TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Arvutitehnika instituut
ati.ttu.ee

Sardsüsteemid
(Embedded Systems)

III Loeng

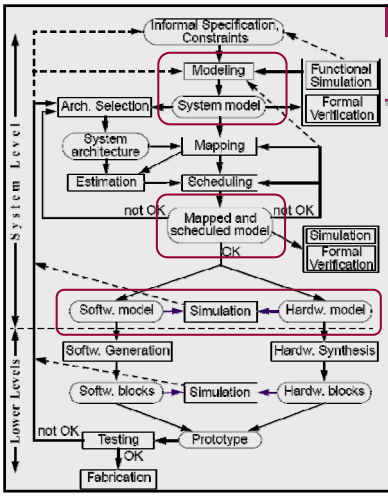
Gert Jervan
Arvutitehnika instituut

www.pld.ttu.ee/~gerje

Graphics: © Alexandra Nolte, Gesine Marwedel, 2003

Osa materjale: Petru Eles, Peter Marwedel

Disainivoog



Ülevaade

- ✓ Sardüsteemid ja usaldusväärsus
- ✓ Võimsus- ja energiatarve
- ✓ Arhitektuurid
- ✓ Protsessorid
- ✓ Platvormid

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Arvutitehnika instituut
ati.ttu.ee

Sardsüsteemid ja usaldusväärsus

Tallinna Tehnikaülikool
Arvutitehnika instituut

Nõudmised usaldusväärsusele

- ✓ **Sardsüsteemid peavad olema usaldusväärsed (dependable)**
- ✓ On süsteeme, kus lubatakse vaid 1 rike 10^9 töötunni kohta, see tähendab 1 rike 114 000 aasta kohta
  - ~ 1000 korda väiksem tüüpilisest kiipide rikete arvust.
  - Ohutuskriitilistes süsteemides peavad süsteemid olema töökindlamad, kui selle komponendid individuaalselt.
  - Tuleb kasutada veakindlust suurendavaid mehhanisme.
- ✓ Madal lubatud rikete arv → süsteemid ei saa olla 100% testitavad.
  - Ohutus on kombinatsioon testimisest ja analüüsist. Liskas peab arvestama nii disaini käigus tehtud vigadega kui ka inimeste poolt põhjustatud riketega.

Veakindlus

- ✓ Veakindlaks nimetatakse süsteeme, mis jätkavad oma ettenähtud ülesannete täitmist isegi siis, kui esinevd rikked:
  - riistvaras
  - tarkvaras
  - kasutaja eksimused
  - keskkond, sisendandmed, ...
- ✓ Veakindlus on eeldus, mis võimaldab süsteemil saavutada veakindla opereerimise

Põhikontseptsioon

- **Veakindlus (fault tolerance)** on väga tihedalt seotud **usaldusväärsusega (dependable)**,
  - **Töökindlus (Reliability)** ***R(t)*** **=** tõenäosus, et süsteem töötab korralikult kui ta töötas ajahetkel *t*=0
  - **Remonditavus (Maintainability)** ***M(d)*** **=** tõenäosus, et süsteem töötab taas korralikult d ajaühikut peale vea esinemist.
  - **Töövalmidus (Availability *A*(*t*))**: Tõenäosus, et süsteem töötab ajahetkel *t*
  - **Ohutus (Safety)**: Süsteem ei põhjusta kahju.
  - **Turvalisus (Security)**: Konfidentsiaalne ja usaldatav kommunikatsioon

Isegi ideaalselt loodud süsteemid võivad läbi kukkuda, kui eeldused süsteemi töökoormuse võimalike vigade kohta on valed.
Süsteeme ei saa teha usaldusväärseks tagantjärgi, vaid sellega tuleb arvestada süsteemi loomise algusest alates.

Põhiterminoloogia

- ✓ Viga (fault): süsteemis esinev defekt või situatsioon, mis võib viia süsteemi töö tõrkeni
- ✓ Rike: vea avaldumie – vale käitumine
- ✓ Tõrge: süsteem ei täida oma ettenähtud funktsiooni

Viga → Rike → Tõrge

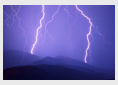
Vigade näited

- ✓ Bit-flipid seoses kosmilise kiirgusega:
  - A person on an airplane over the Atlantic at 35,000 ft working on a laptop with 256 Mbytes (2 Gbits) of memory. At this altitude, the soft error rate (SER) of 600 FITs per megabit becomes 100,000 FITs per megabit, resulting in a potential error every five hours.
  - 1 FIT (failures in time), is the number of failures in 1 billion device-operation hours. A measurement of 1000 FITs corresponds to a MTTF (mean time to failure) of approximately 114 years.

Vigade klassifikatsioon

- ✓ Püsivad: viga on stabiilne ja alaline
  - Vigane komponent tuleb asendada
  - Klassikaline näide: *stuck-at* vead

- ✓ Perioodilised rikked (intermittent)
  - Esinevad ajutiselt, seoses süsteemi või selle komponentide ebastabiilsusega (näiteks ebakindel ühendus)
- ✓ Ajutised rikked (transient)
  - Viga, mis lähtub ajutistest keskkonnamõjudest
  - Näiteks pingelang või EMI



Äikesetormid

Tõrgete klassifikatsioon

- ✓ Domain/Nature
  - Value failure
  - Timing failure
- ✓ Perception
  - Consistent failure
  - Inconsistent failure
- ✓ Effect
  - Benign failure
  - Malign/catastrophic failure
- ✓ Frequency
  - Single failure
  - Repeated failure

Tõrked (Failures)

- ✓ **Crash** Failure: After an error has been detected, the component stops silently.
- ✓ **Omission** Failure: Sometimes a result is missing; when result is available, it is correct.
- ✓ **Consistent** Failure: If there are multiple receivers, all see the same erroneous result.
- ✓ **Byzantine** (Malicious, Asymmetric) Failure: Different receivers see differing results.

Tõrked (2)

- **Timing** Failure: A server's response lies outside the specified time interval.
- **Response** Failure: The server's response is incorrect (value of the response is wrong, server deviates from the correct flow of control).
- **Arbitrary** Failure: A server may produce arbitrary responses at arbitrary times.

Vigadega toime tulemine

- Vigade ellimineerimine: eemalda probleemide algusallikad
  - Kõrvalda defektid: test & debug
  - Robustne disain: vähendab defektide tõenäosust
  - Vähenda keskkonnamõjusid: kaitsmed

Võimatu on vältida kõiki vigu

- Veakindlus: liiasuse lisamine, et vigu maskeerida
  - Vaja on täiendavaid ressursse
  - Näited:
    - Error correcting codes (Hamming, Red Solomon), hääletamine, maskeerimine, kontrollsummad...
    - Backup, replication, ...

Veakindluse saavutamine

- **Vigade avastamine** on protsess, et tuvastada vigade esinemist. Veakindluse saavutamise esmaseid tegevusi. Näiteks error detection codes, isekontrollivad loogikaskeemid, timerid, jne...
- **Vigade lokaliseerimine** on protsess, et tuvastada, kus viga on toimunud, et alustada vastava taastamisprotseduuriga

Veakindluse saavutamine

- **Vigade piiritlemine** on protsess, et viga isoleerida ja vältida selle mõju süsteemi ülejäänud osadele (vältida levimist)
- **Veast taastumine** on protsess, mille käigus süsteem püüab jääda tööle või taastada oma töövõime läbi rekonfiguratsiooni (isegi, kui rike on süsteemis alles). Näited: vigade maskeerimine, kordamine, tagasipöördumine jne...

