FAKULTA ELEKTROTECHNICKÁ
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

POSUDEK OPONENTA DISERTAČNÍ PRÁCE

Assessment of the Doctoral Thesis

Titul, jméno a příjmení studenta: Title, name, surname of student	**Ing. Luděk Elis**
Doktorský studijní program: Doctoral study programme	**Elektrotechnika a informatika**
Studijní obor: Study branch	**Elektronika**
Téma disertační práce: Topic of the disseration	**Řídicí systémy se zvýšenou bezpečností**
Školitel: Supervisor	doc. Ing. Jiří Skála, Ph.D.
Oponent: Opponent	doc. Ing. Pavel Fuchs, CSc.

Zhodnocení významu disertační práce pro obor
Evaluation of the importance of the dissertation for the field

Disertační práce přináší pro obor přínosná v tom, že srozumitelným způsobem transponuje složitou problematiku funkční bezpečnosti do metodického postupu pro návrh řídicích systémů, jejichž bezpečnostní funkce by měly splňovat požadavky na zadanou úroveň integrity bezpečnosti. Evidentním přínosem je tedy metodika, aby projektant ze složité struktury normy pochopil, co má dělat. Právě toto pochopení mnohdy projektantům řídicích systémů schází. V mnoha případech v praxi přistupují projektanti k návrhu řídicího systému, který vykonává bezpečnostní funkce, intuitivně. To vede k tomu, že při konfrontaci s požadavky zákazníka, nejsou schopni prokazovat požadovanou úroveň integrity bezpečnosti. Náprava pak vyžaduje přepracování návrhu, systematické dokladování všech postupů jednotlivých fází/etap životního cyklu řídicího systému a ve svém důsledku vede k prodražování projektu a nedodržení smluvních termínů předání řídicího systému zákazníkovi.
Disertační práce je tedy v tomto případě rozhodně přínosná, protože kromě systematického rozboru problematiky funkční bezpečnosti a zpracování metodiky také tuto metodiku aplikuje na návrhu řídicího systému.

Vyjádření k postupu řešení problému, použitým metodám a splnění určeného cíle
Evaluation of the the problem-solving process, the methods used and the goal to be met

Pro řešení problému byl využit postup spočívající v systematickém prostudování souboru norem na funkční bezpečnost E/E/PE systémů (ČSN EN 61508-x) a norem spojených s funkční bezpečností v dalších oborech. Na základě analýzy poznatků z norem pak byla provedena syntéza, jejímž výsledkem je navržená metodika. Ověření metodiky proběhlo formou její aplikace na návrh řídicího systému REMCS. Na základě konfrontace metodických postupů s procesy probíhajícími při reálném návrhu a vývoji řídicího systémy bylo možné tyto procesy modifikovat a zároveň příslušné poznatky zohlednit i v metodice.
Jako určitý nedostatek shledávám, že není více popsán stav oboru, tedy jak se funkční bezpečnost aplikuje v ČR a v zahraničí. Chápu, že firmy omezují přístup ke know-how, ale existuje značné množství příspěvků na mezinárodních vědeckých a odborných konferencích, ze kterých lze čerpat a lépe popsat stav oboru.

Stanovisko k výsledkům disertační práce a k původnímu konkrétnímu přínosu předkladatele disertační práce
Statement to the results of the dissertation and on the original contribution of the submitter of the dissertation

Pro tuto práci byly stanoveny následující dílčí cíle (cituji):

- zpracování problematiky návrhu systémů pracujících se stanovenou úrovní bezpečnosti

s ohledem na základní požadavky normy ČSN EN 61508,
- sjednocení názvů, pojmů a používaných metod a analýz v oblasti funkční a technické bezpečnosti,
- vytvoření metodické příručky návrhu bezpečných systémů dle obecného standardu série normy ČSN EN 61508,
- modelová ukázka použití metodiky na praktickém příkladu.

