



Hodnocení vedoucího závěrečné práce

Vedoucí práce: Ing. Martin Daňhel, Ph.D.
Student: Martin Mandík
Název práce: Analýza TPM komunikace za pomoci FPGA
Obor / specializace: Bezpečnost a informační technologie
Vytvořeno dne: 9. června 2022

Hodnotící kritéria

1. Splnění zadání

- ▶ [1] zadání splněno
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Práce se zabývá návrhem HW zařízení realizovaného na FPGA, autor použil vývojový kit Basys 3. Navržené zařízení slouží k vyčítání provozu na LPC sběrnici a konkrétně se jedná o komunikaci čipu TPM. Student navržené zařízení řádně otestoval (nejen pomocí klasických simulačních technik, ale také pomocí dalšího HW, který si sám realizoval prostřednictvím kitu Arduino). Datovou analýzu student prováděl na dodaných datech. Zadání práce považuji za splněné bez výhrad, neboť výstupem je nejen navržený HW, ale i zachycený klíč.

2. Písemná část práce

95 /100 (A)

Bakalářská práce je psaná v anglickém jazyce, text je pochopitelný pro cílovou skupinu čtenářů, a navíc se práce velmi dobře čte.

Rozsahem má práce dostatečných 52 stran textu včetně doprovodných obrázků a ukázek kódu.

Práce se skládá ze 7 kapitol včetně úvodu a závěru, které na sebe logicky navazují. Dále jsou k textu práce přidruženy 3 přílohy – kde za zmínku stojí příloha A. Zde se nacházejí popsané větší fragmenty kódu v jazyce Verilog.

Text práce obsahuje dostatečné množství informací o navrhovaném HW, nicméně občas by neškodilo některé pasáže přeci jen více rozepsat, za účelem pochubit se vlastním řešením, např. podrobnější rozkreslení/popsání konečného automatu, bližší vysvětlení jednotlivých signálů apod.

Bakalářská práce dále obsahuje značné množství relevantních zdrojů, které student správně cituje a dostatečně je odděluje od výsledků své vlastní práce.

3. Nepísemná část, přílohy

93 /100 (A)

Praktickým výstupem bakalářské práce je HW design, který je řádně otestován a pro který si student mimo zadání navrhl i vlastní testovací zařízení pomocí vývojového kitu Arduino. Tento přístup velmi oceňuji, vzhledem k tomu, že zaměření studenta není číslicový návrh, musel se věnovat studiu jazyka Verilog, ve kterém je celá HW část implementována.

Dalším výstupem této práce je analýza naměřených (zachycených) dat, na tomto místě je však dobré podotknout, že student analyzoval pouze předem specifikovanou výseč (kterou si specifikoval "na tvrdo" v návrhu FPGA) ze všech naměřených dat.

4. Hodnocení výsledků, jejich využitelnost

94 /100 (A)

Výstupem práce je funkční FPGA design, který slouží k vyčítání TPM čipu po LPC sběrnici. V době vzniku této práce se jednalo o velmi zajímavé téma zvláště s příchodem operačního systému MS Windows 11. Samotná práce byla míněna spíš jako pilotní projekt, kde jsme chtěli ověřit, jak moc je pracné a zda je vůbec možné vyčíst data z čipu TPM a pokusit se je částečně analyzovat, s tím že cílem bylo získat klíč Volume Master Key nástroje BitLocker. Jelikož se tento pokus povedl považuji výsledek práce za funkční produkt.

5. Aktivita studenta

- ▶ [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

Aktivita studenta byla výborná a příkladná, pravidelně se zúčastňoval dohodnutých konzultací, kde předkládal dílčí řešení. Zde bych rád vyzdvihl proaktivní činnost, kdy na řešení práce začal pracovat ještě před jejím vlastním zadáním, aby se ujistil, že má k dispozici potřebný HW a vývojové nástroje.

6. Samostatnost studenta

- ▶ [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Samostatnost studenta byla výborná a příkladná. Zejména oceňuji fakt, že si student hledal sám možnosti, jak práci zlepšit, např. články na téma TPM a MS Windows 11 či testování výsledného návrhu pomocí Arduino externí desky, kterou bylo nutno připravit.

Celkové hodnocení

95 /100 (A)

Pan Martin Mandík předvedl, že je schopen plnit úkoly na patřičné úrovni a v patřičné kvalitě a plně splnil zadání práce. Vzhledem k výše uvedenému práci doporučuji k obhajobě a hodnotím známkou A - výborně.

Instrukce

Splnění zadání

Posudte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posudte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posudte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posudte schopnost studenta samostatně tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.