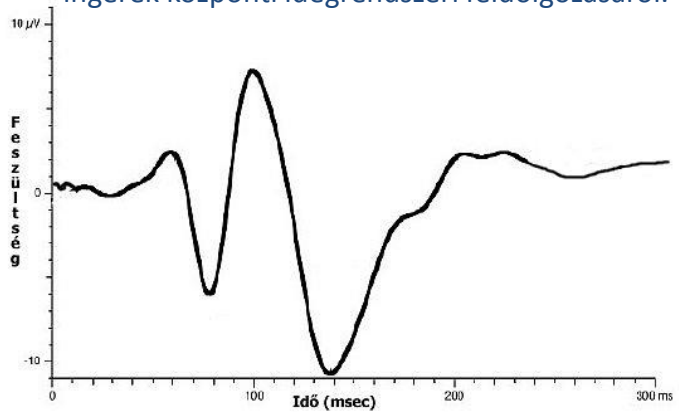
Kiberfizikai rendszerek

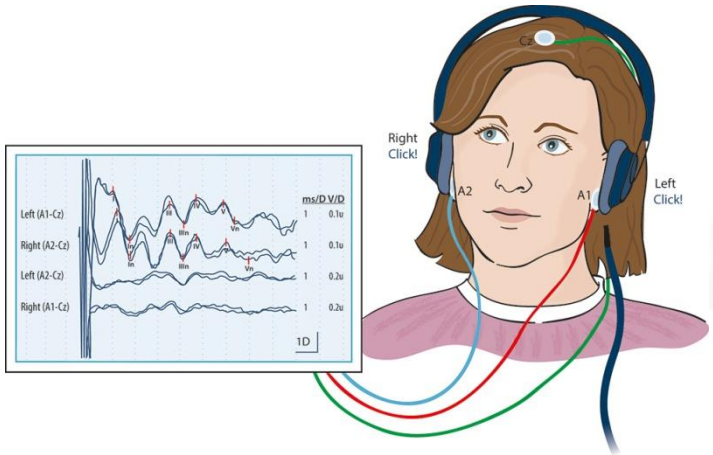
A “fizikai” vonatkozásokról …

2015. november 3.

Befogadó környezetek – befogadott eszközök

KIVÁLTOTT VÁLASZ – A kiváltott válaszok a központi idegrendszer külső ingerlésre létrejövő válaszai. Ezekből információt kaphatunk az idegpályák állapotáról valamint az adott ingerek központi idegrendszeri feldolgozásáról.

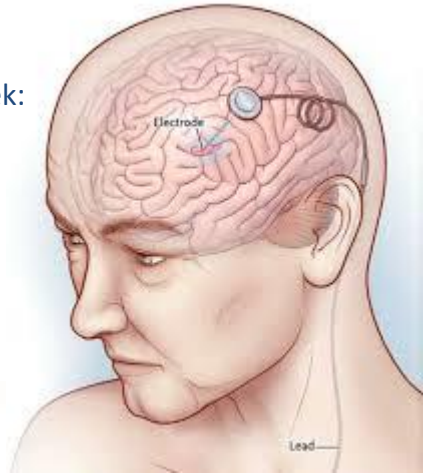


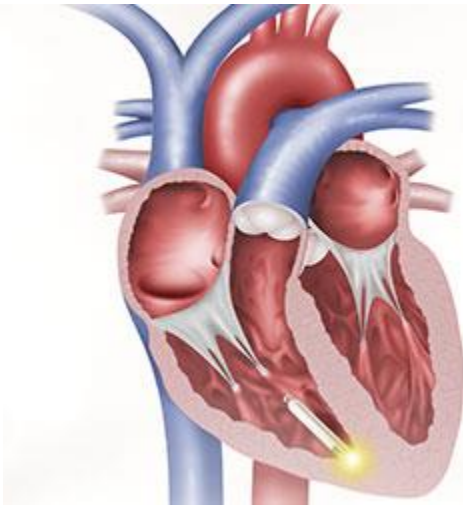


Kezdetek: Kőbányai Gyógyszerárugyár , ma RG Farmakológiai Kutatólaboratórium ~1978 Cavinton …

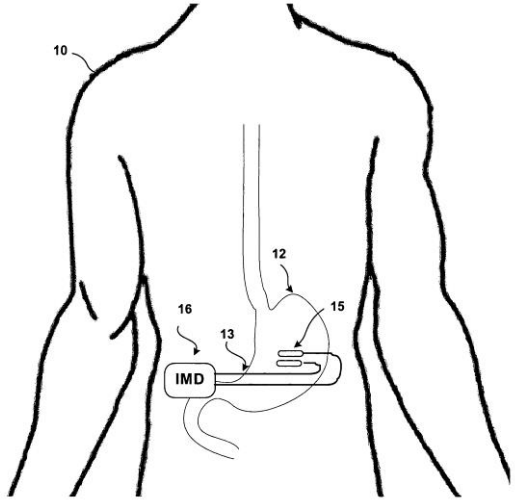
PACEMAKEREK

Kezelt betegségek:
Parkinson-kor
Anorexia
Epilepszia
Migrén
Depresszió
Altzheimer-kor





