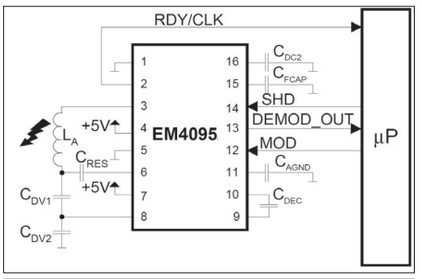
Laboratoř RFID

Při zkoumání bezpečnosti RFID se bez, byť skromné, laboratoře neobejdeme. Dokumentace čipů je totiž často neúplná a sázet na zaručená prohlášení obchodníků je jistou cestou do pekla. Nezbývá proto než ověřovat některé hypotézy vlastními experimenty, na což obvykle zbývá málo času. Správný integrovaný obvod ve správnou chvíli tak mívá cenu zlata. Zde si konkrétně představíme obvody pro pásmo LF (100–150 kHz), které jsme si vypůjčili z pražského ASICentra (www.asicentrum.cz).

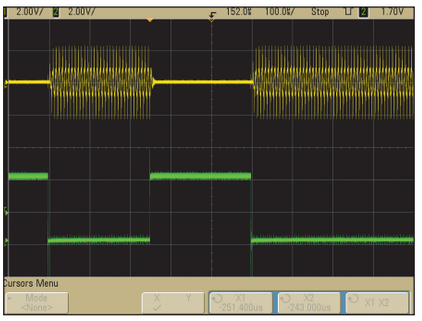
EM4095

Obvod s předpokládaným napájením 4,1–5,5 V je určen pro terminály (slangově čtečky) komunikující s transpondéry RFID, a to jak v jednosměrném, tak také v obousměrném módu. Jeho účelem je spolu s minimem okolních součástek obstarat pro řídicí procesor veškeré analogové aspekty takové komunikace. Naše stručné seznámení provedeme tak, že si okomentujeme typické zapojení z *obr. 1*. Pro připojení procesoru slouží digitální signály SHD, MOD, RDY/CLK a DEMOD_OUT. První dva jsou z pohledu EM4095 vstupní, ostatní výstupní. Sémantika rozhraní je velmi jednoduchá a opírá se o okamžité úrovně jednotlivých signálů. To prakticky umožňuje připojit i jednodušší logiku, než je mikroprocesor, neboť se zcela obejdeme bez přenosů jako SPI, atp. Vstup SHD umožňuje deaktivaci obvodu a přechod do režimu spánku. Vstupem MOD se ovládá modulátor základní nosné (*obr. 2*). Prvoplánovým režimem je 100 % AM, jednoduchou změnou zapojení (viz [1]) lze docílit v zásadě libovolné hloubky modulace. Na výstupu RDY/CLK je k dispozici hodinový signál o frekvenci základní nosné, který je sfázován s buzením anténního obvodu. Na DEMOD_OUT je vyveden digitalizovaný výstup demodulátoru AM (*obr. 3*). Podrobnější popis řízení obvodu viz [1] a [2].

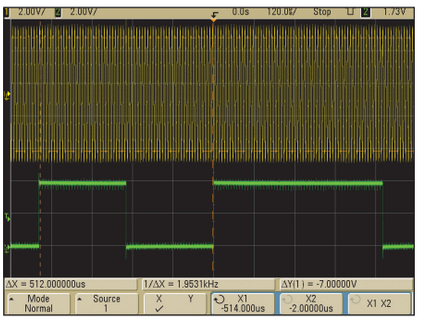
Z analogových pinů si zde všimneme těch s čísly 3, 6 a 8. První dva slouží k buzení magnetické antény v podobě sériového LC článku. Doporučená zátěž je max. 250 mA, v případě potřeby lze pochopitelně připojit tranzistorový posilovač. Osmička je vstup, na který se přes kapacitní dělič přivádí napětí z antény sbírané na rezonančním kondenzátoru. Uvnitř EM4095 zde pracuje jednak demodulátor AM (citlivost 0,85 mV_{pp}) připravující data pro DEMOD_OUT, jednak zpětná vazba fázového závěsu, který generuje signál pro buzení antény a také pro výstup RDY/CLK. Využití fázového závěsu namísto oscilátoru s pevně danou frekvencí zbavuje konstruktéra nutnosti starat se o vyladění antény na konkrétní frekvenci. Stačí se trefit do rozsahu 100–150 kHz a fázový závěs si ji už „najde“. Rovněž tak jsou tím ošetřeny drobné provozní odchylky parametrů antény.