Definitsioonid

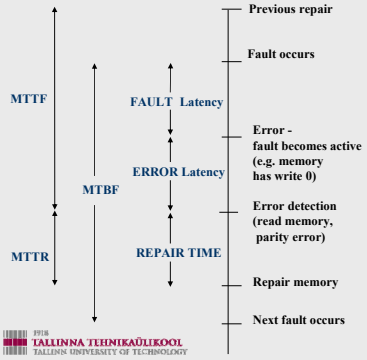
- Tõrgete sagedus (λ):
  - Keskmine sagedus, millega tõrked tekivad.

$$\frac{6\ failures}{7502\ hrs} = 0.0007998\ failures/hr = 799.8 \times 10^{-6}\ failures/hr$$

- Mean time to failure (MTTF):
  - Average time between failures

$$MTTF = \frac{1}{\lambda}$$

Usaldusväärsus



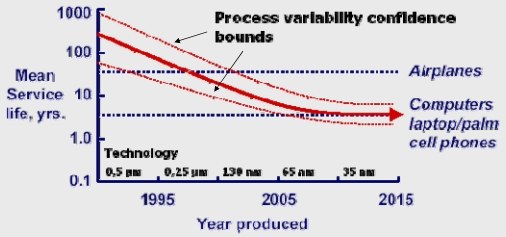
Reliability (Töökindlus):
a measure of the continuous delivery of service;
R(t) is the probability that the system survives (does not fail) throughout [0, t];
expected value: *MTTF(Mean Time To Failure)*

Maintainability (Remonditavus):
a measure of the service interruption
M(t) is the probability that the system will be repaired within a time less than t;
expected value: *MTTR (Mean Time To Repair)*

Availability (Töövalmidus):
a measure of the service delivery with respect to the alternation of the delivery and interruptions
A(t) is the probability that the system delivers a proper (conforming to specification)service at a given time t.
expected value: *EA = MTTF / (MTTF + MTTR)*

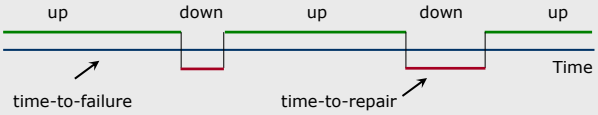
Safety (Ohutus):
a measure of the time to catastrophic failure
S(t) is the probability that no catastrophic failures occur during [0, t];
expected value:
MTTCF(Mean Time To Catastrophic Failure)

Kiipide töökindluse hindamine



*Extrapolated from ITRS roadmap, MRQW-2002, Bernstein

Töövalmidus



$$Availabili\ ty = \frac{MTTF}{MTTF + MTTR}$$

- ✓ Töövalmidus:
  - Probability that system is operational at time *t*
- ✓ Kõrge töövalmidus:
  - MTTF → infinity (high reliability)
  - MTTR → zero (fast recovery)

Remonditavus

- ✓ *M(t)* on tõenäosus, et vigane süsteem on võimalik uuesti töökorda viia ajaperioodi *t* jooksul.
- ✓ Taastamise protsess:
  - Vea lokaliseerimine, näiteks läbi diagnostika
  - Süsteemi parandamine
  - Süsteemi töövalmidusse toomine

Graceful Degradation

- ✓ The ability of system to automatically decrease its level of performance to compensate for hardware failure and software errors.

Töövalmiduse üheksate müüt

Üheksaid	Töövalmidus	Rikkeaeg aastas	Rikkeaeg nädalas	Näide
2 üheksat	99%	3.65 päeva	1.7 tundi	Tavaline veebikülg
3 üheksat	99.9%	8.75 tundi	10.1 min	E-kaubandus
4 üheksat	99.99%	52.5 min	1.0 min	Suur mailiserver
5 üheksat	99.999%	5.25 min	6.0 s	Telefonisüsteem
6 üheksat	99.9999%	31.5 s	0.6 s	Carrier-grade andmeside

Ajalooline areng

- ✓ Mean Time Between Failures:

$$MTBF = MTTR + MTTF$$

- ENIAC. MTBF: 7 minutit (18000 elektronlampi)
- F-8 Crusader – esimene fly-by-wire
  - MD-11
  - A320 family
- Patriot raketikaitse süsteem
  - Vajas rebooti iga 8 tunni järel. Sellest saadi teada väga valusal moel esimese lahesõja ajal...

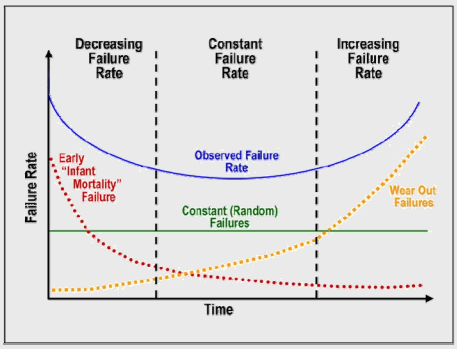
Ultra-töökindlad süsteemid

- Airbus A320 perekonna fly-by-wire süsteem:
  - Kõik täiturid on arvutite poolt kontrollitavad
  - Ei mingeid juhttrosse ega kaableid
  - 5 keskset lennuarvutit
  - Kasutatakse erinevaid riistvaralisi lahendusi
    - Thomson CSF => 68010
    - SFENA => 80186
  - Tarkvara mõlemale platvormile on kirjutatud erinevate tarkvaraloojate poolt (sõltumatult)
  - Kogu rikete avastamine & debug teostati eraldi
  - Arvuti lubab piloodil lennata mingite ettenähtud parameetrite piires (flight envelope)
    - väljaspool seda võtab arvuti juhtimise üle

Riistvara ja keskkonna tõrked

- Liikuvad osad, suur kiirus, madal tolerants, suur keerukus: kettad, tape drives/libraries
- Madalaim MTBF on ventilaatoritel ja toiteallikatel
- Tihti ventilaatorid "väsivad" → väikesed juhuslikud rikked CPUs, mälus, backplane'is
- Keskkond: Vool, jahutus, niiskus, kaablid, tuli, kokku kukkuvad rackid, ventilatsioon, tormid, ...

Vanni kõver



Kopetz'i 12 disainipõhimõtet (1-3)

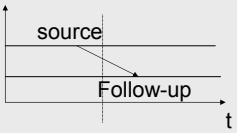
1. Safety considerations may have to be used as the important part of the specification, driving the entire design process.
2. Precise specifications of design hypotheses must be made right at the beginning. These include expected failures and their probability.
3. Fault containment regions (FCRs) must be considered. Faults in one FCR should not affect other FCRs.

Passenger compart-ment stable

Safety-critical & non-safety critical electronics

Kopetz'i 12 disainipõhimõtet (4-6)

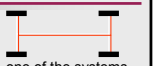
4. A consistent notion of time and state must be established. Otherwise, it will be impossible to differentiate between original and follow-up errors.
5. Well-defined interfaces have to hide the internals of components.
6. It must be ensured that components fail independently.