Kezelt betegségek:
Fibrilláció
Aritmia

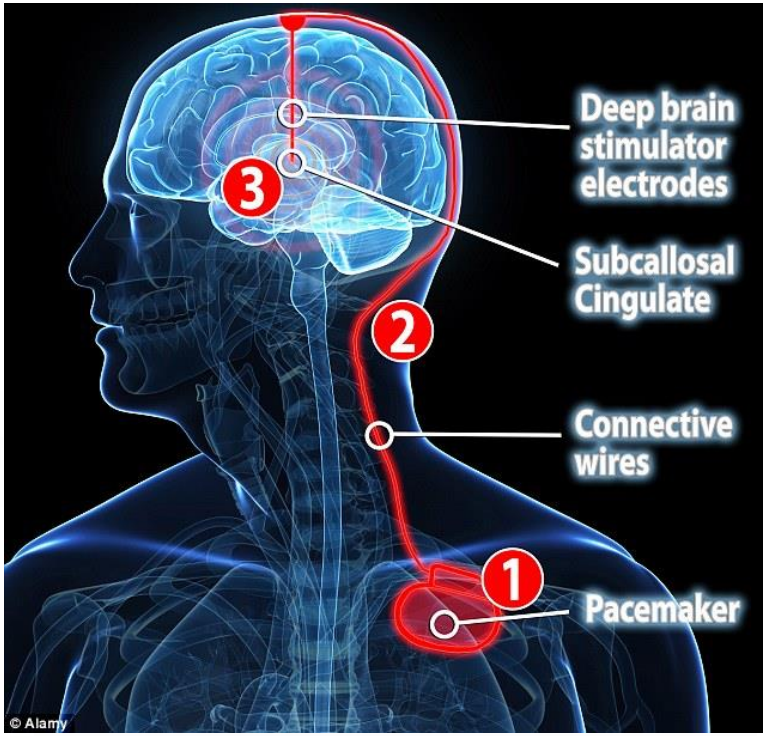


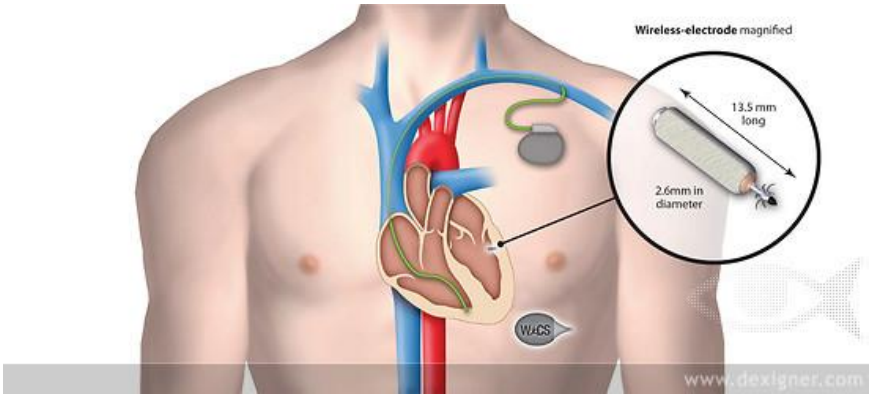
Terápiás cél:
Jóllakottság érzet előidézése, hányinger, hányás elkerülése

Befogadott-beágyazott eszközök

Hagyományos pacemaker
2009 óta akár Internet kapcsolattal
Beépítés: 45’

Vezetéknélküli pacemaker
Beépítés katéteren keresztül: 7’





Beágyazott rendszer funkciók

Beágyazott rendszer ~ Központi idegrendszer:

→ megfigyel → analizál → dönt → cselekszik

A német gépjármű, automatizálási és orvosi ipar évente ~15 milliárd € -ot invesztál beágyazott rendszerek kutatás-fejlesztésére, miközben éves forgalmuk meghaladja az 500 milliárd € -ot.

Tulajdonságai:

Intenzív információs kapcsolat
Autonóm működés
Szolgáltatásbiztonság
„Láthatatlanság”

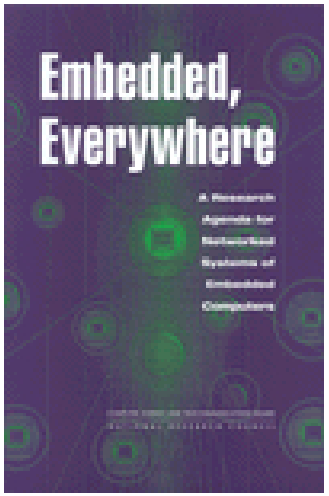
Alternatív elnevezések:

Embedded System
Pervasive Computing
Ubiquitous Computing
Ambient intelligence

Egy lehetséges definíció:

A befogadó fizikai/kémiai/biológiai környezetükkel intenzív, valós idejű információs kapcsolatban álló,

- emberi beavatkozás nélkül működő,
- nagyon biztonságos,
- sokszor “láthatatlan”

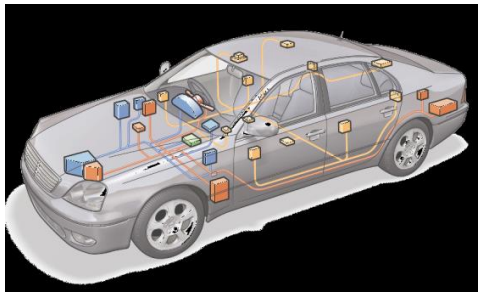


A Research Agenda for Networked Systems of Embedded Computers National Academy of Sciences (2001)

számítógépes rendszerek, melyek

- egy-egy eleme (általában) erősen korlátozott képességű,
- rendszert alkotva azonban (általában) bőséges erőforrásokkal (memória, sávszélesség, ...) rendelkeznek.

