VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Oponentní posudek disertační práce

Uchazeč: Ing. Jakub Arm

Název disertační práce: Detekce anomálií běhu RTOS aplikace

Oponent: doc. Ing. Petr Blecha, Ph.D.

Pracoviště oponenta: VUT v Brně, FSI, ÚVSSR

Oponent se v posudku vyjádří dle Studijního a zkušebního řádu VUT zejména:
a) k aktuálnosti tématu disertační práce,
b) zda disertační práce splnila stanovený cíl,
c) k postupu řešení problému a k výsledkům disertační práce s uvedením konkrétního přínosu doktoranda,
d) k významu pro praxi nebo rozvoj oboru,
e) k formální úpravě disertační práce a její jazykové úrovni,
f) zda disertační práce splňuje podmínky uvedené v § 47 odst. 4 zákona,
g) zda student prokázal nebo neprokázal tvůrčí schopnosti v dané oblasti výzkumu a zda práce splňuje nebo nesplňuje požadavky standardně kladené na disertační práce v daném oboru. Bez tohoto závěru je posudek neplatný.
Ke každému z níže uvedených bodů je nutno doplnit stručný komentář.

Ad a) Aktuálnost tématu disertační práce

Téma disertační práce je velmi aktuální.

Komentář:
Práce je zaměřena na zlepšování diagnostického pokrytí anomálií vzniklých při běhu operačního systému reálného času (RTOS). Včasná identifikace nebezpečných chyb v reálném čase má u běžícího programu velký vliv na úroveň funkční bezpečnosti řízeného objektu. Jedná se o problematiku, jejíž aktuální správná technická praxe je popsána pouze na obecné úrovni v ČSN EN 61508-3 ed. 2:2011 a ČSN EN 61508-7 ed. 2:2011. Se vzrůstajícími požadavky na komplexní bezpečnost řízených zařízení (EUC) jsou inženýři stavěni před problém zvyšování úrovně integrované bezpečnosti (SIL) softwaru implementovaného do hardwaru. U systematických chyb je možné zvyšovat úroveň integrované bezpečnosti důsledným managementem kvality návrhu SW a HW. U náhodných chyb je potom jedinou možností zvyšování SIL zlepšování diagnostického pokrytí. V této oblasti ale zatím žádná správná technická praxe neexistuje a zvolené metody je nezbytné opřít o postupy osvědčené v praxi nebo o výsledky vědecké práce.

Ad b) Splnění stanoveného cíle disertační práce

Cíl disertační práce byl splněn.

Komentář:
Obecným cílem práce bylo přinést zlepšení v oblasti funkční bezpečnosti operačního systému reálného času, který umožňuje okamžitě reagovat na události týkající se řízeného objektu. Z celé řady aspektů ovlivňujících funkční bezpečnost se doktorand soustředil na verifikaci softwarového vybavení za jeho běhu na základě modelu sestaveného z návrhových vzorů. Vytyčený cíl doplnil doktorand čtyřmi hypotézami (kapitola 1.3), které v závěru (kapitola 10.1) vyhodnotil vzhledem k dosaženým výsledkům disertační práce. S vyhodnocením hypotéz souhlasím a konstatuji, že byl cíl disertační práce splněn.

Ad c) Postup řešení problému a výsledky disertační práce s uvedením konkrétního přínosu doktoranda

Postup řešení problému a výsledky disertační práce jsou vynikající.

Komentář:
Řešená problematika v disertační práci je velmi rozsáhlá a existuje celá řada doporučených a velmi doporučených přístupů k dosažení požadované úrovně integrované bezpečnosti SW. Této skutečnosti odpovídá i prostor, který doktorand věnoval teoretické části disertační práce. Na základě analýz dostupných postupů a řešení vytvořil návrh kontrolního běhu SW aplikace (kapitola 8) pro jasně vymezený kontext architektury a zamýšlené cíle (aspekty), kterou následně implementoval do HW kontrolního modulu za účelem prvotního ověření funkčnosti dosaženého výsledku (kapitola 9). Podrobně jsou vlastní přínosy doktoranda popsány v kapitole 10.2.

Ad d) Význam pro praxi nebo rozvoj oboru

Význam pro praxi nebo rozvoj oboru je průměrný.