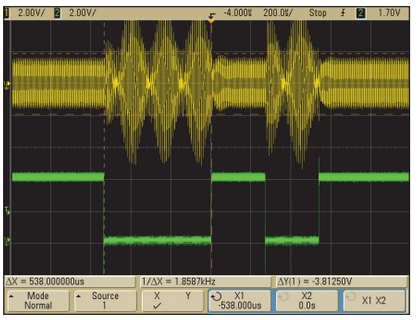
Obr. 1 Typické zapojení EM4095 pro čtení/zápis [1]



Obr. 2 Příklad klíčování nosné (žlutě)



Obr. 3 Výstup demodulátoru (zeleně)



Obr. 4 Zázněje při pokusu o aktivní emulaci (žlutě)

Všechny zbývající výpočty periferních součástek (kondenzátory v děliči, jakost antény, atp.) jsou v [2] předzpracovány tak, aby je zvládl každý zkušenější uživatel kalkulačky.

Kódování přenášených dat (v obou směrech) nechává EM4095 již na řídicím procesoru. Předpokládá se pouze, že finálními modulacemi jsou AM základní nosné pro data čtečky a zátěžová AM pro data transpondéru. Mimoto zde může existovat několikero kódování, pomocných nosných, atp. Pozor je třeba ještě dát na šířku pásma. Vzhledem k tomu, že obvod je primárně určen pro transpondéry EM, začíná podle [2] demodulátor už mezi cca 12 kHz až 20 kHz zřetelně tlumit. Nicméně například s obvody HID na 125 kHz vyžadujícími přenést alespoň 15,625 kHz jsme problémy neměli (ST 9/2008).

Režim odposlechu

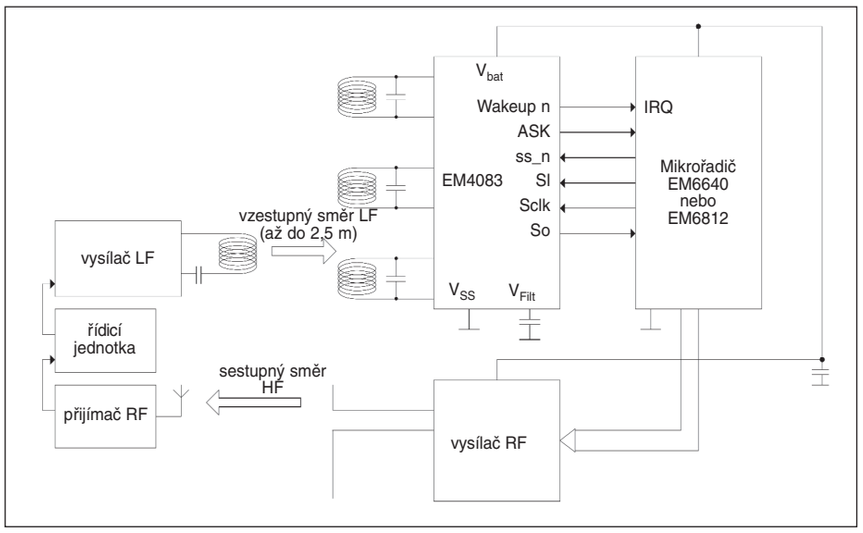
Jedná se o nestandardní režim, který se výborně hodí právě k laboratorním experimentům, neboť umožňuje odposlech komunikace mezi transpondérem a jinou čtečkou. Vlastně jde o další příjemný důsledek použití fázového závěsu. Nám se osvědčilo hned nejjednodušší zapojení: Anténu jsme odpojili od pinů 3, 6 a zapojili ji jako paralelní rezonanční obvod, ze kterého jsme odebírali napětí pro kapacitní dělič na vstup 8. Pak už jen fázový závěs s demodulátorem udělaly, co měly. Na výstupu RDY/CLK se objevily hodiny sledující základní nosnou přijímanou z pole druhé čtečky, a na DEMOD_OUT byl demodulovaný digitální signál transpondéru. Situaci zkomplikuje, pokud potřebujeme odposlouchávat komunikaci obousměrnou. Hlubší modulace základní nosné poslouchané čtečky totiž způsobuje očekávatelné výpadky závěsu. Zde lze doporučit sledovat signál z antény samostatným detektorem sloužícím jen pro čtení dat čtečky. K ošetření vazby závěsu (delší výpadek ohrožuje příjem rychlé odpovědi transpondéru) navrhujeme při výpadku externí nosné nastavit MOD = H. Vedlejším efektem tohoto pokusu o klíčování odpojeného(!) budiče antény je podle [1] konzervace nastavení závěsu. Hodiny na RDY/CLK přitom pokračují dál. Po naběhnutí nosné a uvolnění MOD je vazba zase obnovena.