Fly-by-wire



Drive-by-wire

BMW 745i:
53 db 8-bites,
11 db 32-bites,
7 db 16-bites processzor,
2 000 000 sor kód,
Windows CE OS,
többszörös hálózat.

A processzorok 2%-a IT és PC felhasználású, 98% beágyazott alkalmazás: jármű, háztartási gép, mobil telefon, stb.

A főszereplő: a beágyazott szoftver

„Szabványos” hardver és szoftver építőelemek (COTS) alkalmazása mellett, az egyedi képességeket a beágyazott/alkalmazói szoftver valósítja meg. A valós rendszerek alkotóelemei egyre inkább „számítástechnikai” kölcsönhatások révén működnek együtt. (Prémium kategóriás autók: több ezer jelvezeték, 70 – 100+ elektronikus vezérlőegység)

A beágyazott szoftver: univerzális rendszerépítő eszköz

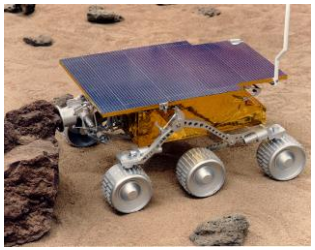
Következmények:

- A szoftver egyrészt abszorbeálja a környezetét, másrészt az adott alkalmazás részévé válik.
- A szoftverek a funkcionális és fizikai követelményeknek is eleget tesznek.

„... Software is Hard and Hardware is Soft ...”

Jó hír: szoftverrel megvalósítva sok minden lehetséges …
Rossz hír: szoftverrel megvalósítva sok minden lehetséges …

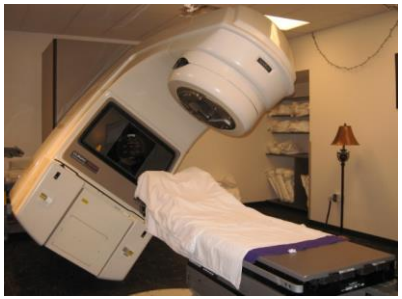
Kihívások, tanulságok:



1996. december 4. Mars Pathfinder misszió. Prioritás inverzió …

1996. június 4. Felrobbant egy Ariane 5. Szoftver hiba: 64 bites lebegőpontos -> 16 bites fixpontos ábrázolás

1993. szeptember 14. Varsó . Oldalszél , majd hirtelen hátszél + logikai hiba: túlfutás -> 2 halott, 54 sebesült …



1985 és 1987 között a Therac-25 számítógép-vezérelt sugárterápiás készülék súlyosan (~100-szoros dózis) túlterhelt hat pácienst.

Az USA-ban **1.5M** Honda Accord, CR-V és Element gépkocsit hívtak vissza: “to update the software that controls their automatic transmissions”

1991. február 25. Dahran: Egy Patriot rakéta elvételt egy scud rakétát. 28 halott, 97 sebesült. Szoftver hiba, amit február 16-án kijavítottak …

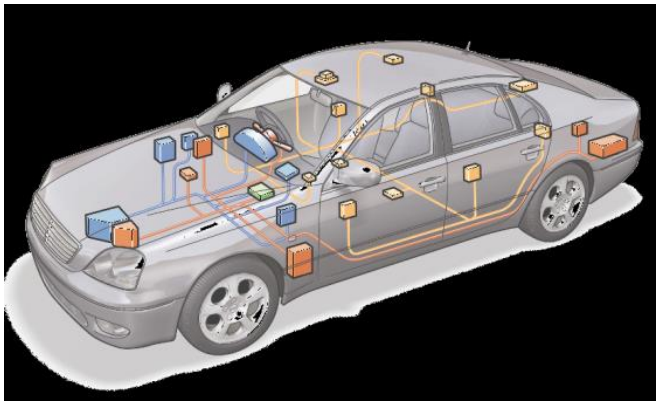
1993. augusztus 8-án lezuhant egy fly-by-wire harci-gép, mert túl lassan reagált a pilóta utasítására.

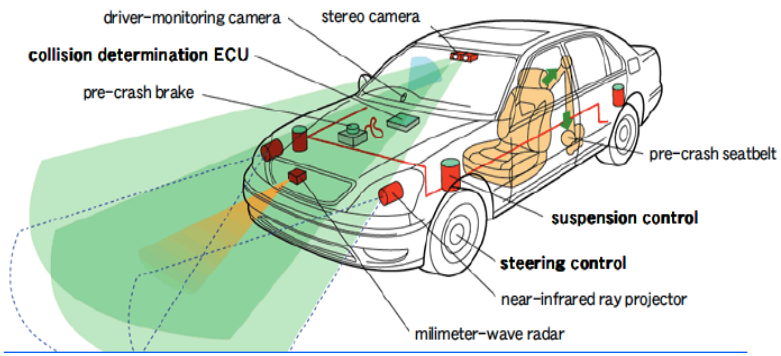
1990-2000 között 500 000 pacemakert hívtak vissza!

