Formal verification of real-time data processing of the LHC Beam Loss Monitoring system

Judit Ács

judit@aut.me.hu

2014. December 10.

Áttekintés

Bevezetés

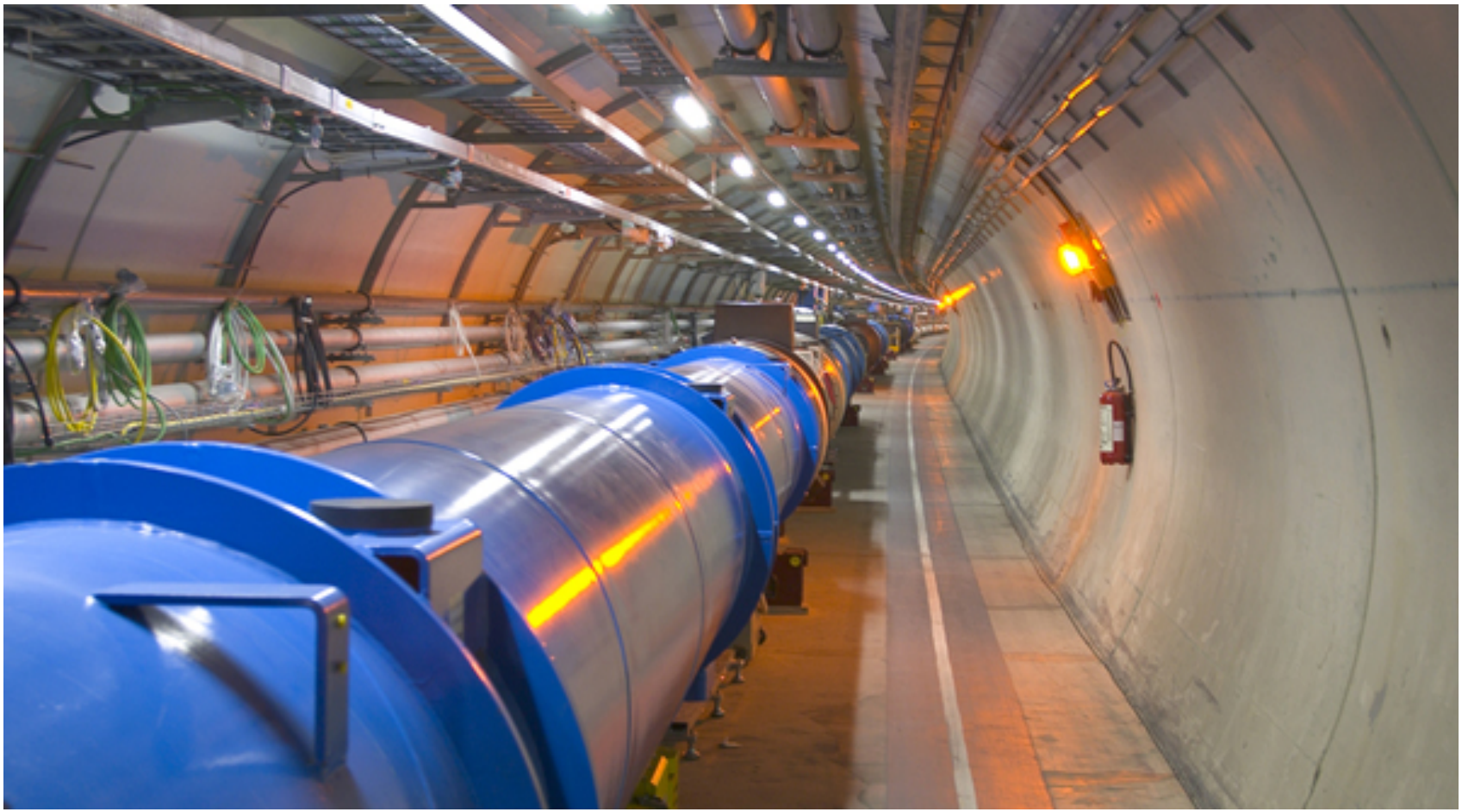
Successive Running Sums

Konklúzió

Nagy hadronütköztető (LHC)

- világ legnagyobb részecskegyorsítója, 7 TeV-ra energiára gyorsítja a protonokat
- mágneses térhez szupravezetők
- keringő protonnyalábok energiája 700 MJ
- nagyon kis rész a falnak ütközve megszünteti a szupravezetést
  - *quench*
- néhány óra – néhány hónap kiesés