Komentář:
Očekávané využití dosaženého výsledku lze předpokládat u softwarového vybavení programovatelných prostředků průmyslové automatizace. Proto, aby mohl být dosažený výsledek použit v průmyslové praxi, je nutné jej implementovat do správné technické praxe nezbytné pro úspěšnou certifikaci bezpečnostního SW. Jak uvádí doktorand v kapitole 2.2, vytyčené cíle práce byly orientovány na akademické účely, nikoliv potřeby praxe. Tomu odpovídá i míra rešerše vztažené k řadě norem ČSN EN 61508 ed.2:2011.

Ad e) Formální úprava disertační práce a její jazyková úroveň

Formální úprava disertační práce a její jazyková úroveň jsou průměrné.

Komentář:
Po jazykové stránce obsahuje disertační práce jen nepatrné množství překlepů. V seznamu citované literatury nejsou uvedeny normy, na které se doktorand odkazuje. Zároveň tyto odkazy na normy nejsou ve formátu umožňujícím identifikovat vydání normy, na které se doktorand odkazuje (např. IEC 61508 na str. 11 a 14, ČSN ISO 12100 na str. 20 nebo ČSN ISO 13849-1 na str. 20 – správně by mělo být např. řada norem IEC 61508:2010 nebo ČSN EN 61508 ed. 2:2011, ČSN **EN** ISO 12100:2011 a ČSN **EN** ISO 13849-1:2017). Text v kapitole 2.2.1 neobsahuje některá slova významná z pohledu definice pojmů – například analýza a posouzení rizik – 4. řádek zdola, novotvary jako imunita proti poruchám nebo řízení procesu funkční bezpečnosti. Definice vyplývající z ČSN jsou odkazovány na nezdrojové dokumenty, např. citace [65] na str. 21. nebo Safe Failure Fraction jako zbytkové riziko dle IEC 61508 (správně podíl bezpečných chyb) na str. 22, jakožto i další originální překlady anglických termínů vedou společně s neuspořádaným a nekompletním seznamem použitých zkratek k zhoršené orientaci v napsaném textu.

Ad f) Disertační práce splňuje podmínky uvedené v § 47 odst. 4 zákona

Disertační práce podmínky uvedené v § 47 odst. 4*) zákona č. 111/1998 sb. o vysokých školách splňuje.

((4) Studium se řádně ukončuje státní doktorskou zkouškou a obhajobou disertační práce, kterými se prokazuje schopnost a připravenost k samostatné činnosti v oblasti výzkumu nebo vývoje nebo k samostatné teoretické a tvůrčí umělecké činnosti. Disertační práce musí obsahovat původní a uveřejněné výsledky nebo výsledky přijaté k uveřejnění.*

Ad g) Prokázání tvůrčí schopnosti studenta v dané oblasti výzkumu, a zda práce splňuje nebo nesplňuje požadavky standardně kladené na disertační práce v daném oboru.

Doktorand prokázal tvůrčí schopnosti v dané oblasti výzkumu a práce splňuje požadavky standardně kladené na disertační práce v daném oboru.

Komentář:
Disertační práce obsahuje všechny prvky vědeckého textu, je založena na více jak 150 citovaných dokumentech a obsahuje vlastní originální výsledky autora, které byly publikovány na vědeckých fórech.

Celkové hodnocení:

Dle mého názoru předložená disertační práce „Detekce anomálií běhu RTOS aplikace" uchazeče Ing. Jakuba Arma i přes uvedené připomínky odpovídá obecně uznávaným požadavkům k udělení akademického titulu „Doktor" (ve zkratce Ph.D.).

Otázky oponenta:

1) Vysvětlete Vaše tvrzení, proč zařízení RTOS nemohou z hlediska funkční bezpečnosti dosahovat úrovně integrované bezpečnosti SIL 4 (viz str. 88 třetí odstavec).
2) Které semi-formální metody by bylo možné použít pro dosažení úrovně integrované bezpečnosti SIL3?
3) Popište, jak se může výsledek vaší disertační práce uplatnit v praxi v rámci doporučeného postupu a metod dle ČSN EN 61508-3 ed. 2:2011 respektive ČSN EN 61508-7 ed. 2:2011.

Disertační práci k obhajobě ☒**doporučuji** ☐**nedoporučuji.**

Dne: 23.10.2020

Pod