~75K Toyota Hybrid-et hívtak vissza: “could enter a "fail-safe“ mode that shuts down the engine, allowing only limited operation using the electric motor. The problem, caused by a software error in the Electronic Control Module (ECM) system, triggers up to five warning lights while shutting down the engine.”

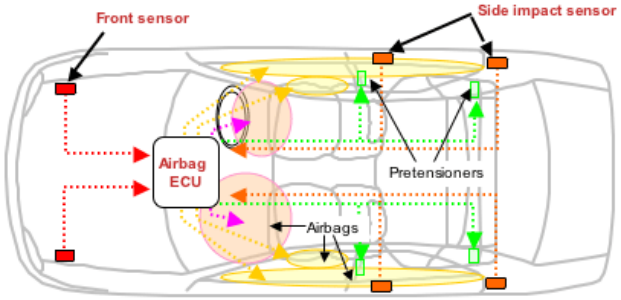
~8K Volvo S60-at hívtak vissza: to fix “ software for fuel pump units, as the software was not compatible with all fuel pumps and components.

A beágyazott eszközök együttműködése: rendszerek rendszerei





Ütközés előtti biztonsági rendszer



Légzsák rendszer

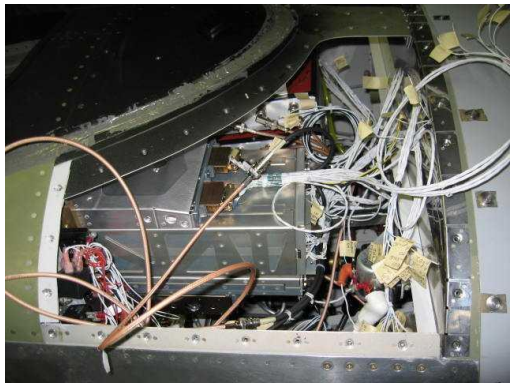
A **kábelezés** a gépkocsi 3. legdrágább alkatrésze a motor és a karosszéria után. A kábelezés a gépkocsi legnehezebb alkatrésze a karosszéria és a motor után:

átlagos súlya **100 kg**, hossza ~**5km**.

A kábelkorbács előállítási árának fele bérköltség.

Sokféle járműipari hálózat:
CAN, LIN, Flexray, MOST, TTCAN, TT-Ethernet, …

A beágyazott eszközök és az internet



IEEE 802.3 alapú **Avionic Full-Duplex Switched Internet**: Az Airbus A380, A400M és a Boing 787 Dreamliner már ezt használja!
IEEE 802.3bp szabvány bejelentés 2015-re: gépkocsikban 1 Gbit/s-os **Internet egyetlen csavart érpáron!** A piacon 2019-től!
Az Internet **embereket, adatokat, folyamatokat és tárgyakat** köt össze. A tárgyak autonóm adatszolgáltató képessége erősödik!

A tárgyak internete: a fizikai világ internet felhasználásával megvalósuló digitális-virtuális leképezése annak jobb megismerhetősége, követhetősége, valamint és befolyásolhatósága érdekében. Mindez beágyazott számítógépek és hálózataik fizikai folyamatokkal történő integrációját jelenti. Ez együtt jár olyan visszacsatolásokkal, amelyek révén fizikai folyamatok számításokat befolyásolnak, ill. megfordítva: számítások pedig fizikai rendszereket.

Az amerikai **US Food and Drug Administration** nemrégiben figyelmeztetést adott ki, hogy több mint 300 orvosi eszközt **kiber támadások** szempontjából kockázatosnak ítélt: köztük inzulin pumpákat, pacemakereket, infúziós pumpákat, érzéstelenítő berendezéseket.

Rendszerek rendszerei → Komplexitás → Biztonság?

A jövő beágyazott rendszerei: trendek és szóhasználatok

Beágyazott rendszerek (Embedded Systems)
- rendszerek beágyazott szoftverrel …

Hálózatba kapcsolt beágyazott rendszerek (Networked Embedded Systems)
- kommunikáló beágyazott rendszerek …

Rendszerek rendszerei (Systems of Systems)
- kommunikáló és kooperáló rendszerek …

Tárgyak és Szolgáltatások Internete (Internet of Things and Services)
- tárgyak és szolgáltatások kommunikációja és kooperációja …

Kiber-fizikai rendszerek (Cyber-Physical Systems)
- beágyazott rendszerek és a globális hálózatok integrációja

a felhasználó (emberiség) „beágyazása” érdekében!

Cél az új minőség:
mindenki életvitelében, az egészségügyi ellátásában, az élelmiszer termelésben és ellátásban, az idősekről és az elesettekről történő gondoskodásban,
és mindezek érdekében
az energiagazdálkodásban, a közlekedésben, a környezetvédelemben, a katasztrófák elleni védelemben, az élet- és vagyonvédelemben, …

Európai kezdeményezések:

FP5, FP6, FP7 programok, Eureka ITEA, ARTEMIS: Advanced Research & Technology for Embedded Intelligent Systems, Horizon 2020 előkészítés, CHIST-ERA, Alliance for Internet of Things Innovation (AIOTI), Industry 4.0, ...

