Laboratorní práce - zabezpečení datových přenosů pomocí CRC

Tým: Skupina č.4 - středa 14:30 - 16:00 (Lukáš Cafourek, Daniela Lukešová, Hlib Bunin)

Úkol: Seznámení s detekčními vlastnostmi CRC a ověření jeho spolehlivosti

Pomůcky: Program Matlab, dvě simulační schémata (CRC a Bernoulli)

Postup měření:

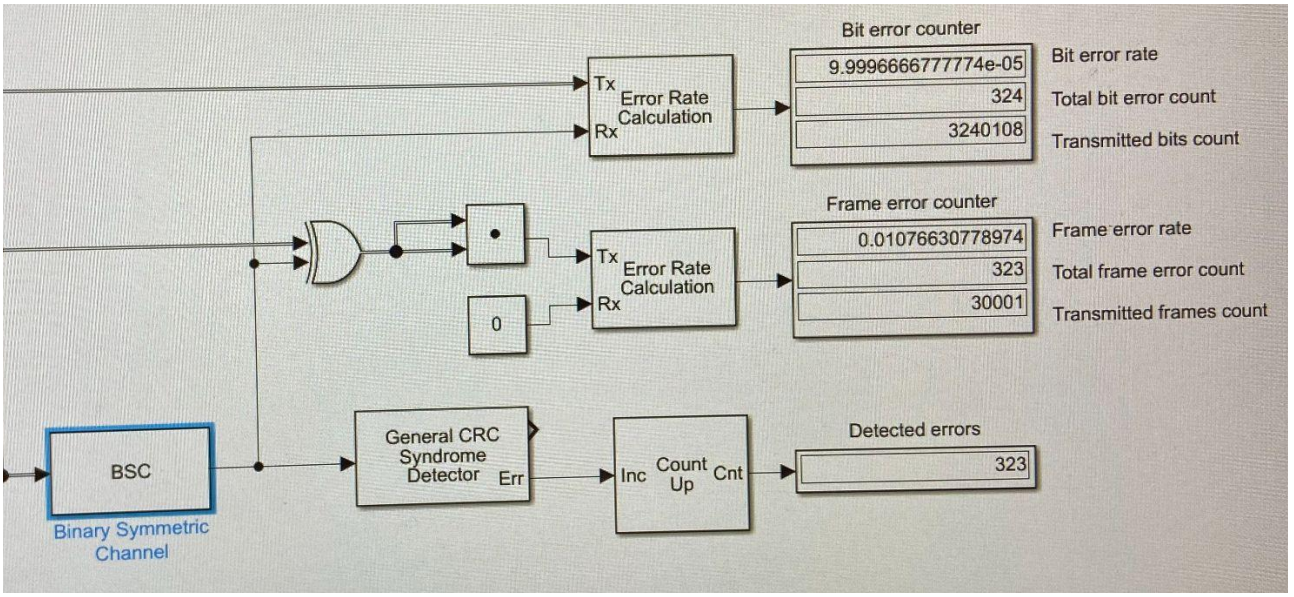
1. **Detekční vlastnosti**
   Spustili jsme program Matlab, do bloku Frame jsme umístili datový rámec s délkou 8 bitů. Zvolili jsme generující polynom CRC3 (x^3 + x + 1). Nejdříve jsme zvolili chybový vektor bez chyb a program potvrdil, že CRC žádnou chybu neobjevilo. Poté jsme zvolili vektor s jednou chybou, kde všechny vzniklé chyby byly odhaleny. Po správném nastavení systému jsme začali ověřovat hypotézy:
   a. Je-li chybový vektor posunem generujícího polynomu (násobení obecnou mocninou), chyba není detekována.
      Jako chybový vektor jsme použili 00000010110.
   b. Je-li chybový vektor beze zbytku dělitelný generujícím polynomem, chyba není detekována.
      Použili jsme vektor 00000011101
   c. Každá jednonásobná chyba je detekována, pokud má generující polynom koeficient 1 u x^0 a zároveň má alespoň jeden další člen.
      Použili jsme vektor 00000010000.
   d. Pokud je generující polynom beze zbytku dělitelný polynomem $x \oplus 1$, pak detekuje jakýkoliv lichý počet chyb.
      Použili jsme vektor 00000011111.
   e. Pokud x^$i \oplus 1$ není beze zbytku dělitelné generujícím polynomem pro všechna $i \in [1, n - 1]$, kde n je délka kódového slova, pak jsou detekovány všechny dvojnásobné chyby.
      Použili jsme vektor 10001000000 (podmínku náš generující polynom splňuje).
   f. Pokud je chybový vektor typu x^j (x^(t−1) $\oplus$ …$\oplus$ 1), kde t je menší nebo rovno stupni generujícího polynomu (shluk chyb s délkou menší nebo rovnou počtu bitů CRC), pak jsou všechny takovéto chyby detekovány.
      Použili jsme vektor 11100000000 (stupeň generujícího polynomu je 4 a délka shluku chyb je 3 - tedy splňuje podmínku).