2 independent brake hose systems

Kopetz'i 12 disainipõhimõtet (7-9)

7. Components should consider themselves to be correct unless two or more other components pretend the contrary to be true (principle of self-confidence).
8. Fault tolerance mechanisms must be designed such that they do not create any additional difficulty in explaining the behavior of the system. Fault tolerance mechanisms should be decoupled from the regular function.
9. The system must be designed for diagnosis. For example, it has to be possible to identifying existing (but masked) errors.



one of the systems sufficient for braking

Kopetz'i 12 disainipõhimõtet (10)

10. The man-machine interface must be intuitive and forgiving. Safety should be maintained despite mistakes made by humans


airbag

Kopetz'i 12 disainipõhimõtet (11-12)

11. Every anomaly should be recorded. These anomalies may be unobservable at the regular interface level. Recording to involve internal effects, otherwise they may be masked by fault-tolerance mechanisms.

12. Provide a never-give up strategy. ES may have to provide uninterrupted service. Going offline is unacceptable.

IAF0030
Arvutitehnika erikursus I

Veakindlad arvutisüsteemid
Fault Tolerant Computer Systems

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Arvutitehnika instituut
ati.ttu.ee

Energia- ja võimsustarve

Tallinna Tehnikaülikool
Arvutitehnika instituut

Miks on energiatarve nii oluline?

- ✓ Kaasaskantavad süsteemid – aku eluiga!
- ✓ Süsteemid väga limiteeritud energiaeelarvega: Mars Pathfinder, UAV
- ✓ Desktopid ja severid: väga suur võimustarve
  - Tõstab temperatuuri ning vähendab jõudlust ning usaldusväärsust
  - Tõstab vajadust kallite jahutusmehhanismide järele
- ✓ Üks kõrge jõudlusega kiipide loomise põhitakistusi on kuumuse eemaldamine
- ✓ Suur võimsustarve toob kaasa ka majanduslikud ja keskkonna-alased probleemid (green computing)

Võimsustarve CMOS tehnoloogia seadmetes

- ✓ CMOS (Complementary Metal-Oxide Semiconductor)

Dünaamiline Staatiline

$$P = \underbrace{\frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW}}_{\text{Ümberlülitused}} + \underbrace{Q_{SC} \cdot V_{DD} \cdot f \cdot N_{SW}}_{\text{Lühised}} + \underbrace{I_{leak} \cdot V_{DD}}_{\text{Lekked}}$$

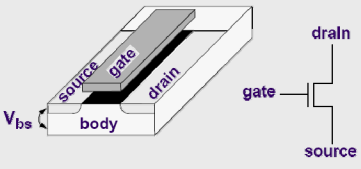
Ümberlülitused Switching Power | Lühised Short circuit power | Lekked Leakage power

- C = node capacitances
- N_{SW} = switching activities (number of gate transitions per clock cycle)
- f = frequency of operation
- V_{DD} = supply voltage
- Q_{SC} = charge carried by short circuit current per transition
- I_{leak} = leakage current

Power, Energy, Voltage, Power consumption
Võimsus, energia, pinge, võimsustarve

Võimsustarve CMOS tehnoloogia seadmetes (2)

CMOS transistor (N-type)



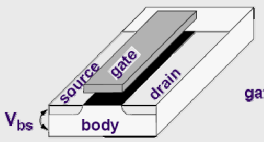
Threshold voltage:
- **The minimal voltage required at the gate to turn on the transistor**

V_{bs} = body bias voltage
V_{th} = threshold voltage

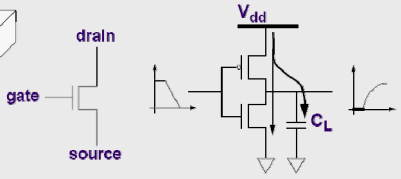
$V_{DD, max}$ = 3,3 V → V_{th} ≈ 0,8 V

Võimsustarve CMOS tehnoloogia seadmetes (3)

CMOS transistor (N-type)



CMOS inverter



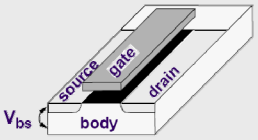
V_{bs} = body bias voltage
V_{th} = threshold voltage
V_{dd} = supply voltage
C_L = output load capacitance

Dynamic power

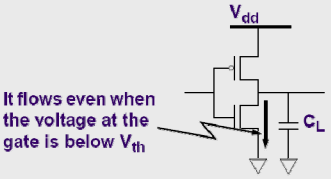
- Charging and discharging the output load capacitance
- Momentary short circuits at a gate's output

Võimsustarve CMOS tehnoloogia seadmetes (4)

CMOS transistor (N-type)



CMOS inverter



V_{bs} = body bias voltage
V_{th} = threshold voltage
V_{dd} = supply voltage
C_L = output load capacitance

Static power

- Subthreshold leakage conduction
- Junction leakage (drain and source to body)

Võimsustarve CMOS tehnoloogia seadmetes (5)

- ✓ Pikka aega on lekkevoolu võimsust peetud tühiseks võrreldes dünaamilise võimsusega
- ✓ Tänapäeval on need kaks saanud võrreldavateks
- ✓ Tehnoloogia arenemisel alla 65 nm hakkab lekkevoolu võimsus ületama dünaamilist

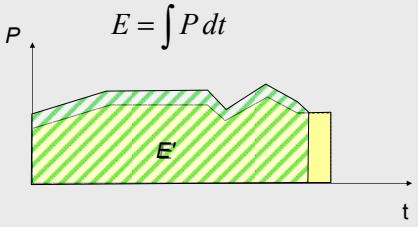
Võimsustarve CMOS tehnoloogia seadmetes (5)

- ✓ Lekkevool eksisteerib isegi siis kui seadmed ei ole kasutuses (standby). Ainukene võimalus vabaneda sellest on toiteallika eemaldamine
- ✓ Lühiste energia on ca 10% kogu energiast
- ✓ Lülituste energia on tänapäevastes kiipides endiselt suurim probleemide allikas
- ✓ Edaspidiselt räägime vaid lülituste energiast, kui ei ole mainitud midagi eraldi

Võimsus ja energia

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW}$$

$$E = \int P\,dt$$



- ✓ Paljudel juhtudel tähendab kiirem täitmine ka vähem energiat kuid see võib olla ka vastupidi, kui kiirema täitmise saavutamiseks tuleb võisust tõsta

Võimsustarve v. energiatarve

- ✓ Võimsustarbe vähendamine on oluline:
  - Toiteallika disainil
  - Pingeregulaatorite disainil
  - Ühenduste dimensioneerimisel
  - Lühiajalisel jahutamisel
- ✓ Energiatarbe vähendamine on oluline:
  - Piiratud energiaressursiga süsteemides (i.e. mobiilsed süsteemid)
    - limiteeritud aku
    - kallis energia
  - Jahutus
    - kõrge hind
    - limiteeritud pind
  - Usaldusväärsus
  - Pikk eluiga, madalad temperatuurid

