Biztonsági rendszerek létrehozásának szempontjai

Dr Gyenes Károly Ph.D.

Budapesti Műszaki és Gazdaságtudományi Egyetem

1111 Bp. Bertalan Lajos u. 2. Z.ép. 504.

Tel.: (36-1-) 463-19-93

e-mail: gyenes.karoly@mail.bme.hu

Vasúti fail-safe rendszerek

A vasútüzem a forgalommal kapcsolatos veszélyhelyzeteket vasútbiztosító berendezések üzemeltetésével kerüli el (legalábbis megkísérli ezek bekövetkezését elkerülni).

Ezek a berendezések eleget tesznek a biztonság követelményeinek, azaz adott üzemi körülmények között meggátolják a veszélyhelyzet kialakulását.

Teljes biztonság elméletileg nem érhető el, ezért a biztonság valószínűségi változóként fogható fel, amelynek értéke az ésszerűség határain belül az 1-et alulról közelíti.

A berendezések fail-safe (hibatűrő) tulajdonsággal rendelkeznek. Ennek értelmében a berendezés bármely hibájának fellépése nem okozhat veszélyhelyzetet.

A berendezéseknek megbízhatóknak kell lenniük, azaz a specifikáció szerinti működésük tartósan fennmarad.

A megbízhatóság mérőszáma a rendelkezésre állás, amely a hibamentes működési idő (t_m) és a javításra fordított idő (t_{jav})viszonyszáma:

$$Mb = t_m / (t_m + t_{jav})$$

Fontos jellemző a berendezés **élettartama, amely specifikáció szerinti működés időtartama**. Ezt az időtartamot a műszaki kialakítás minősége és az elavulás befolyásolja.

A biztonsági rendszerek alapelve:

A hiba bekövetkezése elkerülhetetlen, de a hiba rejtve maradása elkerülhető.

Ezek szerint kiemelt fontosságú cél a hiba felfedése.

Fail-safe rendszer elemei

1. Hardware elemek

2. Software elemek

3. Biztonsági adatátvitel

4. Gyártás és minőségbiztosítás kritériumai (ezzel jelen cikk nem foglalkozik)

1. Hardware elemek

A biztonság elérésének alapja a redundancia alkalmazása

A redundáns HW rendszerek főbb kialakítási módozatai (vázlatos áttekintés):