Všechny uvedené dílčí cíle byly v plném rozsahu splněny. Z předložené práce je zřejmé, že se jedná o práci původní a její vytvoření vyžadovalo značné pracovní úsilí doktoranda a schopnost pochopit do hloubky procesy návrhu bezpečnostních systémů.
Připomínku mám k zavádějícímu názvu disertační práce "Řídicí systémy se zvýšenou bezpečností", jelikož podstatnou a velmi přínosnou částí je metodika. Kdyby se k tomu dal podtitul např. "Metodika pro návrh", bylo by hned patrné, že jde o tvůrčí transformaci obecných postupů do praktické roviny.

Vyjádření k systematice, přehlednosti, formální úpravě a jazykové úrovni disertační práce
Statement to the systematics, clarity, formal adaptation and language level of the dissertation

Práce má uspřádanou strukturu, která vychází z logického postupu řešení. Avšak tato struktura není v souladu se směrnicí děkana fakulty (Příloha č. 11 směrnice děkana č. 2D/2019). Vzhledem k tomu, že směrnice je datována k roku 2019 a já nejsem obeznámen s předchozími požadavky fakulty na strukturu disertačních prací, zdržím se dalšího porovnávání struktury disertační práce s požadavky směrnice.
Z hlediska výkladu problematiky funkční bezpečnosti a její transpozice do metodiky a ověření při návrhu řídicího systému, považuji strukturu práce za velmi dobrou.
Formální úprava práce je velmi dobrá, texty, tabulky a obrázky jsou srozumitelné.
Jazyková úroveň disertační práce je velmi dobrá, syntaxe a srozumitelnost projevu je výborná.

Vyjádření k publikacím studenta
Statement to student's publications

Z přehledu autorových publikací je zřejmé, že převážná část publikační činnosti proběhla v rámci akcí ZČU v Plzni. Publikační činnost na zahraničních konferencích je v menšině. Bohatě dokumentovaná je autorova činnost v oblasti prototypů a funkčních vzorků. To potvrzuje orientaci autora na aplikační část VaV aktivit.

Celkové zhodnocení a otázky k obhajobě
Total evaluation and questions for defence

Práci hodnotím jako velmi přínosnou pro praxi. Teoretické poznatky v aplikaci norem se nevyskytují. Praktické dopady práce do návrhu spolehlivého řídicího systému jsou však nesporné.
Dotaz 1: V tab. 1 (SIL) se používají různé míry poruch – PFD avg/PFH. Jaký je mezi nimi rozdíl a proč by použití PFH pro režim s nízkým vyžádáním nebylo vhodné?
Dotaz 2: Na obr. 19 (graf rizik) se určuje potřebná SIL. Věříte, že ten postup je správný? Uveďte důvody proč je, nebo není, správný.

Doporučuji disertační práci k obhajobě
I recommend the dissertation for the defence

ano
yes

Datum
Date

11. 8. 2019

Podpis oponenta:
Signature of opponent

FAKULTA
ELEKTROTECHNICKÁ
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

POSUDEK OPONENTA DISERTAČNÍ PRÁCE

Assessment of the Doctoral Thesis

Titul, jméno a příjmení studenta: Title, name, surname of student	**Ing. Luděk Elis**
Doktorský studijní program: Doctoral study programme	**Elektrotechnika a informatika**
Studijní obor: Study branch	**Elektronika**
Téma disertační práce: Topic of the disseration	**Řídicí systémy se zvýšenou bezpečností**
Školitel: Supervisor	Doc. Ing. Jiří Skála, Ph.D.
Oponent: Opponent	prof. Ing. Karol Rástočný, PhD.

Zhodnocení významu disertační práce pro obor
Evaluation of the importance of the dissertation for the field

Dizertačná práca je venovaná problematike bezpečnosti technických systémov. V bežnej praxi bola bezpečnosť technických systémov, a teda aj riadiacich systémov, donedávna považovaná za okrajový problém a pozornosť sa sústreďovala najmä na funkčné vlastnosti riadiacich systémov. V ostatnom čase sa čoraz častejšie možno stretnúť s požiadavkou na riadiace systémy, ktoré dokážu eliminovať riziko súvisiace s riadeným procesom. Dôvodom je fakt, že riadiace systémy čím ďalej tým viac preberajú úlohy riadenia, ktoré vykonával obslužný persomál a tieto úlohy sú čoraz komplikovanejšie. Existujú prípady, keď zlyhanie riadiaceho systému môže byť príčinou nehody a to aj s fatálnymi následkami. Preto pokladám každý prínos k rozpracovaniu metód na znižovanie rizika súvisiaceho s vývojom riadiacich systémov a metód na hodnotenie bezpečnosti riadiacich systémov za veľmi významný.