LHC



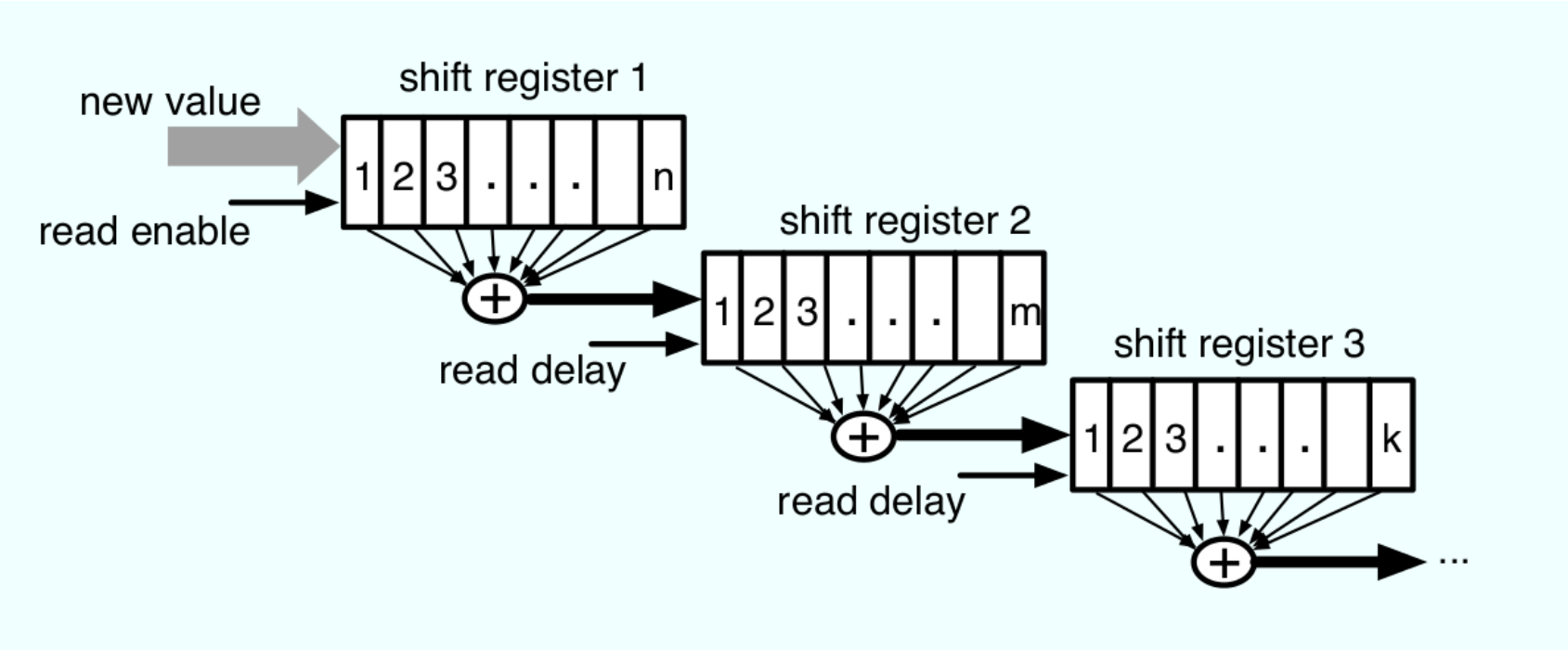
Beam Loss Monitoring System (BLMS)

- képes kivonni a sugarakat és biztonságosan leállítani az ütköztetőt
- 27 km hosszú csőben kb. 4000 ionizációs kamrával méri a szóródó részecskéket
- adatfeldolgozó egység összegzi az adatokat
- *Successive Running Sums*

