Posudek vedoucího diplomové práce

Autor práce: Bc. Ondřej Kulatý
Název práce: Message authentication for CAN bus and AUTOSAR software architecture
Vedoucí: Ing. Michal Sojka, Ph.D.

V poslední době se do médií stále častěji dostávají zprávy o tom, že zabezpečení řídicích a komunikačních systémů automobilů proti nežádoucím zásahům má svá slabá místa. Zejména u automobilů vyšších tříd, kde je hodně elektroniky a „vše komunikuje se vším" existuje velké riziko napadení auta hackery. Diplomová práce pana Kulatého je součástí počínající snahy automobilového průmyslu tato rizika eliminovat.

Na začátku práce student převzal již existující implementaci protokolu MaCAN a úkolem bylo pokračovat v jejím vývoji – zejména na odstraňování chyb a zajištění kompatibility s jinou implementací od firmy Volkswagen. Na základě této práce pak bylo vytvořeno demo, které je nyní používáno firmou Volkswagen k internímu marketingu jako ukázka toho, že je možné protokol implementovat i na méně výkonných procesorech požívaných v automobilových řídicích jednotkách.

Druhá část práce spočívala v integraci protokolu do architektury AUTOSAR, která definuje strukturu softwaru pro řídicí jednotky aut. Zde bylo obtížné jak nastudování celé rozsáhlé architektury a nalezení vhodného místa pro začlenění nového modulu MaCAN, tak ověření funkčnosti v konkrétní implementaci AUTOSARu. Výsledkem byla opět funkční demonstrační aplikace.

Student pracoval poměrně samostatně. Aktivně se podílel na sehnání vhodného hardwaru k zapůjčení pro účely testování a na tento hardware pak samostatně naportoval implementaci protokolu MaCAN. Na konzultace chodil student připraven a řídil se radami vedoucího. Drobnou komplikací pro mě byla menší komunikativnost studenta, která měla za následek, že jsem si někdy nebyl jist, jestli student porozuměl tomu, o čem jsme se bavili. Na další konzultaci se ale vždy ukázalo, že všemu porozuměl.

Další výtku bych měl k časovému rozvržení prací. Po dokončení první části práce se aktivita studenta snížila a vypadalo to, že kvalita druhé části bude nevalná. Jsem rád, že jsme se dohodli na prodloužení studia a odevzdání až o semestr později. Na kvalitě výsledku se to projevilo zásadním způsobem. Samotný text práce je velmi dobrý a bude možné jej přímo poskytnout našim průmyslovým partnerům, se kterými na této problematice spolupracujeme.

Část práce (cca dva měsíce) probíhala formou placené prázdninové brigády. Práci navrhuji hodnotit stupněm A – **výborně**.

V Praze dne 16. ledna 2015

Ing. Michal Sojka, Ph.D.
katedra řídicí techniky

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