6. Tab. 4.2 – prvý a druhý riadok tabuľky uvádza rovnakú kvantifikáciu intenzity nebezpečenstva. Je to správne? Na základe akej matematickej úvahy ste dospeli k tvrdeniu o zhodnosti údajov pre pravdepodobnosť a intenzitu?
7. Tab. 4.3 – s kritikou predpisu súhlasím, ale tento kritický postoj sa už nepremietol do obsahu tabuľky. Tabuľka v princípe nerozlišuje medzi závažnosťou humánnych škôd. Napr. 4 smrteľné úrazy by boli rovnako hodnotené ako 4 zranenia – rozumiem tomu správne?
8. Tab. 4.5 – vychádza zo štatistických údajov o nehodách, ktoré vznikli už pri existencii opatrení na minimalizáciu rizika (existencie zabezpečovacích zariadení). Možno na základe týchto údajov, bez podrobnejšej analýzy príčin mimoriadnych udalostí, formulovať závery smerom k prijateľnosti rizika?
9. Tab. 4. 6, tab. 4.7 – aký je vzťah medzi RAC a THR? Pre konkrétne nebezpečenstvo sa pomocou tab. 4.6 určí RAC. Ako sa od nebezpečenstva prejde k bezpečnostnej funkcii? Čo znamenajú skratky S1, S2, S3, S4?
10. Str. 86 (posledný odsek) – nesúhlasím s interpretáciou vzťahu medzi SIL a THR. SIL môže byť vyjadrená kvalitatívne aj kvantitatívne (podľa toho či ide o integritu proti náhodným poruchám alebo o integritu proti systematickým poruchám). Kvantitatívne je SIL vyjadrovaná prostredníctvom THR.
11. Str. 87 (komentár k citácii normy) – domnievam sa, že postupy navrhované v predmetnej norme sú správne. Tiež sa domnievam sa, že zo strany doktoranda došlo k zámene medzi pojmami bezpečnostná funkcia a bezpečnostná požiadavka a tým aj k nesprávnej interpretácii obsahu citácie. Na základe analýzy rizika treba definovať bezpečnostné funkcie a k nim prislúchajúce THR a tieto ďalej rozpracovať na bezpečnostné požiadavky.
12. Str. 105, časť III. odsek c) – zlyhanie (ii) určitej funkcie môže mať za následok napríklad zranenie (iv). Je prípustná takáto kumulácia dvoch následkov?
13. Str. 108 – výpočet intenzity vrcholovej udalosti. Ako si treba vysvetliť prvú vetu o platnosti vzorcov? Ako treba postupovať, ak nebezpečenstvo na vyššej úrovni môže nastať, ak súčasne nastanú dve nebezpečenstvá na nižšej úrovni (vznikne potreba aplikovať operátor AND)?
14. Ku kvalite práce by určite prospelo, ak by navrhnuté metódy a postupy boli verifikované prípadne aspoň konfrontované s postupmi, ktoré boli použité pracovnou skupinou UNISIG RAMS WP pre ETCS na úrovni generického produktu. V Prílohe č. 5 je síce ukážka použitia navrhovanej metodiky, ale bez vyhodnotenia dosiahnutých výsledkov.

Žiadam doktoranda, aby sa počas obhajoby doktorandskej práce vyjadril k otázkam a pripomienkam uvedeným pod bodmi 5, 6, 7, 8 a 9.

Cieľom tejto časti posudku nie je moja snaha o zníženie kvality predloženej práce (prácu doktoranda si veľmi vážim), ale upozorniť autora práce na niektoré problémy, ak sa bude ďalej venovať problematike analýzy rizika.

7. Záverečné zhodnotenie

Na základe už uvedených faktov konštatujem, že doktorand preukázal schopnosť samostatne vedecky a tvorivo pracovať. Prácu hodnotím pozitívne a stanovené ciele považujem za splnené. Práca formálne spĺňa požiadavky kladené na doktorandské dizertačné práce a je prínosom pre ďalší rozvoj študijného odboru Dopravní prostředky a infrastruktura. Prácu **odporúčam na obhajobu** a po jej úspešnej obhajobe odporúčam udeliť pánovi **Ing. Jakubovi Marekovi** akademický titul

doktor (Ph.D.)

v študijnom odbore **Dopravní prostředky a infrastruktura.**

V Žiline dňa 17. 03. 2014 prof. Ing. Karol Rástočný, PhD.