Esettanulmány

- Ghafari et al.
- HOL4 bizonyítórendszer
- SRS formális verifikálása

Successive Running Sums



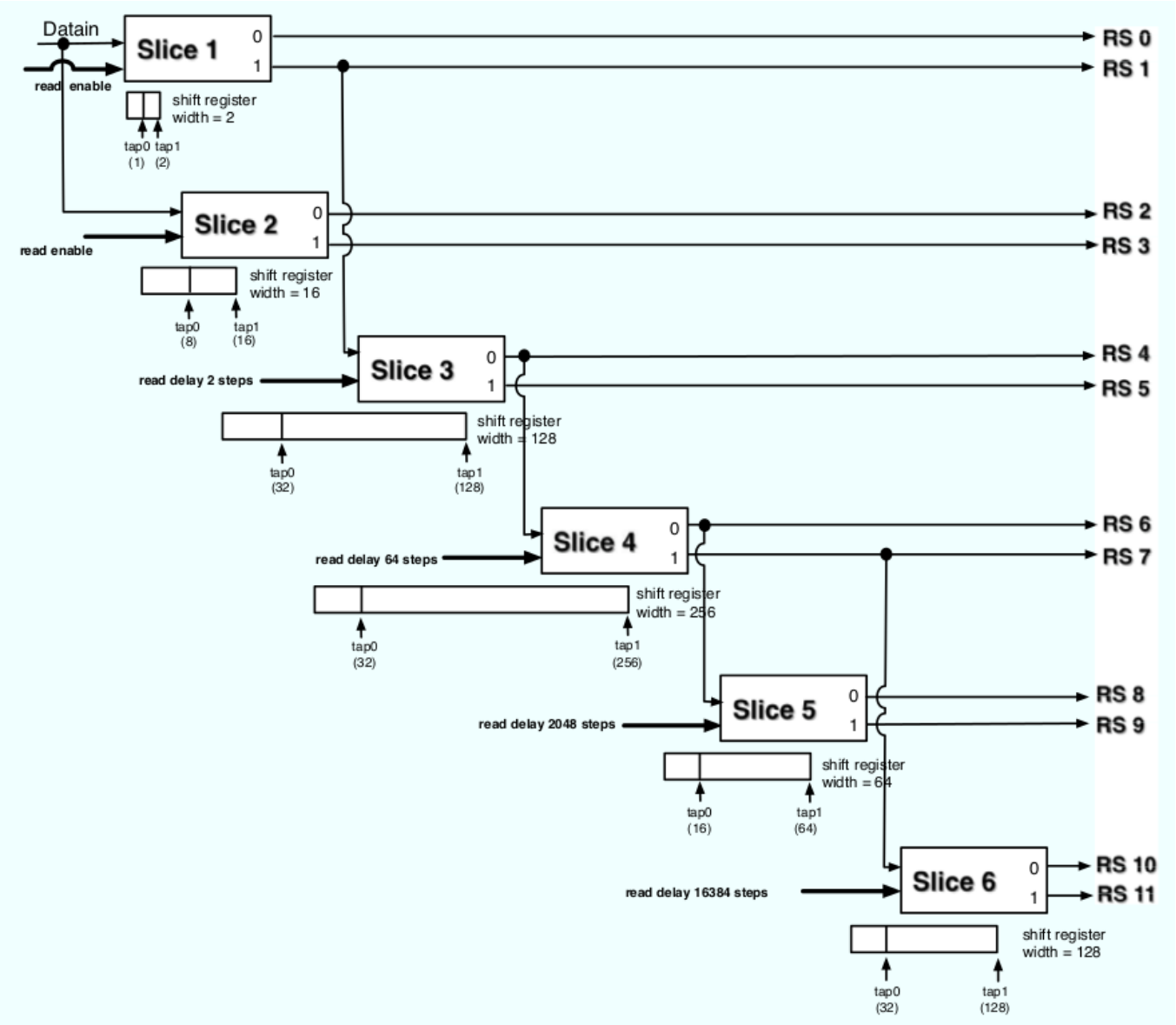
Successive Running Sums

- Slice: egy db shift regisztert tartalmazó réteg
- Tap: kimenetek, több is lehet slice-onként (0-tól indexel)
- Valóságban: 6 slice, 12 kimenet
- diszkrét idő: t
- bemenet t időpillanatban: D t
- true_sum n: n input után a tényleges összeg
- integrációs ablak: egy shift regiszter celláinak száma
- verifikálásnál általánosítanak: n kimenet (RS)

Cél

$$\forall n \cdot \mathrm{RS}\ n = \mathrm{true\_sum}\ n \pm \text{acceptable error}$$

Successive Running Sums



Állítások

- egy regiszter akkor frissül, ha a felette lévő slice megtelik,
- az integrációs ablaka egy shift regiszternek diszjunkt részek sorozatára bontható, amelyek az előző réteg intergrációs ablakával egyenlő méretűek (kivéve az elsőt),

Állítások

- az inicializáció után az egy regiszterben tárolt értékek megegyeznek az előző utolsó w kimenetével, ahol w az előző regiszter szélessége,
- az inicializáció után az egyes regiszterek kimenete megegyezik a regiszter értékeinek összegével

Formális állítás I.

$$\text{output}\ D\ n\ x\ t = \sum_{m=0}^{((\text{tap}\ n\ x)+1)\times(\text{delay})-1} \begin{cases} 0, t \leq m + \text{delay\_sum}\ n \\ D(t - m - \text{delay\_sum}\ n), \textit{otherwise} \end{cases} \tag{1}$$

Formális állítás I.

- indukcióval levezethető, hogy

$$\mathrm{SR}\ D\ n\ m\ t = \mathrm{SR}\ D\ n\ 0(t - (m \times \mathrm{delay}\ n)),$$

$$\mathrm{output}\ D\ n\ x\ t = \sum_{m=0}^{\mathrm{tap}\ n\ x} \mathrm{SR}\ D\ n\ m\ t$$

Formális állítás II.

$$\text{output}\ D\ n\ x\ t =$$

$$0, \text{last\_update}\ n\ t + 1 \leq \text{delay\_sum}\ n$$
$$\text{exact}\ D\ n\ x(\text{last\_update}\ n\ t + 1 - \text{delay\_sum}\ n), \mathit{otherwis}$$

Formális állítás III.

$$t > (\text{tap}\, n\, x{+}0){\times}(\text{delay}\, n){+}\text{delay}\, n{+}\text{delay\_sum}\, n \rightarrow$$
$$|\text{output}\, D\, n\, x\, t - \text{exact}\, D\, n\, x\, t|$$
$$\leq (\text{tap}\, n\, x + 1) \times (\text{delay}\, n) \times k$$
$$\times\, (\text{delay\_sum}\, n - 1 + t \mod \text{delay}\, n) \quad (3)$$

Konklúzió

- III. állítás ad felső korlátot az összeg hibájára az idő, a slice és a tapek függvényében
- a valódi összeg relatív hibájaként hasznosabb lenne (20%)
- nem állították még fel ezt a kapcsolatot
- a modell általánosabb, mint a működő rendszer
- lehetséges fejlesztés: alacsonyabb absztrakciós szint, hardverközelibb