   Všechny hypotézy jsme potvrdili.

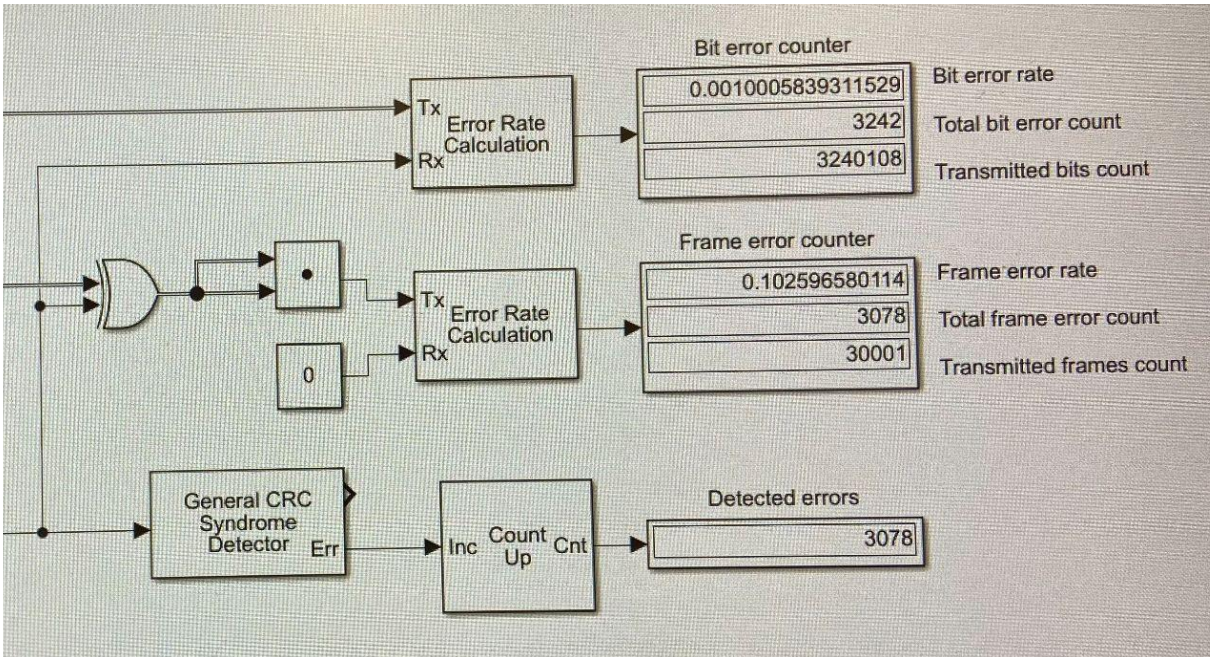
2. **Spolehlivost**
   V Simulinku jsme otevřeli předpřipravené simulační schéma Bernoulli Binary Generator. Poté jsme zkoušeli simulace pro různé pravděpodobnosti chyb a různé generující polynomy CRC. Následující tabulka ukazuje poměr celkového počtu chyb a počtu objevených chyb.

	Pravděpodobnost chyby

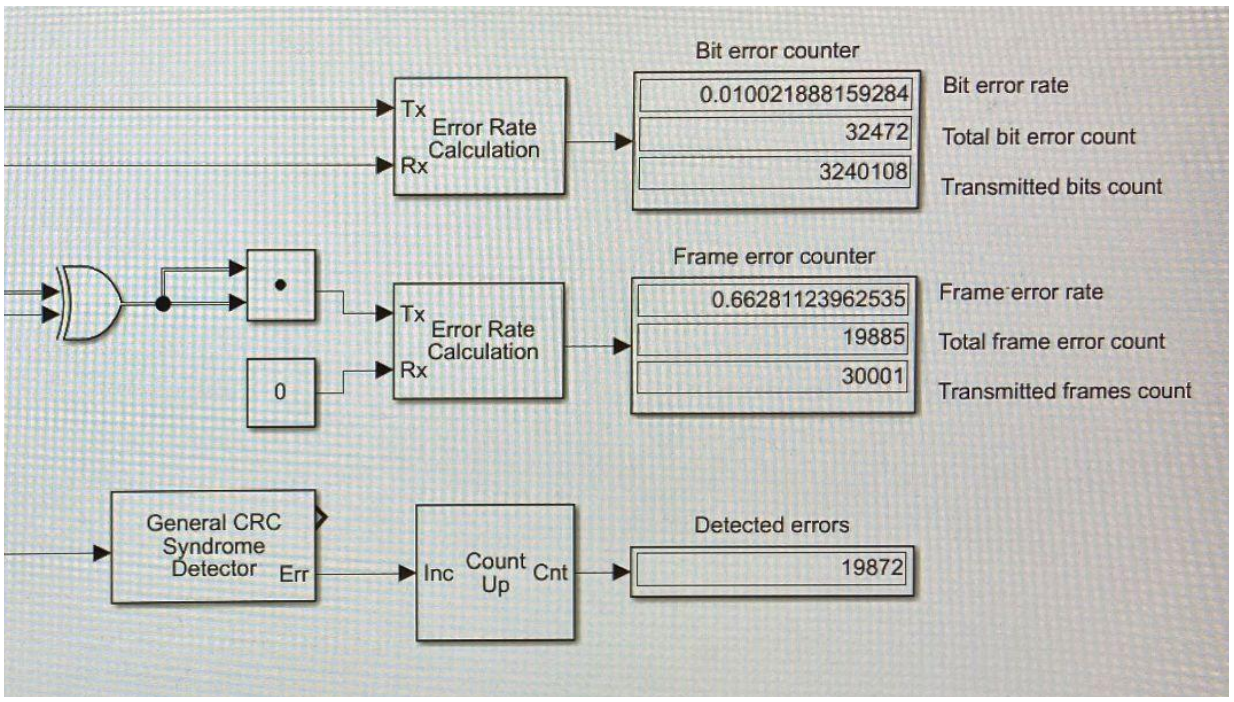
	0,1 ‰	1 ‰	1%
CRC3	304/304	2921/2905	19388/18280
CRC8	323/323	3078/3078	19885/19872
CRC16 (IBM)	×	×	20569/20568