2-ből 2 felépítés AND logikával

3-ból 2 felépítés MAJORITÁS logikával

2 * 2-ből 2 felépítés lazán csatolt logikával

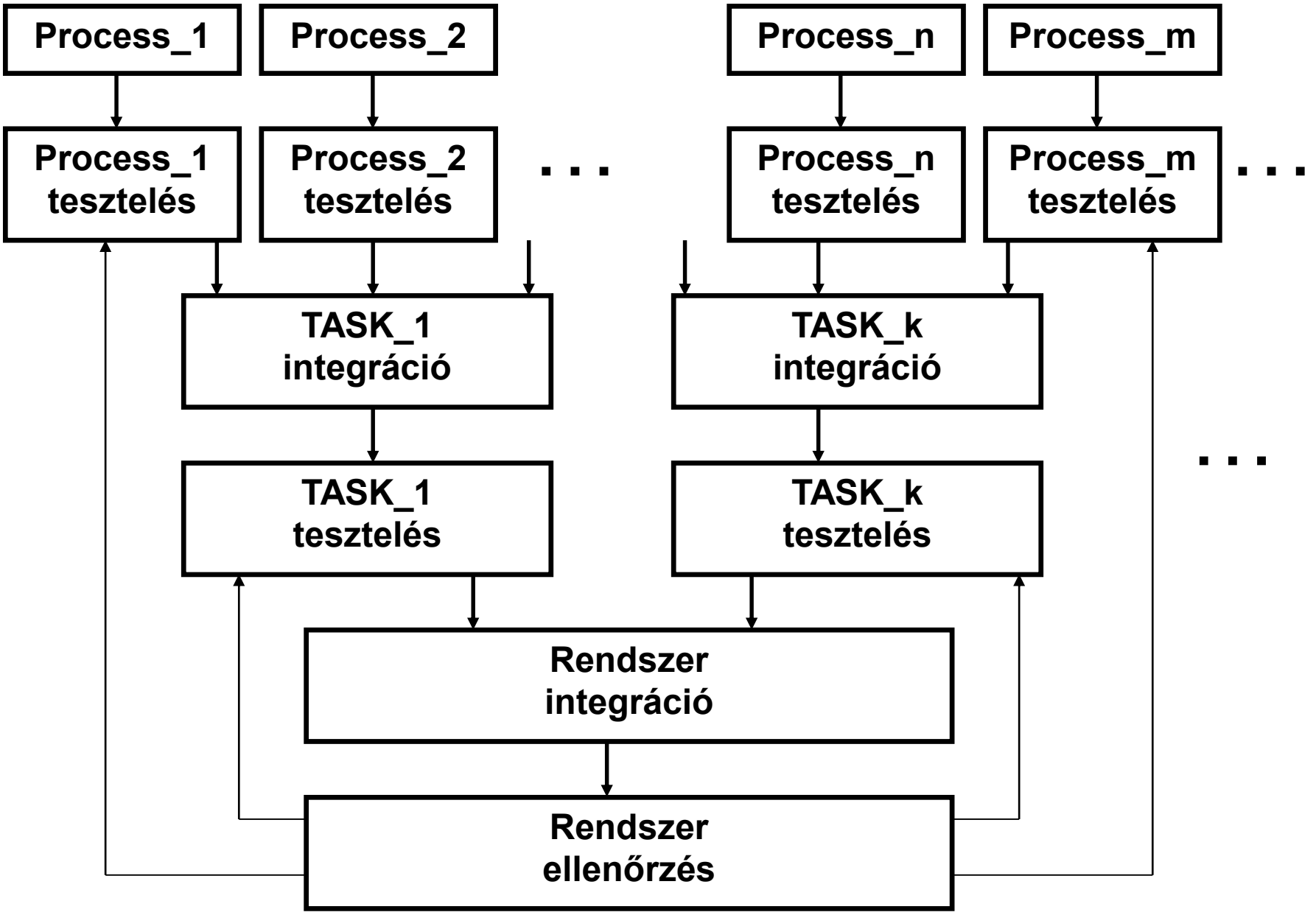
2 * 3-ból 2 felépítés szinkronizált működtetéssel

2. Software elemek

A biztonság elérésének alapja a diverzitás és a biztonsági programozás alkalmazása

A diverzitás megköveteli, hogy az adott feladatot több, egymástól független program hajtsa végre. (Ez redundáns HW konfigurációt igényel.)

A biztonsági programozás **hierarchikus fejlesztői** környezetet kíván meg. Ennek sémája a következő dián látható.


Process_1
Process_2
Process_n
Process_m
Process_1 tesztelés
Process_2 tesztelés
Process_n tesztelés
Process_m tesztelés
TASK_1 integráció
TASK_k integráció
TASK_1 tesztelés
TASK_k tesztelés
Rendszer integráció
Rendszer ellenőrzés

Moduláris programozás: funkció szerinti modulok készítése és önálló tesztelése.

A modulok jól dokumentált be-kimeneti interfésszel készüljenek.

Logikus változó nevek használata, amelyek utalnak a változó szerepére és típusára.

A-B-C programozási elv betartása:

A programozó az egyik csatorna kódolását,
B programozó a másik csatorna kódolását
C rendszer szakember az ellenőrzést végzi el.

A B C személyek egymástól szakmailag függetlenek.

Különböző biztonsági programozási nyelvek használata.