Võimsus/energiatarbe vähendamine

- Põhilised võimalused:
  - Toitepinge vähendamine
  - Ümberlülituste arvu vähendamine
  - Mahtuvuse vähendamine
  - Tsüklite arvu vähendamine

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW}$$

$$E = \int P\,dt$$

Võimsus/energiatarbe vähendamine (2)

- Skeemi tasemel
  - Transistoride ümberjärjestamine (mõjutab mahtuvust)
  - Transitoride suurused
- Loogikatasemel
  - "Don't care" (X) optimeeriminem et vähendada ümberlülituste arvu
  - "Valede" ümberlülituste vähendamine läbi viidete ühtlustamise
  - Tehnoloogia sidumine
  - Olekute sobiv kodeerimine, et vähendada ümberlülituste arvu olekumuutusel
  - Kodeerimine, et vähendada ümberlülituste arvu siinil või ALUs
  - Gated clocks

Võimsus/energiatarbe vähendamine (3)

- Käitumuslikul tasemel
  - Planeeri ja seo ülesanded sedasi, et tsüklite arv oleks väiksem (rohkem tegevust ühe takti jooksul) → väiksem töökiirus → madalam toitepinge
  - Hõiva ja jaga mooduleid sedasi, et võimsustarve oleks väiksem

Võimsus/energiatarbe vähendamine (4)

- Arhitektuursel tasemel
  - Spetsiaalne käsustik, andmeosa ja registrite struktuur, mis vastaksid valitud arhitektuurile, eesmärgiga võimsuse vähendamine
    - Kiibil asuvad ja töötavad ainult need ressursid, mida tõesti vaja on
  - Siini võimsustarbe vähendamine
    - Väiksem ümberlülituste arv: tark kodeerimine, aadressisiini lülituste arvu vähendamine kasutades korrelatsioone
    - Siini pikkuse vähendamine ressursside õige paigutamise teel (vähendab mahtuvust)
    - Siini segmentideks jaotamine: pika suure koormusega siini jaotamine kohalikeks segmentideks

Võimsus/energiatarbe vähendamine (5)

- Mälustruktuuri optimeerimine
  - Mälu poole pöördumised on eriti energianäljased. Üks mälusiire võtab 33x rohkem energiat kui liitmisoperatsioon!

    ↓

    Mälu poole pöördumiste arvu vähendamine on väga edukas meetod võimsustarbe vähendamiseks
  - Cache'i kohandamine (arv, suurus, assotsiatiivsus, rea pikkus) vastavale rakendusele → aitab kokku hoida mälu poole pöördumiste arvu
  - Huvitav küsimus: suuremad cache'id tarbivad rohkem energiat, kuid aitavad vähendada mälu poole pöördumiste arvu. Milline on õige tasakaal?

Võimsus/energiatarbe vähendamine (6)

- Võimsustarbe haldamine (power management):
  - Käsud, mis võimaldavad süsteemi mõningate osade ootele panemist või seiskamist
  - Käsud, mis võimaldavad dünaamiliselt muuta toitepinget

Võimsus/energiatarbe vähendamine (7)

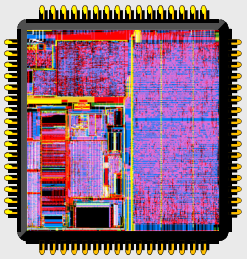
- Süsteemi tasemel
  - Staatilised tehnikad, mida rakendatakse disaini käigus
    - Kompileerimine madala energiatarbe jaoks: käskude valimine, andmete mälusse jaotamine, registrite jaotamine
    - Algoritmi disain: leida algoritm, mis on kõige energiaefektiivsem
    - Ülesannete sidumine ja planeerimine
  - Dünaamilised tehnikad, mida rakendatakse töö käigus
    - Neid tehnikaid rakendatakse töö käigus, et ära kasutada nii ooterežiime, kui ka madala koormuse perioode

ASIC - Application Specific Circuits

- Spetsiaalskeemid on vajalikud, kui eesmärgiks on:
  - Suurim kiirus
  - Energia efektiivsus

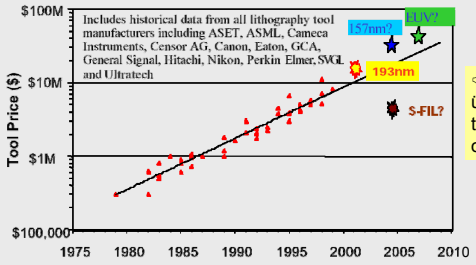
  ja

  - neid saab müüa miljoneid
- Probleemiks
  - Väljatöötamiseks kuluv aeg
  - Paindlikkuse puudus
  - Kõrge hind (maskide hinnad on miljonites dollarites)



Riistvara väljakutsed

- Paindlikkuse puudumine (muutuvad standardid)
- Maskide ülikõrge maksuvus



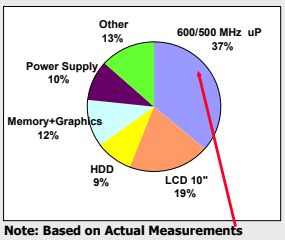
☞ Suund on üha suuremale tarkvara osatähtsusele

[http://www.molecularimprints.com/Technology/tech_articles/MII_COO_NIST_2001.PDF9]

Protsessor v. süsteem

[Courtesy: N. Dutt; Source: V. Tiwari]

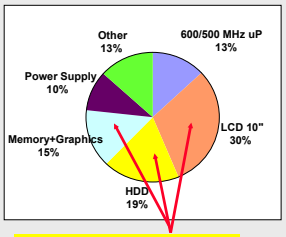
Mobile PC (notebook) Thermal Design (TDP) System Power



Note: Based on Actual Measurements

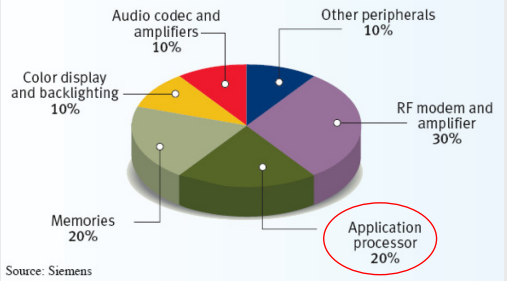
CPU domineerib termovõimsuse osas

Mobile PC (notebook) Average System Power



Mitmed platvormi elemendid on olulised keskmise võimustarbe puhul

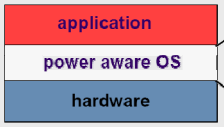
Energiatarve kaasaskantavates seadmetes



[O. Vargas (Infineon Technologies): Minimum power consumption in mobile-phone memory subsystems; Pennwell Portable Design - September 2005;] Thanks to Thorsten Koch (Nokia/ Univ. Dortmund) for providing this source.

