



Hodnocení diplomové práce oponentem

Název práce:	Návrh úložiště kryptografických klíčů protokolu EURORADIO pro železniční zabezpečovací zařízení		
Student:	Bc. Pavel ŠMEJKAL	Std. číslo:	
Oponent:	Milan Pidrman		

Kritéria hodnocení práce oponentem	Max. body	Přidělené body
Splnění zadání práce (posuzuje se i stupeň kvality splnění)	25	13
Odborná úroveň práce	50	40
Interpretace výsledků a jejich diskuze, příp. aplikace	15	10
Formální zpracování práce, dodržování norem	10	10

Hodnocení obsahu a kvality práce, připomínky:

- Práce je srozumitelná a dobře čitelná.
- V teoretické části DP jsou popsány základní principy klíčového managementu protokolu EURORADIO v souladu se subsety 037, 038, 114 ERTMS.
- První polovina závěru práce vyznívá spíše jako úvod práce.
- Praktická část obsahuje některé nesrovnalosti, na které poukazují dotazy k práci.
- V práci kompletně chybí celkové schéma, kde by bylo vidět zapojení i druhého MCU a jeho propojení s hlavním MCU, jeho paměti a také chybí zapojení druhého USB rozhraní a další obvody.
- Použitý obvod FT232BL nedisponuje funkcí USB host, která by umožňovala připojení USB flash disku jakožto periférie, ale jedná se o USB/UART(fifo) převodník, který očekává na straně USB host port. Tento obvod by neumožňoval zápis a čtení souborů na flash disku.

Dotazy oponenta k práci:

- 1) Bude navržený systém skutečně pracovat jako 1 ze 2 i pokud přestane pracovat hlavní MCU a pomocný MCU tím pádem nebude mít přístup k USB rozhraní pro offline zavádění klíčů? Proč každý MCU neobsluhuje své USB rozhraní, ale obě USB rozhraní jsou připojena jen ke hlavnímu MCU (viz 5.2 odst. 2, str 49)?
- 2) Jaký jiný typ IO, např. od firmy FTDI, by měl být použit pro řešení připojení USB flash disku?
- 3) Není odhadovaná cena modulu v závěru práce příliš nízká? Jaká je např. reálná cena jen MCU nebo výroby DPS?
- 4) Jakým způsobem se generuje hodinový signál pro MCU, pokud není ve schématu připojen žádný krystal ani oscilátor k MCU?

Diplomovou práci hodnotím klasifikací **velmi dobře** (podle klasifikační stupnice dané směrnicí děkana FEL)

Dne: 15.5.2012

Pidrman

.....
podpis oponenta práce