Javasolt nyelvek:

- **ADA**
- **C**
- **CHILL**
- **Assembler**

Biztonsági rendszerekben kerülni kell az operációs rendszerek beépített alkalmazását.

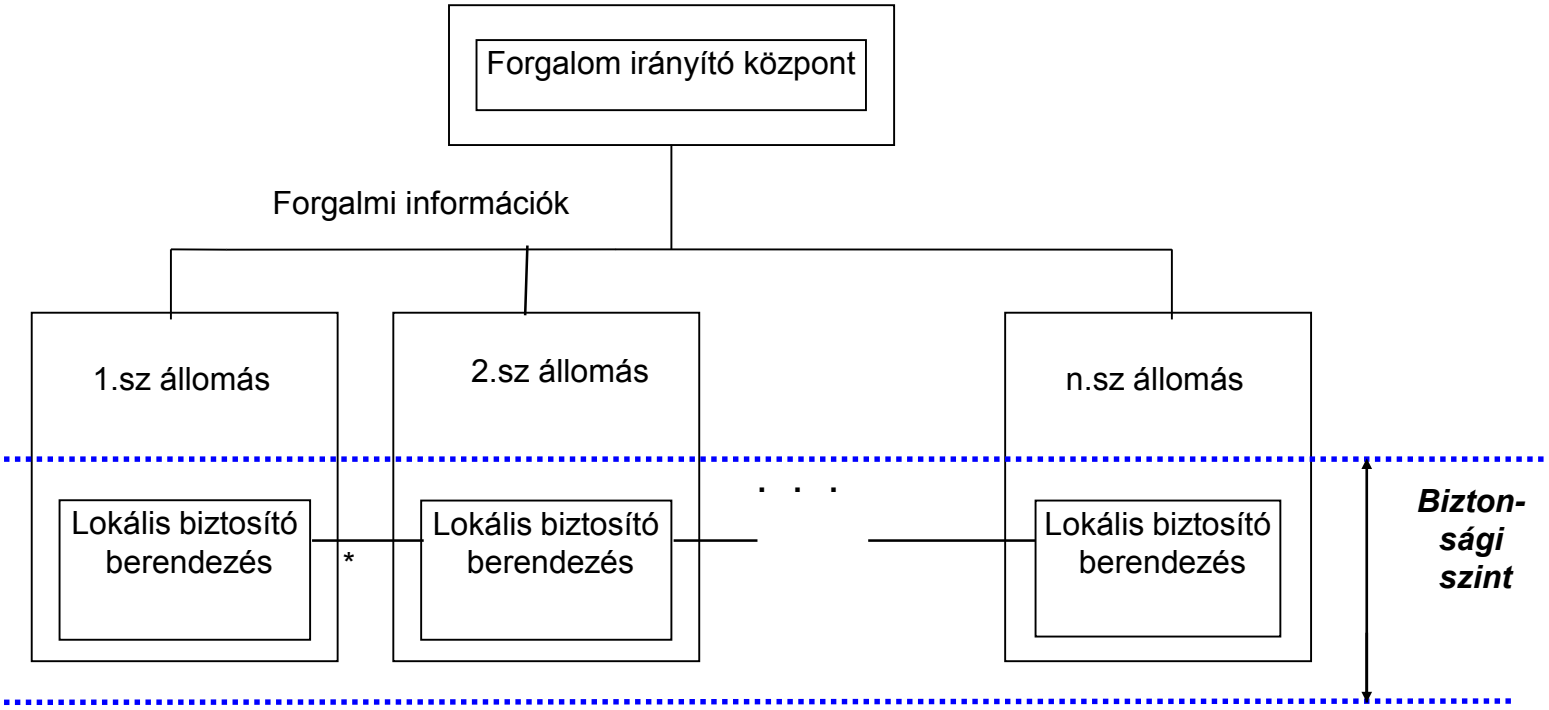
Fokozott memória védelem alkalmazása

Időtúllépés figyelése (SW watch-dog, time-out)