Vyjádření k postupu řešení problému, použitým metodám a splnění určeného cíle
Evaluation of the the problem-solving process, the methods used and the goal to be met

Hlavný cieľ dizertačnej práce je orientovaný najmä na návrh metodiky použiteľnej pri návrhu systému súvisiaceho s bezpečnosťou (SRS) a na jej aplikáciu pri návrhu konkrétneho riadiaceho systému. Uvedený cieľ je veľmi ambiciózny a jeho dôsledné splnenie by si vyžiadalo dlhodobú prácu väčšej skupiny ľudí. Tento fakt som bral do úvahy pri hodnotení dosiahnutých výsledkov.
Doktorand riešenie zadanej úlohy založil na analýze normy ČSN EN 61508. Táto norma sa zaoberá problematikou funkčnej bezpečnosti E/E/EP systémov súvisiacich s bezpečnosťou a definuje aktivity pre jednotlivé fázy životného cyklu (LC), ale v mnohých prípadoch len principiálne. Preto nie je jednoduché túto normu pochopiť a správne aplikovať.
Doktorand v práci analyzoval aktivity definované normou ČSN EN 61508, pričom postupoval metodicky po jednotlivých fázach životného cyklu SRS - od počiatočnej fázy (Koncept) ku konečnej fáze (Vyradenie z prevádzky a likvidácia). Pre jednotlivé fázy uvádza základné informácie týkajúce sa postupov, ktoré treba použiť, aby sa splnili požadované úlohy. Pozitívne hodnotím snahu doktoranda previazať aktivity jednotlivých fáz tak, aby na seba nadväzovali. Aj keď táto časť práce je pomerne rozsiahla (kap. 3.; str. 32 až str. 116) splnenie tejto úlohy by si vyžiadalo výrazne väčší priestor. Predpokladám, že doktorand tieto svoje poznatky a skúsenosti využil pri tvorbe, resp. úprave interných smerníc organizácie RICE (Regionální inovační centrum elektrotechniky), ktoré sú použiteľné pri vývoji SRS.
Praktické použitie časti tejto metodiky doktorand prezentoval v kap. 4. (Aplikace metodiky pro návrh systému kompenzace zemních spojení).
Konštatujem, že uvedený cieľ doktorand splnil.

Stanovisko k výsledkům disertační práce a k původnímu konkrétnímu přínosu předkladatele disertační práce
Statement to the results of the dissertation and on the original contribution of the submitter of the dissertation