Dünaamiline võimuse haldamine (DPM)

DPM: Dynamic Power Management



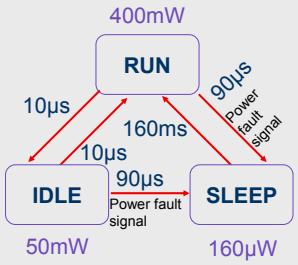
- Otsused:
  - Erinevate olekute vahel ümberlülitamine
    - Idle
    - Sleep
    - Run
  - Erinevate töösageduste ja toitepingete vahel ümberlülitamine

Eesmärgid:
- Energia optimeerimine
- Teenuse kvaliteedi tagamine

Dünaamiline võimuse haldamine (DPM)

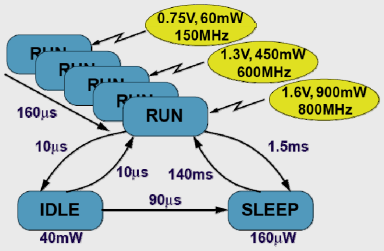
Näide: STRONGARM SA1100

- RUN: tavaline töötamine
- IDLE: tarkvara peatab CPU töö, kuid jälgib katkestusi
- SLEEP: kiibi tegevus peatatakse, äratus läbi "wake-up" sündmuse



Dünaamiline võimuse haldamine (DPM)

- Riistvara toega: Intel Xscale



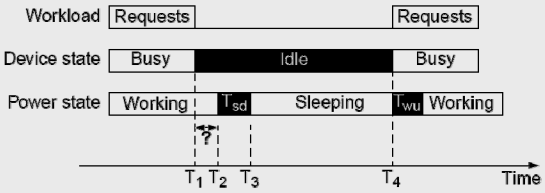
Võimalikud vahepealsed olekud: DEEP IDLE, STANDBY, DEEP SLEEP

Dünaamiline võimuse haldamine (DPM)

- DPMi kasutatakse palju laptopides, PDA'des ja teistes kaasaskantavates seadmetes, et sulgeda või panna ootele mittevajalikke komponente. Eesmärgiks on energia kokkuhoid
- DPMi jaoks on OSide tugi (näiteks Windows 2000 ja uuemad)

DPMi põhimõte

- Kui seadme poole pöördutakse, siis seade on hõivatud, vastasel juhul ootel (idle)
- Kui seade on ootel, siis võib selle kas sulgeda või üle viia madala energiaga ooteasendisse (sleeping)



Dünaamiline pinge muutmine (DVS)

DVS: Dynamic Voltage Scaling

CMOSi energiatarve (lekete ignoreerimisel):

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW}$$

CMOSi viide:

$$\tau = kC \frac{V_{dd}}{(V_{dd} - V_t)^2} \text{ with}$$

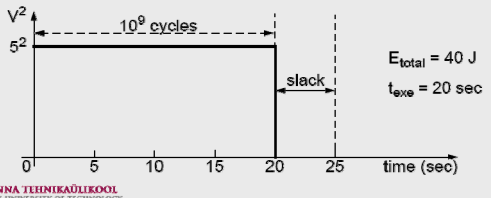
V_t :threshhold voltage

(V_t < than V_{dd})

☞ V_{dd} vähendamisel väheneb P kahekordselt, samas algoritmide täitmiseks kuluv aeg kasvab vaid lineaarselt
$E=P \times t$ väheneb lineaarselt (ignoreerides mälusüsteemi ja V_t)

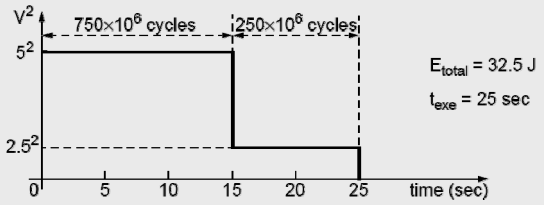
DVS põhimõte

- Olgu meil ülesanne T:
  - Kogu arvutusaeg on 10^9 tsüklit
  - Deadline: 25 sek
  - Protsessori nominaalne toitepinge: 5V
  - Energia: 40 nJ/tsükkel nominaalsel pingel
  - Protsessori kiirus: 50 MHz (50×10^6 tsüklit sekundis) nominaalsel pingel



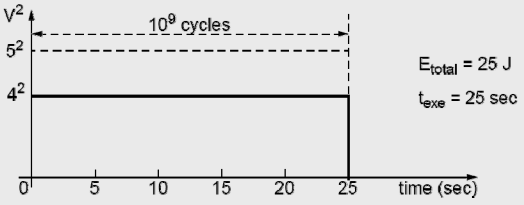
DVS põhimõte (2)

- ✓ Teeme aeglasemaks!
  - VDD = 2,5 V
    - Energia: $40x2,5^2/5^2$ = 10 nJ/tsükkel
    - Kiirus: 50x2,5/5 = 25 MHz



DVS põhimõte (3)

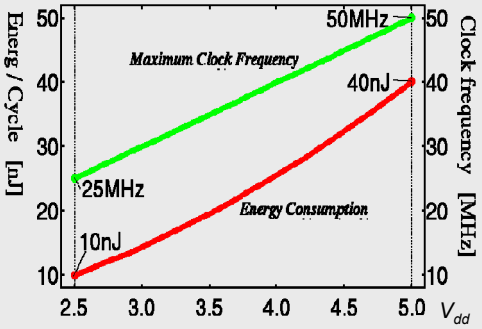
- ✓ VDD = 4 V
  - Energia: $40x4^2/5^2$ = 25 nJ/tsükkel
  - Kiirus: 50x4/5 = 40 MHz



Dünaamiline pinge muutmine (DVS)

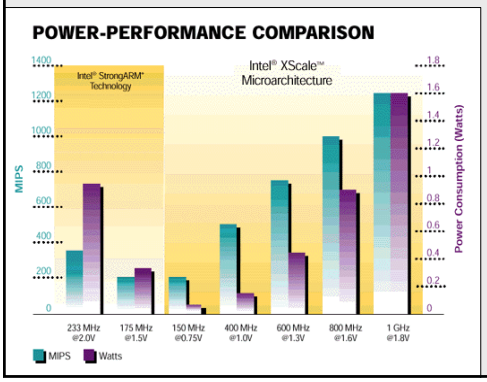
- ✓ Transmeta Crusoe protsessor:
  - 32 erinevat pingetaset, vahemikus 1,1 – 1,6 V
  - Taktsignaal vahemikus 200 MHz – 700 MHz (33 MHz sammuga)
  - Siire ühelt pinge/sageduse paarilt teisele võtab ca 20 ms
- ✓ Inteli SpeedStep tehnoloogia (Mobile Pentium III):
  - 2 pinge/sageduse paari

DVS näide



[Courtesy, Yasuura, 2000]

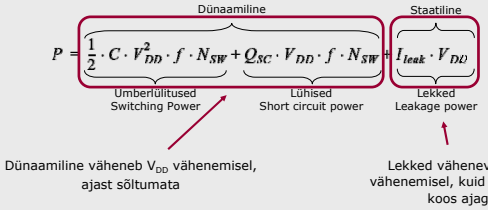
DVS: Intel Xscale



OS peab tegelema energia-eelarve ajalise jaotusega

www.intel.com

Lekked!