Dále jsme zkoušeli použít EM4095 k emulaci transpondéru. Teoreticky by zátěžová modulace transpondéru měla jít nahradit aktivním vysíláním modulovaného signálu. Jak ale ukazuje *obr. 4*, není to tak jednoduché. Zde jasně vidíme, že sebemenší odchylka nosné hlavní čtečky od nosné emulátoru způsobí v poli vznik nežádoucích záznějí. Náš skromný experiment ukazuje, že v praxi bude nutné nosnou emulátoru maximálně potlačit a vysílat jen postranní pásma AM. Pro takové

operace se ovšem mnohem víc hodí pásmo HF. Ne náhodou jsou proto úspěšné pokusy tohoto druhu hlášeny právě odtud.

EM4083

Tento obvod si zatím představíme jen krátce. Jeho hlavní doménou jsou aktivní transpondéry podle *obr. 5*. Data do transpondéru jsou zasílána klasickou LF čtečkou, odpovědi pak putují přes spoj v pásmu HF či UHF (obstarává jiný modul). Pro příjem dat ze čtečky je obvod vybaven třemi nezávislými anténními okruhy umožňujícími připojení tří separátních magnetických antén pokrývajících co nejlépe okolí zamýšleného transpondéru. Na vývojovém přípravku EMDB403 je pro tento účel k dispozici 3D feritová anténa v provedení SMD. EM4083 umožňuje digitálně řízené ladění rezonanční frekvence a jakosti jednotlivých okruhů pomocí příznaků ve vnitřní paměti EEPROM. Po restartu obvod periodicky poslouchá jednotlivé antény a snaží se detekovat základní nosnou nějaké LF čtečky v okolí. Jakmile ji najde, uzamkne přijímací cestu na konkrétní anténu a začne vyhledávat spouštěcí bajt (tento krok lze přeskočit). Po jeho zachycení aktivuje signál probouzející připojenou řídicí jednotku a přejde do režimu kontinuálního sériového příjmu dat ze čtečky. Pro veškerý datový přenos je předpokládána 100% AM s kódováním manchester rychlostí 4 kbps. Toto je ovšem požadavek standardního zapojení. Podobně jako EM4095 je i EM4083 díky své koncepci velmi univerzální, takže pokud oželíme pomocné datové hodiny generované pro výše uvedené přenosové schéma, můžeme možnosti kódování a rychlosti podstatně rozšířit.



Obr. 5 Aktivní transpondér s EM4083 [3]

Z hlediska bezpečnosti je velmi zajímavá schopnost obvodu přijímat data LF čtečky (100% AM) až na vzdálenost několika metrů [3]. Díky nezávislému napájení aktivního transpondéru totiž nyní z pole čtečky stačí zachytit již jen zlomek intenzity nutný toliko pro správnou funkci citlivého přijímače (1 mV_{pp}). Stranou původního účelu se tak obvod výborně hodí pro dálkový (metry) odposlech hesel zasílaných často v otevřeném tvaru ze čtečky do transpondéru, atp. Doufáme, že pro tuto pozoruhodnou schopnost najdeme brzy nějaké zajímavé uplatnění.

Závěr

Obvody švýcarské firmy EM Microelectronic, jejíž součástí je i ASICentrum, jsou kromě jiného zajímavé svou univerzálností a schopností pracovat spolehlivě i za poněkud nestandardních podmínek. To je přesně to, co v naší skromné laboratoři potřebujeme.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, tomas.rosa@rb.cz

LITERATURA

[1] EM4095 – Read/Write analog front end for 125 kHz RFID Basestation, EM Microelectronic-Marin SA, SWATCH Group, 2001.
[2] EM4095 – Application Note 404, EM Microelectronic-Marin SA, SWATCH Group, 2006.
[3] EM4083 – 3D Active Long Range Front-End, EM Microelectronic-Marin SA, SWATCH Group, 2003.
[4] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz