Posudek oponenta na diplomovou práci

Název práce: **Message authentication for CAN bus and AUTOSAR software architecture**

Student: Bc. Ondřej Kulatý

Oponent: Ing. Ondřej Hynčica

Předložená práce se zabývá implementací protokolu MaCAN (Message authenticated CAN) do mikrokontrolérové platformy ARM se systémem AUTOSAR. Student se v rámci práce zabýval problematikou komunikace po sběrnici CAN, informační bezpečností komunikace a architekturou systému AUTOSAR. Související problematika je velmi široká, student provedl podrobné nastudování i analýzu a vše podrobně zdokumentoval. Dále provedl úpravy již realizované knihovny pro implementaci MaCAN protokolu, vytvořil ovladač pro systém AUTOSAR, který tuto knihovnu využívá, a provedl ověření funkčnosti vytvořeného řešení. Zadání diplomové práce tedy bylo splněno v plném rozsahu.

Diplomová práce je psána v anglickém jazyce, na vysoké jazykové úrovni, je přehledně členěna, problematika je podrobně a srozumitelně popsána. V textu jsem objevil pouze několik překlepů, především přebývající neurčité členy. Rozsah práce je spíše větší, než je obvyklé, ale velkou část práce zabírá podrobný popis konfigurace a implementace řešení, který bude velmi cenný pro další navazující práce. Použité zdroje jsou v práci uvedeny a citovány v dostatečném rozsahu.

Po odborné stránce student prokázal dobrou orientaci v problematice a velmi kladně hodnotím, že se zorientoval v rozsáhlých zdrojových kódech a konfiguraci MaCAN knihovny a především pak systému AUTOSAR. Samotná vlastní práce studenta – tedy programování vlastního kódu nebo provedení testů je spíše menšího rozsahu. Vytknul bych použití přímého přístupu k periferiím procesoru z CDD modulu MACAN odporující architektuře AUTOSAR, který byl ale zvolen pouze pro zjednodušení (jak student v práci vysvětluje). Další výtka se týká provedených testů náročnosti protokolu MaCAN oproti běžné CAN komunikaci, což byl jeden z bodů zadání diplomové práce. Analýza je zaměřena pouze na paměťové nároky (pouze data, nikoli programové paměti) a měření času vykonávání kryptografických funkcí (bez uvedení rozlišení měření nebo podrobnějšího popisu). Očekával bych srovnání pro implementaci v systému AUTOSAR, například dobu odezvy nebo propustnost s/bez modulu protokolu MaCAN.

I přes uvedené připomínky považuji předloženou diplomovou práci rozsahem a zpracováním za velmi zdařilou a navrhuji hodnocení **výborně/A**.

V Brně dne 13.1.2014 Ing. Ondřej Hynčica