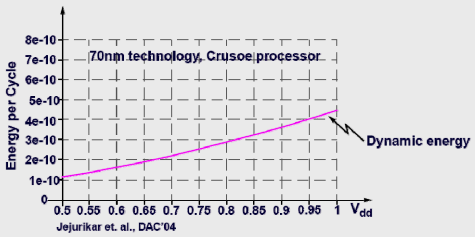
- ✓ Me oleme siiani rääkinud mitte globaalsest energia vähendamisest vaid ainult selle ühe osa vähendamisest
- ✓ Kuid selle tulemusena võib energiatarve koguni hoopis suureneda!

Lekked! (2)

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW} + Q_{SC} \cdot V_{DD} \cdot f \cdot N_{SW} + I_{leak} \cdot V_{DD}$$

Dünaamiline / Staatiline

Ümberlülitused Switching Power | Lühised Short circuit power | Lekked Leakage power

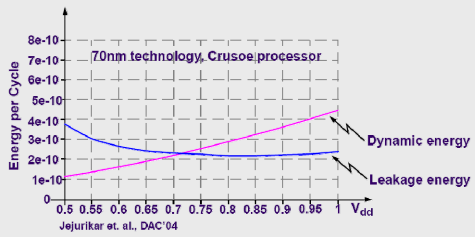


Lekked! (2)

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW} + Q_{SC} \cdot V_{DD} \cdot f \cdot N_{SW} + I_{leak} \cdot V_{DD}$$

Dünaamiline / Staatiline

Ümberlülitused Switching Power | Lühised Short circuit power | Lekked Leakage power

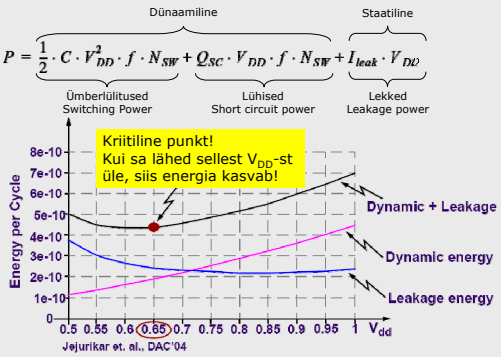


Lekked! (2)

$$P = \frac{1}{2} \cdot C \cdot V_{DD}^2 \cdot f \cdot N_{SW} + Q_{SC} \cdot V_{DD} \cdot f \cdot N_{SW} + I_{leak} \cdot V_{DD}$$

Dünaamiline / Staatiline

Ümberlülitused Switching Power | Lühised Short circuit power | Lekked Leakage power



1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY

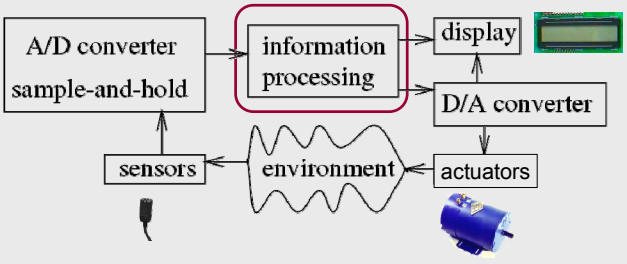
Arvutitehnika instituut
ati.ttu.ee

Arhitektuurid ja platvormid

Tallinna Tehnikaülikool
Arvutitehnika instituut

Sardsüsteemide riistvara

- Sardsüsteemide riistvara kasutatakse tihti tsüklis („*hardware in a loop*"):



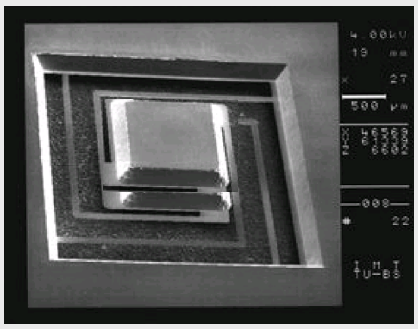
Palju näiteid sellistest tsüklitest

- Küttesüsteemid
- Valgustus
- ECU
- Toiteallikad
- ...
- Robotid

Sensorid

- ✓ Andmete töötlemine algab andmete hõivamisest
- ✓ Sensoreid on võimalik luua põhimõtteliselt suvaliste füüsiliste või keemiliste ühikute jaoks
  - mass, kiirus, kiirendus, elektrivool, pinge, temperatuur, jne.
  - keemilised ühendid.
- ✓ Paljud sensorid põhinevad erinevatel füüsika fundamentaalprintsiipidel.
  - Näiteks induktsioon
- ✓ Sensorite arv on viimastel aastatel plahvatuslikult kasvanud

Näide: Kiirendussensor



Courtesy & ©: S. Bütgenbach, TU Braunschweig

Veel sensoreid

- Vihmasensorid („Sensors multiply like rabbits" [ITT automotive])
- Rõhusensorid
- Läheduse sensorid
- Mootori kontrolli sensorid
- Hall'i effekti sensorid

Arhitektuuri valik

General Purpose **vs.** Application Specific
- Use a general purpose, existing platform and map the application on it.
- or something in-between
- Build a customised architecture strictly optimised for the particular application.

Software **vs.** Hardware
- Use programmable processors running software.
- or both
- Use dedicated electronics: fixed / reconfigurable

Mono **vs.** Multipr. Single **vs.** Multichip
- Monoprocessor
- Multiprocessor: single chip / multi chip

Valikud

Arhitektuuri valik (2)

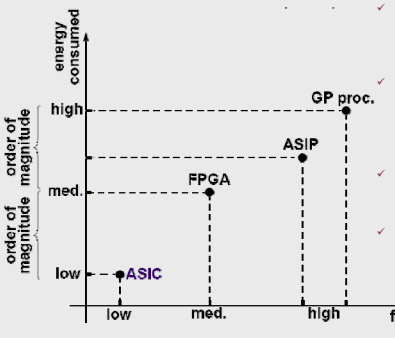
- ✓ Põhilised kompromissid:
  - Performance (high speed, low power consumption)

Application specific	high	Hardware	high
General purpose	low	Reconfigurable hardware	
		Software	low

  - Flexibility (how easy it is to upgrade or modify)

General purpose	high	Software	high
Application specific	low	Reconfigurable hardware	
		Hardware	low

Arhitektuuri valik (3)



- ✓ **GP** (General Purpose processor) – Tavaline laiatarbe protsessor, i.e. x86 perekond, Pentium jms.
- ✓ **ASIP** (Application Specific Instruction set Processors) – rakendus-spetsiifilise käsustikuga protsessor. Näiteks: i960
- ✓ **FPGA** (Field Programmable Gate Array) – programmeeritav loogika
- ✓ **ASIC** (Application Specific Integrated Circuit) – rakendusspetsiifiline integraalskeem

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Arvutitehnika instituut
ati.ttu.ee

Protsessorid

Tallinna Tehnikaülikool
Arvutitehnika instituut

Protsessorid

- Laiatarbe protsessorid ja ASIPid võivad olla nii RISCid, CISCid, DSPd, mikrokontrollerid jms.
  - DSPd ja mikrokontrellerid võivad olla spetsiaalselt loodud DSPks ja kontrolliks
  - Kuid rakendus-spetsiifiline DSP või mikrokontroller on palju spetsiifilisemad
- Laiatarbe protsessorid:
  - Ei käsustik, mikroarhitektuur ega mälusüsteem ei ole kohandatud ühegi rakenduse või valdkonna jaoks
- ASIPid
  - Käsustik, mikroarhitektuur ja/või mälusüsteem on kohandatud spetsiaalse rakenduse või valdkonna jaoks
  - Selle tulemusel on saavutatav suurem jõudlus ning väiksem võimsustarve