Kiemelt alkalmazási területek:

- Hatékony és biztonságos mobilitás (szárazföldi és légi, …)
- Jólét és egészség (otthoni-kórházi ápolás, …)
- Fenntartható termelés (élelmiszer, energia, bányászat, …)
- Intelligens közösségek (intelligens és biztonságos városok, terek, …)

A kihívások és lehetőségek címszavai: biztonságkritikus rendszerek, virtuális világ, nagymennyiségű adat, rendszerek rendszerei, felfő szolgáltatások, autonóm, adaptív és prediktív szabályozás, tárgyak internete, számítások sokmagú processzorral.

+ Horizon 2020: Leadership in enabling and industrial technologies

Smart Cyber-Physical Systems ICT-01-2014, ICT1.1-2016
Smart System Integration ICT-02-2014, ICT1.3-2016
Smart Anything Everywhere Initiative ICT1.4-2016
IoT and Platforms for Connected Smart Objects ICT-30-2015
R&I on IoT integration and platforms ICT7.3 – 2016

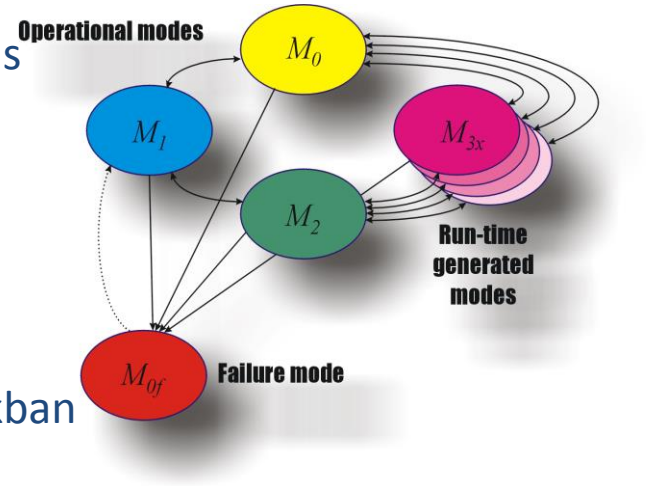
Kihívások, feladatok, további megalapozó kutatások

Az adat- és jelfeldolgozás területén:

A valós idejű adat minősége és a kapcsolódó feldolgozás lehetőségei
- Adat pontosság/érvényesség/elévülés, adatvesztés
- Nem egyenletes mintavételezés, órák és adatok szinkronizációja
- Kvantálási hibák időben és amplitúdóban
- Modellillesztés, modell-alapú és adaptív jelfeldolgozás

a rendszer- és irányításelmélet területén:

A többszintű és elosztott rendszerek irányítása
- Hálózatba kapcsolt rendszerek stabilitása, passzivitás alapú rendszerek
- Adaptivitás és kooperativitás: átkapcsolás és újrakonfigurálás, tranziens menedzsment
- Hibrid rendszerek, hibrid szimuláció: hardver-a-hurokban
- Robusztusság, szolgáltatásbiztonság, hibatűrés

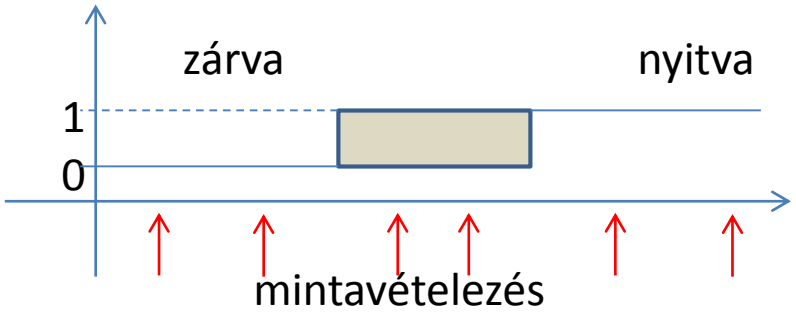


a szoftver rendszertechnika területén:
- Modell-alapú rendszertervezés
- Beágyazott virtualizáció, beágyazott rendszerek felhőben

+ a fejlesztési technológiákhoz, rendszer és hálózati szoftverekhez, a verifikációs, validációs és tanúsítási eszközökhöz kötődő szerteágazó K+F+I

Mennyiségek, változók valós idejű rendszerekben

- ***Real-time változók*** (RT entities): állapotváltozók, mint pl. folyadék áram, szabályozó alapjele, szabályozó szelep kívánt pozíciója. Vannak statikus és időben változó, dinamikus attribútumai.
- Minden *RT változó* annak az alrendszernek az ún. befolyásolhatósági tartományában (sphere of control, SOC) van, amelyik jogosult értékét megváltoztatni. Azon kívülről a *RT változó* csak olvasható.
- Egy *RT változó* lehet diszkrét vagy folytonos értékű.
- A diszkrét *RT változó* lehet definiálatlan. Példa: nyíló garázsajtó: nincs se nyitva, se csukva.