Výsledkom práce vývojového tímu, ktorého súčasťou bol aj doktorand, je systém REMCS (Modulární řídicí systém), ktorý bude nasadený do skúšobnej prevádzky v rozvodni spoločnosti ČEZ Kralovice. Hlavnou úlohou doktoranda pri vývoji systému REMCS bola realizácia bezpečnostných analýz (ide o analýzu rizika a kvantitatívne hodnotenie integrity bezpečnosti hardvéru). Preto pri hodnotení výsledkov práce doktoranda som sa sústredil najmä na tie časti práce, ktoré súvisia s uvedenými aktivitami.
Pri bezpečnostných analýzach systému REMCS doktorand postupoval v zhode s metodikou uvedenou v teoretickej časti práce; t. j. definoval systém a vymedzil hranice jeho pôsobnosti, urobil jeho dekompozíciu a vyčlenil časti súvisiace s bezpečnosťou, analyzoval riziko, definoval opatrenia na zníženie rizika a overil dostatočnosť navrhnutých opatrení.
Pri analýze rizika vychádzal z predpokladu, že k dispozícii je už existujúci systém REMCS (čo nie je v rozpore s odporúčanými postupmi pri vývoji SRS, aj keď vo všeobecnosti nejde o štandardný postup, ale v tomto prípade je takýto prístup vhodný) a analyzoval riziká súvisiace s prevádzkou tohto systému. Identifikoval jednotlivé nebezpečenstvá a dôsledky súvisiace s výskytom jednotlivých nebezpečenstiev. Odhad rizika realizoval pomocou metódy ALARP. Na určenie požadovanej SIL pre bezpečnostnú funkciu použil metódu označovanú ako Diagram rizika. S výberom metód a spôsobom ich aplikácie možno súhlasiť. Aj keď doktorand si bol vedomý problémov súvisiacich s nejednotnou a nejednoznačnou terminológiou (str. 12), tak v tejto časti práce sa týmto problémom nevyhol, čo spôsobilo, že terminologicky pôsobí táto časť práce zmätočne.
Na analýzu dôsledkov porúch na integritu bezpečnosti systému REMCS použil metódu FMEA, resp. jej derivát FMECA. Svojou podstatou sú to kvalitatívne metódy. Keďže ide o elektronický systém, odporúčal by som radšej použiť niektorú so štandardne používaných kvantitatívnych metód (napr. RBD, FTA) a metódu FMEA použiť len ako doplnkovú metódu. V prípade elektronických prvkov je veľmi problematické (až nemožné) zostaviť pre tieto prvky zoznam porúch. Vhodnosť použitej architektúry doktorand overil pomocou výpočtu *SSF* (*Safe Failure Fraction*) a následným určením tolerancie danej architektúry proti poruchovým stavom hardvéru. Aplikáciu týchto metód a postupov považujem za správnu. K výsledkom analýzy sa však, vzhľadom na obmedzený rozsah informácií, nedokážem vyjadriť.

Vyjádření k systematice, přehlednosti, formální úpravě a jazykové úrovni disertační práce
Statement to the systematics, clarity, formal adaptation and language level of the dissertation

Práca je napísaná na primeranej odbornej úrovni. Po formálnej a grafickej stránke práca spĺňa kritériá kladené na dizertačné práce. Občas sa v práci vyskytujú formálne a logické nepresnosti. Pre ilustráciu uvádzam niektoré z nich:

- Str. 25: Tvrdenie uvedené pod tabuľkou 1, ktoré vyjadruje vzťah medzi *PFD* a *PFH* je nepresné a zavádzajúce.
- Str. 27: Normy ČSN EN 50159-1 a ČSN EN 50159-2 boli nahradené normou ČSN EN 50159 (účinnosť od 09/2011).
- Str. 42: Tvrdenie „Výstupem 2. fáze LC (definice systému) je podrobná dokumentace systému …“ je nesprávne. V tejto fáze LC ešte systém neexistuje.
- Str. 43, obr. 10.: Označenie „Zbytkové riziko“ je v jednom prípade použité nesprávne.
- Str. 43 – 44: Vysvetlenie pojmov Riziko a Nebezpečí je nepresné a zavádzajúce (pozn.: otázka k obhajobe).
- Str. 45. obr. 11.: Výsledkom procesu aplikácie opatrení na minimalizáciu rizika nie je akceptovateľné riziko (to musí vyť vopred dané), ale zostatkové riziko. Obdobne aj na obr. 12.
- Str. 57, obr. 18.: Rozdelenie oblasti ALARP na dve oblasti (prípustnú a prijateľnú) považujem za nevhodné a tvrdenie „Následně je pro každé riziko odhadnuta četnost jeho výskytu a očekávaný následek.“ za nesprávne.
- Str. 60, obr. 19.: Nie je vysvetlený význam označenia „a“, „b“.