Mille poolest on ASIP "spetsiifiline"

- Mille poolest annab protsessorit teha "spetsiifiliseks"
  - Käsustiku (Instruction Set) spetsialiseerimine
    - Eemaldada käsud, mida ei ole vaja
      - vähendab käsusõna pikkust (vähem bitte kodeerimiseks)
      - hoiab kontrolleri ja andmeosa lihtsana
    - Kasutusele võtta antud rakendusele vajalikud spetsiifilised käsud. Isegi eksootilised: aritmeetiliste operatsioonide kombinatsioonid (multply-accumulate), väikesed algoritmid (kodeerimine/dekodeerimine, filtrid), vektoroperatsioonid, stringide töötlemine, pikslite töötlus jne.
      - Vähendab koodi suurust → vähendab mälu hulka, mälu lugemise laiust, võimsustarvet, täitmise aega

Mille poolest on ASIP "spetsiifiline" (2)

- Funktsionaalsete blokkide ja andmeosade spetsialiseerimine:
  - Kui spetsiifiline käsustik on defineeritud, siis selle implementeerimimiseks on võimalik kasutada spetsiaalset andmeosa ja rohkem või vähem spetsiifilisi funktsionaalseid blokke
    - Sõna pikkuse kohandamine
    - Registrite arvu kohandamine
    - Funktsionaalsete blokkide kohandamine:
      - Võib kasutusele võtta väga spetsiifilisi funktsionaalseid blokke stringide töötlemiseks, pikslite töötluseks, aritmeetikaks ja isegi keerulisi blokke mingite käsujadade täitmiseks (kaasprotsessorid)

Mille poolest on ASIP "spetsiifiline" (3)

- Spetsiifiline mälu
  - Mälublokkide arv ja suurus
  - Mälu ligipääs
    - Mõlemad mõjutavad mälu poole pöördumise paralleelsust
    - Mitu väikest blokki (ühe suure asemel) suurendavad paralleelsust ja kiirust ning vähendavad võimsustarvet
    - Keerulised mälustruktuurid võivad suurendada maksumust ja nõudmisi andmesiinile
  - Vahemälu (cache) konfiguratsioon
    - eraldi andmed/instruktsioonid
    - assotsiatiivsus
    - suurus
    - ridade suurus

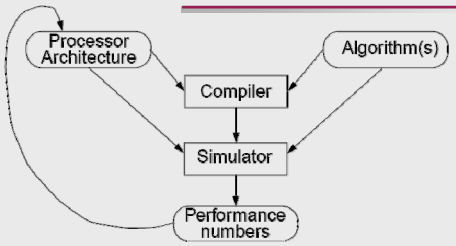
    } Sõltub väga palju antud rakenduse iseloomust ning enneköike lokaalsusest.

    Väga suur mõju jõudlusele ja võimsutarvele

Mille poolest on ASIP "spetsiifiline" (4)

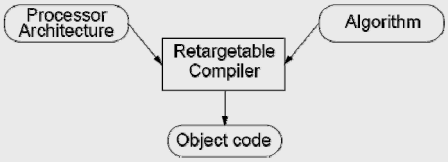
- Ühenduste spetsialiseerimine
  - Funktsionaalsete moodulite ja registrite ühendused
  - Mälu ja cache'i ühendused
    - Kui mitu sisemist siini?
    - Milline protokoll?
    - Täiendavad ühendused annavad täiendavaid võimalusi parallelismiks
- Kontrolli spetsialiseerimine
  - Tsentraliseeritud või hajutatud kontroll (globaalselt asünkroonne)?
  - Konveierid?
  - "Out of order" täitmine?
  - Aparatuurne või mikroprogrammeritud?

ASIPite disainivoog



- Et saada spetsiaalset arhitektuuri on vaja:
  - Ümber häälestatavat kompilaatorit (retargetable)
  - Konfigureeritavat simulaatorit

Retargetable compiler



Retargetable compiler (2)

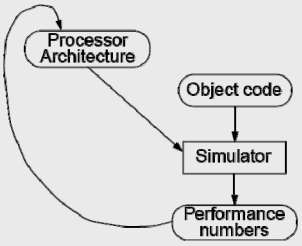
- Automaatselt ümber häälestatavat kompilaatorit on võimalik kasutada erinevate arhitektuuride jaoks

  Koodi optimeerimine ja koodi genereerimine teostatakse kompilaatori poolt ja põhineb arhitektuuri kirjeldusel. Arhitektuuri kirjeldus on antud n.ö. arhitektuuri kirjelduse keeles

- Hea kompilaator ei ole vajalik mitte ainult protsessori spetsialiseerimise käigus

  Sobiva ASIPi puhul on vaja head kompilaatorit ka selle efektiivseks kasutamiseks

Konfigureeritav simulaator

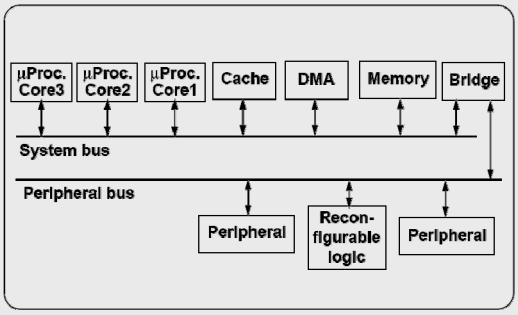


- Sellist simulaatorit on võimalik häälestada sobiva arhitektuuri jaoks (põhinedes arhitektuuri kirjeldusele)
- Kõige olulisem väljund on jõudust kajastavad numbrid:
  - Läbilaskevõime
  - Viide
  - Energia/võimsustarve

Spetsialiseeritud platvormid

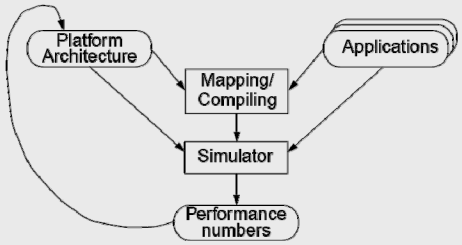
- Mitte ainult protsessoreid vaid ka riistvara platvorme on võimalik spetsialiseerida teatud rakenduste klassi jaoks
- Platvorm defineerib kommunikatsiooni infrastruktuuri (siinid ja protokollid), protsessorite tuumade tüübid, perifeeria, kiirendid ja põhilise mälustruktuuri

Spetsialiseeritud platvormid (2)



Spetsialiseeritud platvormid (3)

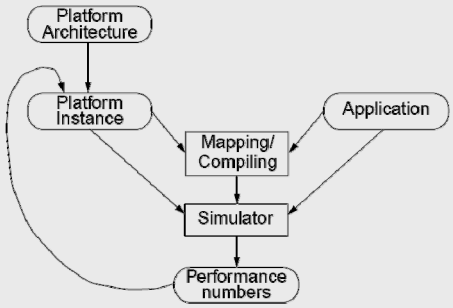
- Lahenduste ruumi uurimine platvormi defineerimisel