Mennyiségek, változók valós idejű rendszerekben

- ***Megfigyelések:*** a RT változó értékei adott időpont(ok)ban.
  - ***Megfigyelés =<név, megfigyelési idő, érték>***
- *Megfigyelések elosztott rendszerekben:* ha nincs globális óra, akkor az időbélyeg használhatósága korlátozott, megfigyelési időnek sokszor az üzenet érkezési idejét veszik. Ezzel jelentős hibát okozhatunk az állapotbecslésben.
- *Indirekt megfigyelések:* sokszor a megfigyelendő mennyiség közvetlenül nem férhető hozzá. Ilyenkor közvetett megfigyeléseket végzünk modellek felhasználásával. (Például belső hőmérséklet megfigyelése a felszínen elhelyezett érzékelőkkel).
- *Állapot megfigyelések:* minden megfigyelés önállóan értelmezhető értéket ad. Jellegzetesen periodikus mintavételezéssel végezzük.
- *Esemény megfigyelések:* az esemény adott időpontban bekövetkező állapotváltozás. Mivel maga a megfigyelés is egy esemény, ezért nem lehetséges egy esemény közvetlen megfigyelése az irányított objektumban, csak annak következményeit tudjuk megfigyelni.

Mennyiségek, változók valós idejű rendszerekben

- ***Real-time változók képe*** (RT images): a RT változó megfeleltetése a számítógépes programban, amelynek értelmezzük az időbeni és az amplitúdó szerinti pontosságát, valamint az időbeni érvényességét. Egy RT változó képe aktuális állapot, ill. esemény megfigyelés, vagy állapot becslés.
- ***Real-time objektumok*** (RT objects): Egy RT objektum az elosztott rendszer csomópontján belül egy olyan tároló, amely egy RT változót, vagy annak képét tartalmazza. Minden ilyen objektumhoz tartozik egy előírt pontosságú óra. Amikor ez üt, egy objektum eljárás aktiválására kerül sor. Ha ez periodikus, akkor szinkron RT objektumról beszélünk. Elosztott RT objektumról beszélünk, ha a különféle csomópontokban másolat formájában van jelen. Erre jó példa a globális óra, amelynek Π együttfutású másolatait hozzuk létre az egyes csomópontokban.

Mennyiségek, változók valós idejű rendszerekben

- ***Időbeni pontosság:*** A megfigyelések révén szerzett információ időbeni megjelenése a számítógépes programban és tényleges megfigyelés tényleges időpontja óhatatlanul eltérnek egymástól. Az időbeni pontosság azzal a $d_{pontosság}$ intervallummal definiálódik, amelyhez tartozóan bekövetkező amplitúdó hiba még éppen elviselhető a vezérelt rendszer szempontjából.
- *Példa:* az alábbi táblázatban néhány gépjármű motor jellemző szerepel együtt a megkívánt amplitúdó pontossággal és az ennek megfeleltethető időintervallumokkal.

RT kép a számítógépben	max. változás	pontosság	időbeni pontosság
Dugattyú pozíció	6000 ford/perc	0.1°	3µsec
Gázpedál pozíció	100%/sec	1%	10 msec
Motor terhelés	50%/sec	1%	20 msec
Olaj és hűtővíz hőmérséklet	10%/perc	1%	6 sec

Az RT képek pontossági intervallumai között több, mint 6 nagyságrend eltérés van. A dugattyú pozíció esetében ez a pontosság praktikusan csak állapotbecsléssel (a programon belüli jóslással) lehetséges.

Mennyiségek, változók valós idejű rendszerekben

A megfigyelés és a felhasználás között eltelt idő egy *v* változó esetén a következő hibát okozza:

$$hiba(t) \cong \frac{dv(t)}{dt}\left[C(t_{felhasználás}) - C(t_{megfigyelés})\right]$$

Ha egy időben pontos RT képet használunk, akkor a *worst-case* hiba:

$$hiba = \underbrace{\max}_{\forall t}\left|\frac{dv(t)}{dt}\right| d_{pontosság}$$

Kiegyensúlyozott tervezés esetén ez utóbbi az amplitúdó mérési hiba nagyságrendjébe kell essen. Ahhoz, hogy az RT képre alapozott számításaink pontosak legyenek, be kell tartanunk az alábbi feltételt

$$\left|C(t_{felhasználás}) - C(t_{megfigyelés})\right| \leq d_{pontosság}$$

Mennyiségek, változók valós idejű rendszerekben

Példa az időbeni érvényességre:

1993. szeptember 14, varsói repülőtér: egy Lufthansa A320-as Airbus túlszaladt a kifutópályán: 2 halott, 54 sebesült. A balesetet az okozta, hogy a gép kilenc másodpercig csak az egyik oldali kerekén támaszkodott, ezért a fékező mechanizmusok bekapcsolása nem történt meg, mivel annak feltételeként a vezérlő logikában mindkét (fő)kerék földet érését írták elő. Valójában az a következtetés, hogy *"a repülőgép még a levegőben van, ezért a fékező mechanizmusok nem aktiválhatók"* időben érvénytelenné vált abban a pillanatban, amikor az egyik kerék földet ért.

Egy periódikusan frissített RT képet ***parametrikusnak***, vagy ***fázis-érzéketlennek*** hívunk, ha

$$d_{pontosság} > \left(d_{frissítés} + WCET_{\text{üzenet továbbítás}}\right).$$

A parametrikus RT kép a vevő oldalon bármikor felhasználható anélkül, hogy a beérkezés és a felhasználás fázisviszonyait mérlegelni kellene: még a pontossági időn belül megjön a frissítés.