Működést dokumentáló-monitorozó modulok alkalmazása szükséges

3. Biztonsági adatátvitel

A hagyományos elektromechanikai, vagy lokális elektronikus biztosítóberendezés sémáját az 1.1. ábra szemlélteti

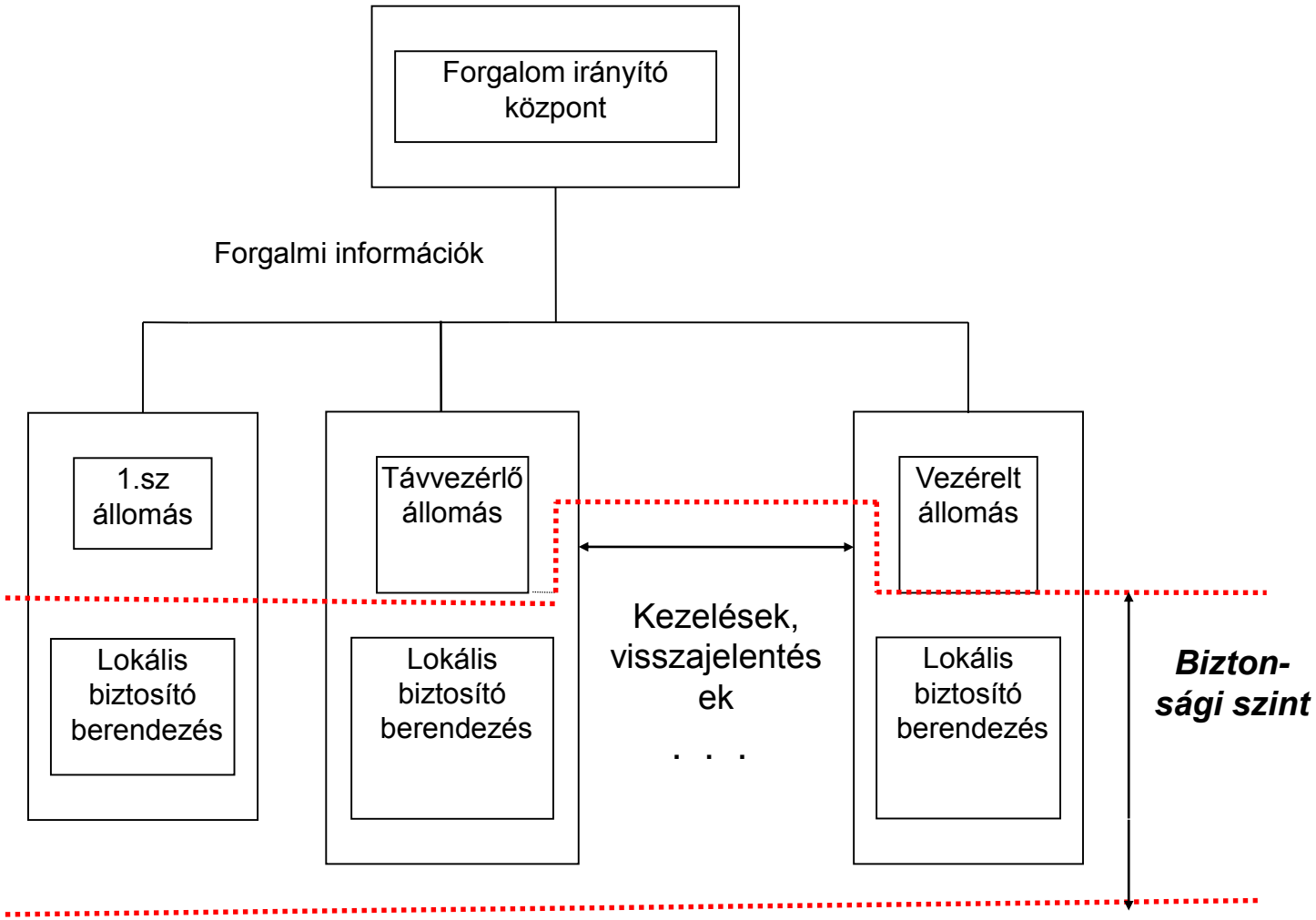


* Vonali berendezések, térközök, stb.