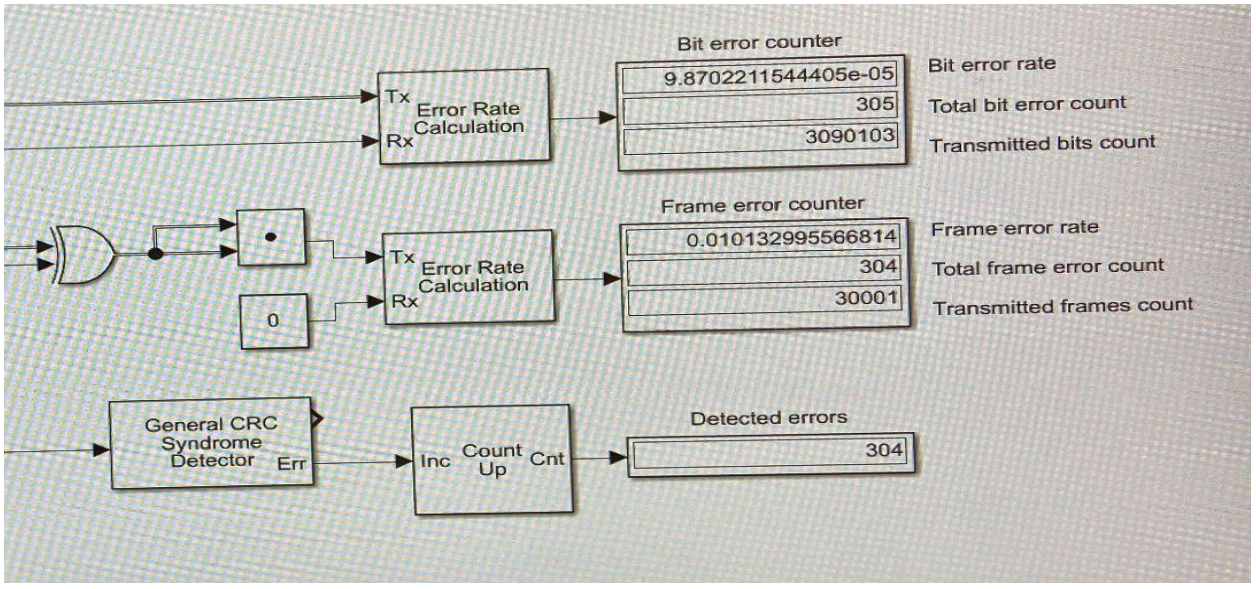
Obrázek 1: 0,1 ‰ pro CRC8



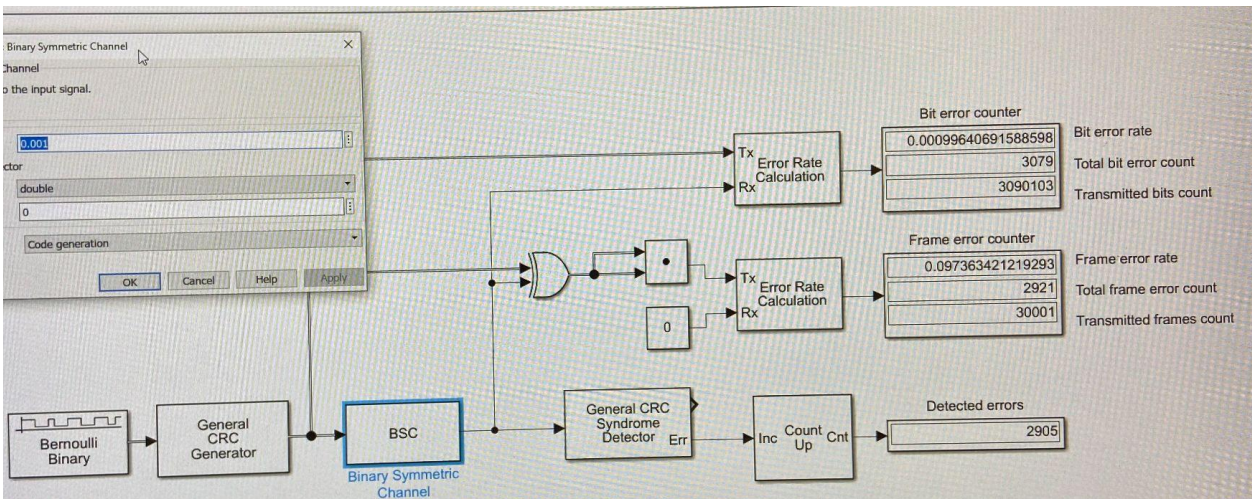
Obrázek 2: 1 ‰ pro CRC8



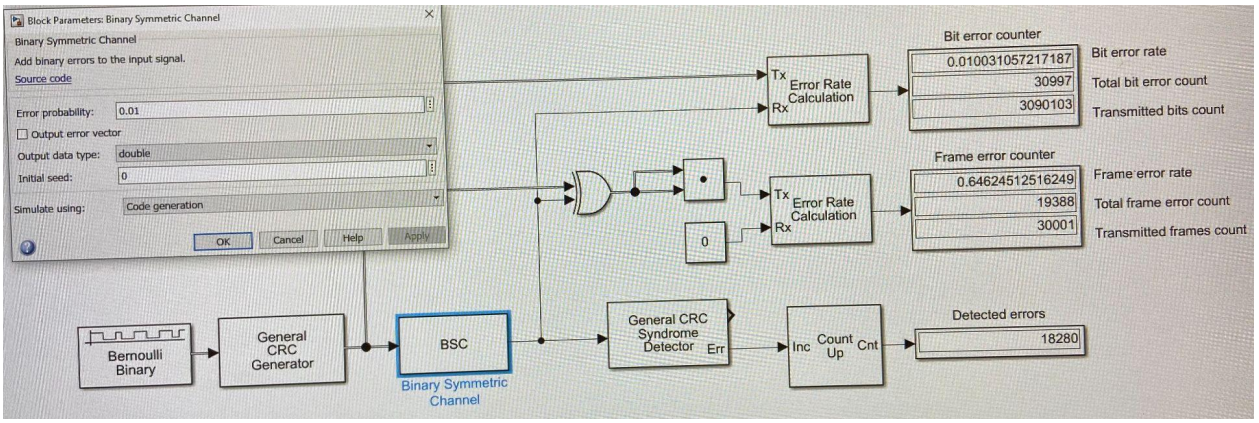
Obrázek 3: 1 % pro CRC8



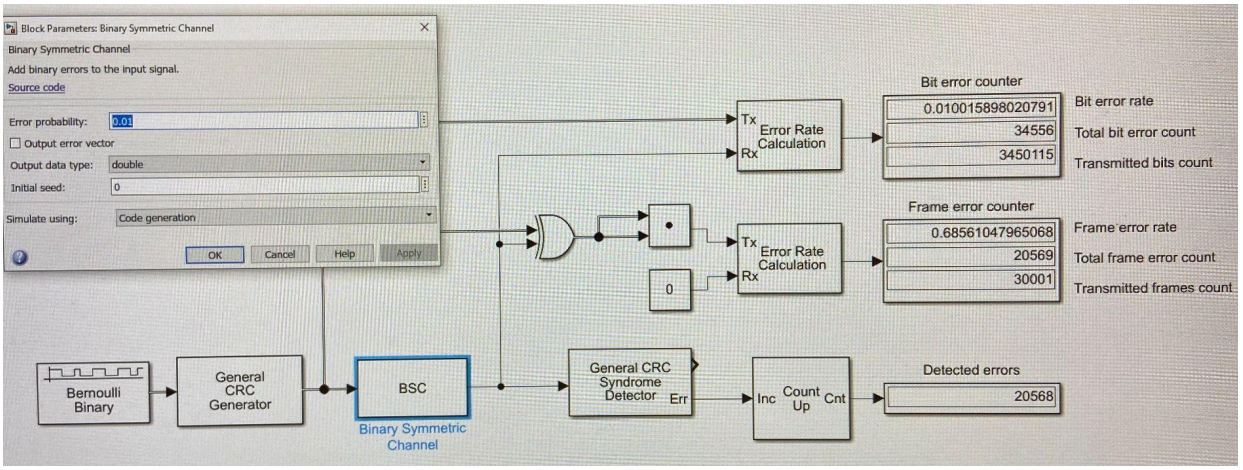
Obrázek 4: 0,1 ‰ pro CRC3



Obrázek 5: 1 ‰ pro CRC3



Obrázek 6: 1 % pro CRC3



Obrázek 7: 1 % pro CRC16-IBM

Závěr:

Prakticky jsme ověřili teoretické znalosti o metodě CRC z přednášek a testovali jsme vliv délky CRC na detekční vlastnosti. Všechny hypotézy jsme potvrdili. Také jsme ověřili, že s rostoucí délkou a stupněm CRC roste i jeho spolehlivost.