Mennyiségek, változók valós idejű rendszerekben

Egy periodikusan frissített RT képet *fázis-érzékenynek* hívunk, ha

$$WCET_{\text{üzenet továbbítás}} < d_{pontosság} < \left(d_{frissítés} + WCET_{\text{üzenet továbbítás}}\right).$$

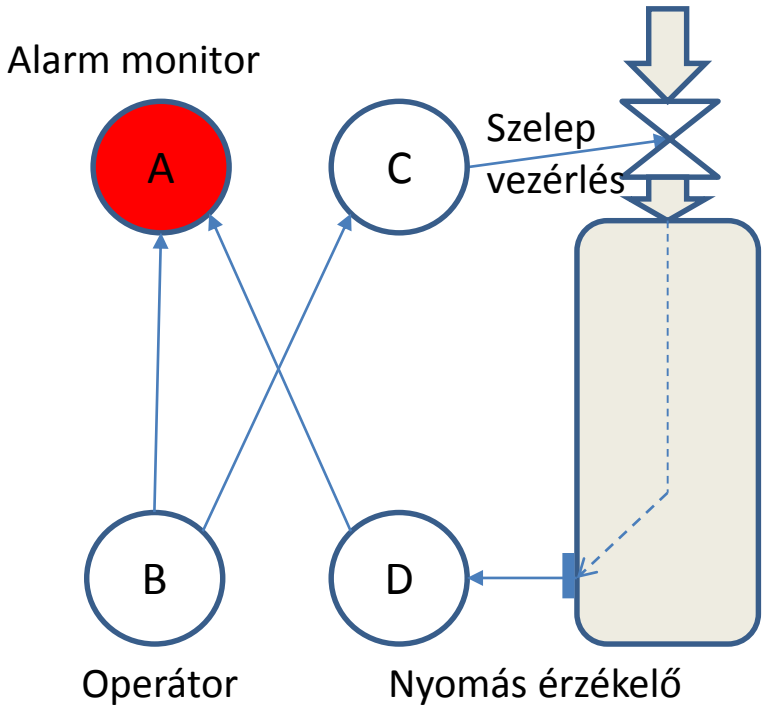
Ilyenkor nem biztos, hogy a pontossági időn belül megjön a frissítés, ezért a frissítés és a felhasználás idejére oda kell figyelni.

Példa: A fenti táblázatban szereplő gázpedál pozíció továbbítási ideje 4 *msec*. Ha ekkor a periodikus lekérdezés üteme kisebb, mint 6 *msec*, akkor az RT kép *parametrikus*, ha pedig pl. 8 *msec*, akkor pedig *fázis-érzékeny*.
A fázis érzékenységet megfelelő mintavételi frekvenciával, vagy állapotbecslés alkalmazásával kerülhetjük el.

Állandóság (Permanence). Jelentése: megmarad/stabilizálódik/érvényessé válik az üzenet állapota. Egy üzenet akkor válik állandóvá/megmaradóvá/érvényessé, amikor a vevő csomópont tudja, hogy minden, a jelen üzenet küldési ideje előtt elküldött üzenet már meg kellett érkezzen, vagy sosem fog megérkezni.

Mennyiségek, változók valós idejű rendszerekben

Példa: Egy tartályban lévő nyomást monitorozunk egy elosztott rendszerrel. ***A*** csomópont: alarm monitor, ***B*** csomópont: operátor, ***C*** csomópont: szabályzó szelep, ***D*** csomópont: nyomás érzékelő. Lehetséges üzenetek: $\mathbf{M}_{DA}$: jelzi, hogy a nyomás hirtelen megváltozott, $\mathbf{M}_{BC}$: operátori parancs a változtatásra, $\mathbf{M}_{BA}$: nincs alarm helyzet, mert operátori beavatkozás volt. Van egy eltakart, a fizikai rendszer működéséből adódó csatorna a szelep és a nyomásérzékelő között. Téves riasztás jöhet létre, ha a $B \rightarrow \mathrm{C} \rightarrow D \rightarrow A$ láncon gyorsabban fut végig az információ, mint a $B \rightarrow A$ láncon. Ennek elkerülése érdekében az alarm monitor minden akcióját késleltetni kell. (Bizonyos akciók visszavonhatatlanok: pilóta katapultál, lőfegyver elsül, stb.)



Vegyük észre, hogy maga a technológia
Is kommunikációs csatornát valósít meg!

Mennyiségek, változók valós idejű rendszerekben

Akció késleltetési idő: (action delay) amíg érvényessé nem válik az üzenet (ezt mindig ki kell várni). Számítása, ha (1) van globális óra:

$$t_{érvényes} = t_{küld} + d_{max} + 2g,$$

ahol g az óra felbontása, ha (2) nincs globális óra:

$$t_{érvényes} = t_{küld} + 2d_{max} - d_{min} + g_l\ ,$$

ahol g_l a lokális óra felbontása. Látható, hogy a második esetben $d_{max} - d_{min}$ idővel többet kell várni, mert valójában a küldés ideje nem ismert, míg az első esetben a küldés időpontja az üzenet részeként elküldhető.