Az elektronikus biztosítóberendezés lehetővé teszi az állomások összehangolt működését. Így az egyes állomások között vezérlő parancsok átvitele történik.

Ennek megfelelően az átvitelt fail-safe elven kell megvalósítani.

Az ilyen elektronikus biztosítóberendezés sémáját a következő dián bemutatott ábra szemlélteti.


Forgalom irányító központ
Forgalmi információk
1.sz állomás
Távvezérlő állomás
Vezérelt állomás
Lokális biztosító berendezés
Lokális biztosító berendezés
Kezelések, visszajelentések
. . .
Lokális biztosító berendezés
Bizton-sági szint

Az átviendő adatok bináris formájú jelek. A bináris rendszereket egyszerű megvalósítani, de mivel információ hordozó képességük alacsony, az információ sok bitet tartalmaz.

Ezért a zavarok hatásának erősen ki vannak szolgáltatva.

A fail-safe átvitelnél az adatokat védeni kell.

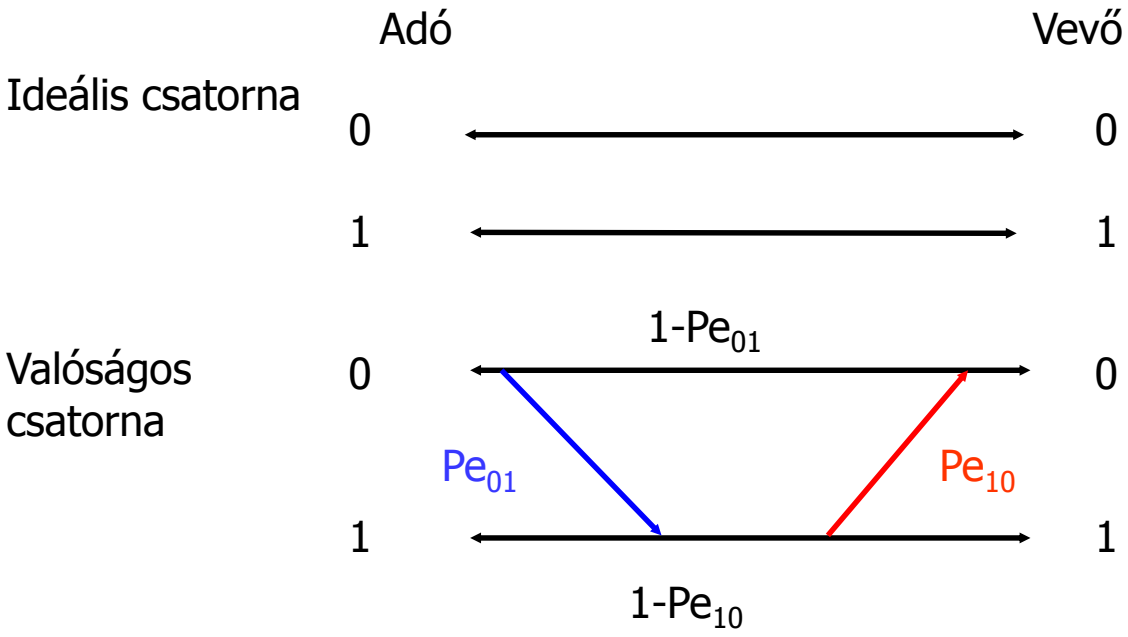
A védelem alapja ismét a redundancia alkalmazása.