- Str. 81, obr. 28. a obr. 29.: V bloku 10.1 sú uvedené dve rovnaké aktivity (nemá byť jedna z nich špecifikácia integrity bezpečnosti?)
- Str. 84, obr. 31.; str. 85, obr. 32.: Nesprávne odkazy na obr. 36. a obr. 37.
- Str. 104 – 105: Vzťahy (3.7) a (3.8) sú správne, ale ich vysvetlenie je nesprávne, pretože v (3.7) ide o pravdepodobnosť a v (3.8) o frekvenciu.
- Str. 106 – 107: Vzťahy na výpočet *PFD* (3.10) až (3.18) a tiež vzťahy na výpočet *PFH* (3.19) až (3.23) sú prebrané z normy ČSN EN 61508-6. Niektoré z nich sú však uvedené chybne.

Tieto pripomienky nie sú však zásadného charakteru a nespochybňujú dosiahnuté výsledky.

Vyjádření k publikacím studenta
Statement to student's publications

Zoznam publikačných prác doktoranda obsahuje 19 titulov už publikovaných prác a 2 tituly pripravovaných publikácií. Ide o publikácie z obdobia rokov 2012 až 2019. Z názvov týchto prác som usúdil, že minimálne 7 z nich priamo súvisí s témou dizertačnej práce. Dá sa predpokladať, že ďalšie publikácie budú nasledovať ako výstupy tejto dizertačnej práce.
Doktorand tiež uvádza účasť na tvorbe 44 funkčných vzorov a prototypov, čo svedčí aj o jeho praktickej zručnosti.
Publikačnú činnosť doktoranda považujem za dostatočnú na to, aby som predloženú dizertačnú prácu odporučil k obhajobe.

Celkové zhodnocení a otázky k obhajobě
Total evaluation and questions for defence

Predložená dizertačná práca zodpovedá požiadavkám na práce tohto typu. Práca celkovo vyznieva pozitívne a je prínosom pre ďalší rozvoj študijného odboru Elektronika.
Práca sa zaoberá veľmi rozsiahlou problematikou a problémy každej fázy životného cyklu môžu byť námetom na rozsiahlu diskusiu. Prácu odporúčam k obhajobe a žiadam doktoranda, aby sa pri obhajobe vyjadril k týmto otázkam:
1. V čom zásadnom sa odlišuje Vaša metodika návrhu systému súvisiaceho s bezpečnosťou od metodiky uvedenej v ČSN EN 61508, resp. v čom zásadnom ju dopĺňa?
2. Boli pri vývoji systému REMCS zistené nejaké nedostatky v smernici (smerniciach) pre vývoji systému súvisiaceho s bezpečnosťou, ktoré sú uplatňované v rámci RICE? Ak áno, tak prosím, uveďte nejaké príklady.
3. Faktom je, že diagnostické vlastnosti (spôsob diagnostiky, čas diagnostiky, diagnostické pokrytie) systému môžu mať výrazný vplyv na jeho integritu bezpečnosti. Napr. kontrolná skúška (periodická skúška, tzv. proof test) môže byť dokonalá alebo nedokonalá. Ako sa táto vlastnosť kontrolnej skúšky prejaví na priebehu *PFD*, resp. *PFH* (väzba na obr. 45.)?
4. Na základe čoho bol stanovený interval periodickej skúšky (2 x za rok; str. 125)? Faktom je, že pri stanovení tohto intervalu treba brať do úvahy aj požiadavky zákazníka a odporúčania výrobcov použitých komponentov, ale tiež treba brať do úvahy aj výsledky analýzy bezpečnosti (dopad technických a prevádzkových vlastností systému na *PFH*). Ako ste preukázali, že takýto interval periodickej skúšky je vyhovujúci vzhľadom na požadovanú SIL?
5. Ako chápete vzťah medzi nebezpečenstvom (nebezpečím), nebezpečnou udalosťou, rizikom, bezpečnostnou funkciou, integritou bezpečnosti systému a úrovňou integrity bezpečnosti (SIL)?
6. Vysvetlite, ako ste postupovali pri definovaní poruchových módov pre jednotlivé bloky systému a rozdelení intenzity porúch na jednotlivé jej časti vzhľadom na výpočet *SFF*.

Doporučuji disertační práci k obhajobě
I recommend the dissertation for the defence

ano yes	

Datum
Date **08. 08. 2019**

Podpis oponenta:
Signature of opponent