Megjegyzés:

(1) Az akció késleltetési idő számítására vonatkozó gondolatmenet megértését segíti, ha elképzelünk egy külső megfigyelőt, aki minden időpontot ismer, és tisztában van azzal is, hogy az egyes csomópontokban mi ismert és mi nem.

(2) (2) Egy RT kép csak az állandóság bekövetkezése után használható. Ha ez nagyobb, mint az RT kép időbeni pontossága, akkor csak az állapotbecslés segíthet.

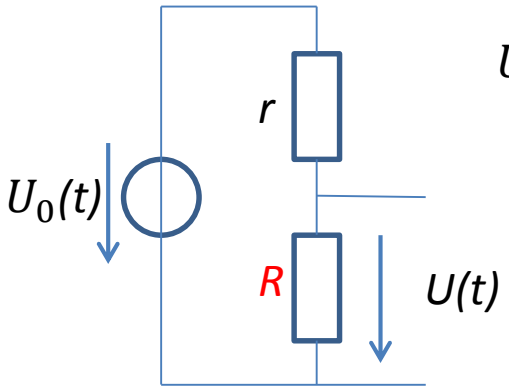
Mennyiségek, változók valós idejű rendszerekben

Idempotencia: Ha ugyanaz az üzenet – tipikusan hibatűrési céllal – többször is megérkezik ugyanarra a csomópontra, akkor ezt az üzenethalmazt idempotensnek nevezzük, ha a a többszöri azonos üzenet hatása ugyanaz, mint az egyszerié. Ez a fogalom azért fontos, mert ha az üzenet úgy konstruáljuk meg, hogy az megváltozást hordozzon, akkor a többszöri üzenetküldés többszöri "korrekciót" eredményez, miközben csak egyszerit szerettünk volna.

Példa: szelep-állás 45° (állapot üzenet) ↔ szelep-állás változás 5° (esemény üzenet).

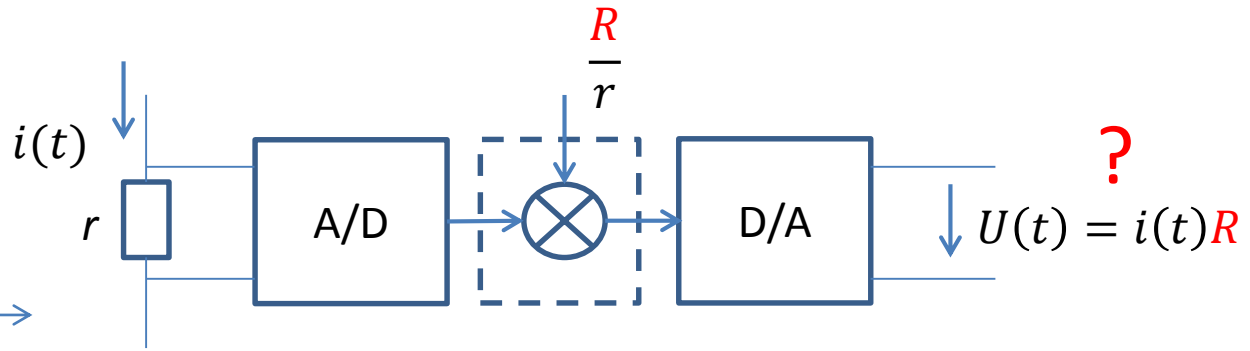
CPS rendszerek modellezési kérdései

Példa: Készítsünk programozható feszültségosztó áramkört-berendezést!

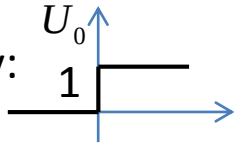


$$U(t) = U_0(t)\frac{R}{r+R} \qquad U(t) = i(t)R \qquad i(t) = \frac{U_0(t)}{r+R}$$

R legyen változtatható! Tegyük R helyébe az alábbi áramkört!



Következmény:



$$i(t=0) = \frac{U_0}{r} \qquad U(t=0) = 0$$

µP, DSP, "felhő", …

$$U(t) = Ri(t-\Delta t)$$

$$i(t=\Delta t) = \left(U_0 - R\frac{U_0}{r}\right)\frac{1}{r} = \left(1-\frac{R}{r}\right)\frac{U_0}{r} \qquad U(t=\Delta t) = R\frac{U_0}{r}$$

$$i(t=2\Delta t) = \left[U_0 - R\left(1-\frac{R}{r}\right)\frac{U_0}{r}\right]\frac{1}{r} = \left(1-\frac{R}{r}+\left(\frac{R}{r}\right)^2\right)\frac{U_0}{r} \qquad U(t=2\Delta t) = R\left(1-\frac{R}{r}\right)\frac{U_0}{r}$$

CPS rendszerek modellezési kérdései

$$i(t = n\Delta t) = \left(1 - \frac{R}{r} + \left(\frac{R}{r}\right)^2 \mp \cdots \pm \left(\frac{R}{r}\right)^n\right)\frac{U_0}{r} \to \frac{U_0}{r+R}$$

$$U(t = n\Delta t) = R\left(1 - \frac{R}{r} + \left(\frac{R}{r}\right)^2 \mp \cdots \mp \left(\frac{R}{r}\right)^{n-1}\right)\frac{U_0}{r} \to U_0\frac{R}{r+R}$$

Ha $\frac{R}{r} < 1$