Adatismétlés (rövid adatok szimplex átvitele)

Hibajavító kódolás

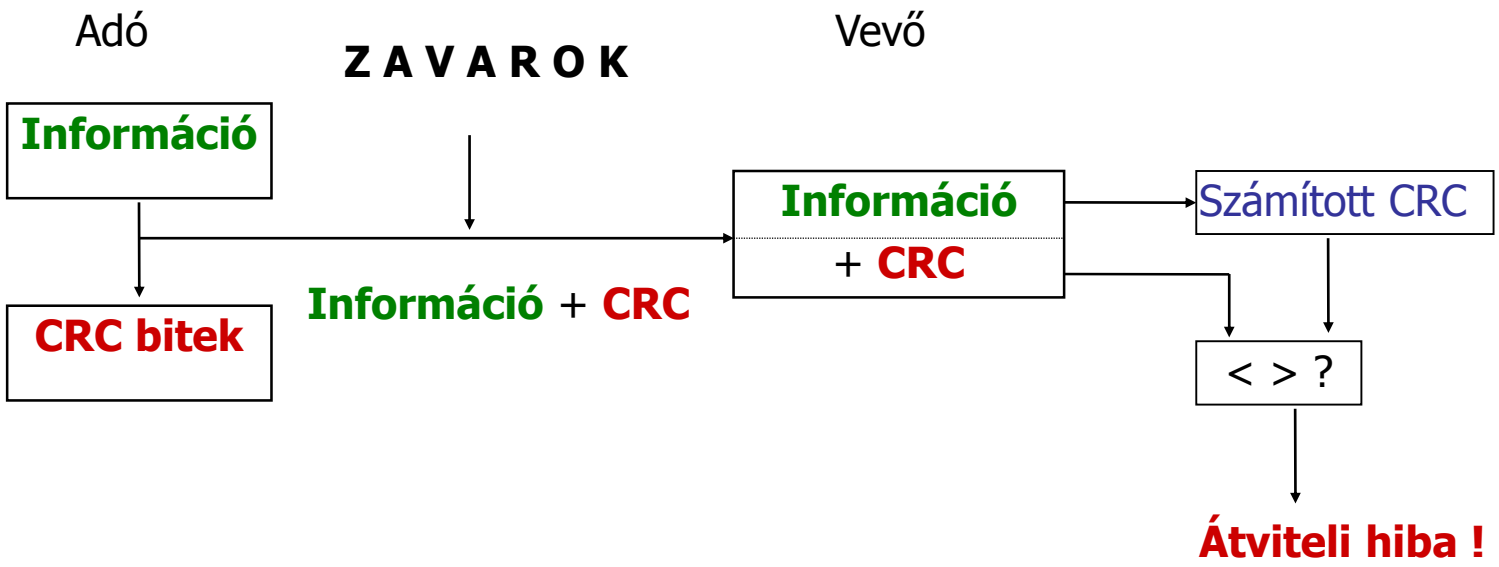
Magasfokú adatvédelem

Adatátviteli csatorna modellje :



Továbbiakban a magasfokú adatvédelem kérdését vizsgálom

A CRC (Ciklikus Redundancia Kód) alapú adatvédelem működési elve



Bináris mező (információ): ***k*** elemű bitsorozat, amelyen lineáris műveleteket végzünk.

A CRC kiszámításához **moduló-2 algebrát** használunk:

A és **B** operandus lehetséges értékei

	0 0 1 1
	0 1 0 1
A+B	0 1 1 0
A -B	0 1 1 0
A*B	0 0 0 1
A/ B	- 0 - 1

A **bináris polinom** a bináris mező elemeiből, mint együtthatókból képzett algebrai kifejezés. Egy k-ad fokú bináris polinom általános alakja:

$$P_k = \sum_{i=0}^{k} m_i * x^i$$

ahol $\mathbf{m_i}$ a bináris mező i-ik bitje, **x** pedig formális változó (bináris polinom esetén értéke 2).

Tekintsük például az 1011001 mezőhöz tartozó bináris polinomot:

$P_6 = x^6 + x^4 + x^3 + 1.$

A legkisebb helyiértékkel a mező jobboldali eleme rendelkezik.

A továbbítandó információ polinom alakban legyen ***u(x).***

A CRC nyerésének módja, hogy az információ polinomját egy ***generátor polinommal***, jele legyen ***g(x)*** ***szorozzuk meg***. Igy a forgalmazandó kódblokk:

$$b(x) = u(x) * g(x)$$

Ha u(x) n bitet, míg g(x) k bitet foglal el, akkor b(x) polinom hossza n+k lesz, azaz a generátor polinom fokszáma adja a redundáns bitek számát.

A következő táblázatban néhány gyakori generátor polinomot mutatunk be:

CRC név	Felhasználó	Polinom
BCH*	EEA**	$x^8 + x^7 + x^6 + x^4 + 1$
FBC***		$x^{23} + x^{18} + x^{16} + x^7 + x^2 + 1$
CRC-12	6 bites átvitel	$x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-16	IBM	$x^{16} + x^{15} + x^2 + 1$
CRC_16 reverse	IBM	$x^{16} + x^{14} + x + 1$
SDLC	CCITT	$x^{16} + x^{12} + x^5 + 1$
Ethernet	LAN	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x+1$

* Bose - Chaudhuri - Hocqueghem

** European Electronics Association

*** Fire - Burton Code

Nézzük mi történik adatátviteli hiba esetén.
Ha az átvitel hibás, akkor a b(x) forgalmazott kódblokk helyett r(x) polinom adódik, amelyet

$$r(x) = b(x) + e(x)$$

alakban írhatunk fel.

Képletünkben e(x) a **hibapolinom** (vagy hiba szindróma), amelynek maximális fokszáma n+k -1 lehet.

A vevő hibátlannak tekinti az átvitelt, ha az osztás elvégzése után a maradék = 0.

A maradék akkor lesz 0, ha e(x) = 0 (ez a hibamentes átvitel esete), vagy ha **e(x) = k*g(x),** azaz a hiba polinom a generátor polinom egész-számú többszöröse (ez a fel nem fedett hibák esete).

Hibajavító stratégiák (mi történjen, ha a vevő hibát észlel)

- FEC (Forward Error Correction) : A felfedett hibát a vevő valamely hibajavító kód alkalmazásával megkíséreli kijavítani.

- ARQ (**A**utomatic **R**epeat Re**q**uest) : Hiba esetén a vevő az adatátvitel ismétlését kezdeményezi.

A fail-safe adatátvitel az ARQ technikát használja

Néhány irodalom:

- Dr K.Gyenes : Design of fault-tolerant data transmission systems
Tutorial for the session of Formal Methods in Informatics
VEAB 2000.

- dr Gyenes Károly : A biztonsági adatátvitel kérdései a vasútnál
Vezetékek Világa I.évf. 4.szám. 5.o. 1996.

- dr Gyenes Károly : A vasúti távvezérlés adatátviteli protokollja
Vezetékek Világa II.évf.4. szám. 12.o. 1997.

- dr Gyenes Károly : A CRC blokk kódolás hibaanalízise számítógépes szimulációval
Vezetékek Világa III.évf. 1.szám. 15.o. 1998.

- dr Gyenes Károly: Mikroszámítógépes vasúti forgalomirányító és távvezérlő Rendszerek biztonsági kérdései
PhD disszertáció BME Közlekedésmérnöki Kar 1999.

- Elek L. dr Gyenes K. Pál Gy. Szabó G. : Korszerű, magas biztonságintegritású ütemadó berendezések a MÁV vonalán
Vezetékek Világa XII.évf. 1.szám. 15.o. 2007.

- Szabó Géza : Kockázati alapú fejlesztési kritériumok a járművek biztonsági rendszereinél http://www.2ge.hu/index.php

Köszönöm a figyelmet