Platvormi kohandamine

- Vastava rakenduse jaoks ei looda uut kiipi (mis koosneks sõltumatutest blokkidest) vaid selle jaoks kohandatakse valitud platvormi (instantiation).
- Mida tähendab platvormi kohandamine:
  - Mälu ja cache'i suuruste valik
  - Tuumade ja perifeeria valik
  - Täiendavate ASICute ja kiirendite lisamine
  - Väliprogrammeeritava loogika lisamine

Platvormi kohandamine



Süsteemi platvormid

- Eelnevalt sai räägitud riistvara platvormidest
- Kuid riistvara antakse tavaliselt üle koos tarkvara kihiga:
  riistvara platvorm + tarkvara kiht = süsteemi platvorm
  - Tarkvara kiht:
    - Real-time OS
    - Draiverid
    - Võrguprotokolli stack
    - Kompilaatorid
  - Tarkvara kiht on vahekiht riistvara ja rakendustarkvara vahel (riistvara abstraktsioon)

IP-põhine disain

- Peamine põhimõte tootlikuse tõstmiseks: taaskasutamine (reuse)

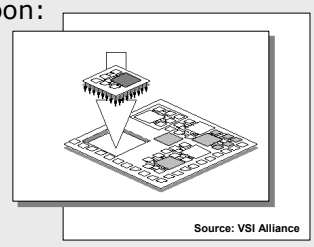
  Et luua uut süsteemi ei ole mõtet alustada nullist vaid tuleks kasutada nii palju kui võimalik (kas siis eelnevatest disainidest pärit või turul saada olevaid) IP blokke (tuumasid)

  IP: Intellectual property; Core: tuum

- Seda kutsutakse: IP-based design, core-based design, reuse techniques jne.
  Core-based design: süsteemi ehitamine olemasolevate komponentide kokku panemise teel

Kiipsüsteemid - Systems-on-Chip

- Milliseid blokke kasutatakse
  - Liidesed, kodeerijad/dekoodeerijad, filtrid, mälud, mikrokontrollerid, DSPd, RISCid, GPd
- Üks võimalik definitsioon:
  - Tuum on blokk, mis on suurem, kui tüüpiline RTL komponent
- Ka tarkvara taaskasutamine


Source: VSI Alliance

Tuumad

- ✓ Eelnevalt loodud ja verifitseeritud blokid
  - Pehmed tuumad (Soft cores)
    - Sünteesitav HDL (RTL või kõrgem)
  - Firm cores
    - Teegi komponentide netlist (optimeerituna valitud tehnoloogiasse)
  - Kõvad tuumad (Hard cores)
    - Layoudi kujul, optimeerituna. Ainult funktsionaalne spec on saadaval.

Tuumad (2)

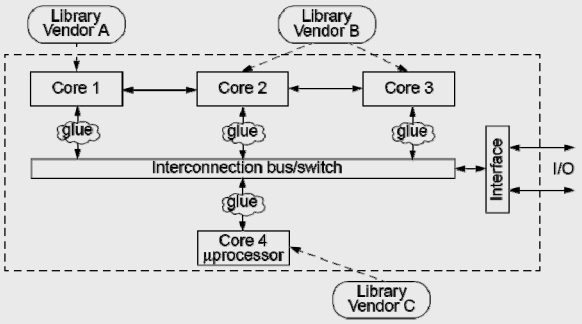
- Hard cores: are fully designed, placed, and routed by the supplier.
  - ⇩ A completely validated layout with definite timing
    - ⇩ rapid integration
    - ⇩ low flexibility
- Firm cores: technology-mapped gate-level netlists.
  - ⇩ less predictability
  - ⇩ flexibility during place and route

Tuumad (3)

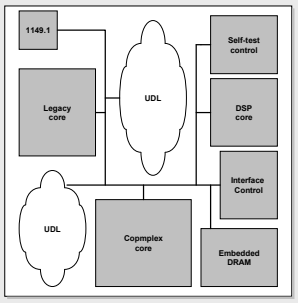
- Soft cores: synthesizable RTL or behavioral descriptions.
  - ⇩ much work with integration and verification.
  - ⇩ maximal flexibility

Flexibility can provide opportunities like e.g. adding application specific instructions to a processor core by modifying the behavioral description.

IP-põhine disain

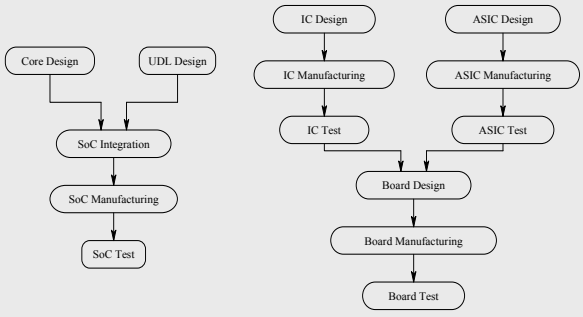


SoC: Arhitektuud



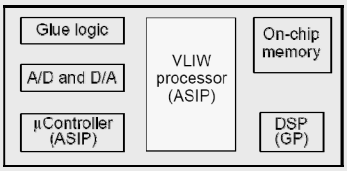
- ✓ 10% UDL
- ✓ 75% mälu
- ✓ 50% "oma" tuumasid
- ✓ 60-70% pehmeid tuumasid

SoC v. SoB



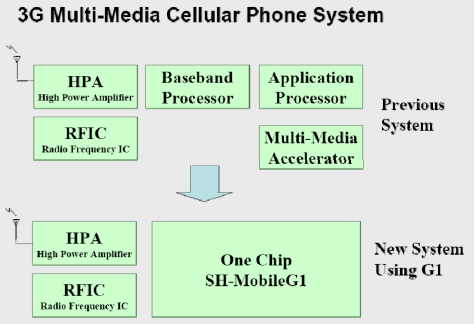
SoC Process | System-on-Board Process

Kiipsüsteem (SoC) multimeedia jaoks



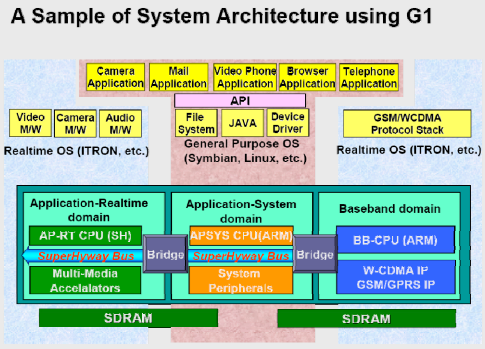
- Tüüpiline rakendus-spetsiifiline platvorm. Loodud ühte tüüpi rakenduste valdkonnale
- Peale GP protsessorite tuumade sisaldab ka ASIPi tuumasid, mis on spetsialiseeritud antud rakenduste valdkonna jaoks
- Rakendus-spetsiifiline mikrokontroller teostab süsteemi üldist kontrolli ning mälu ligipääsu kontrolli
- Standartne (GP) DSP teostab arvutuslikult vähem nõudlikke modemi ja heli kodek operatsioone
- VLIW ASIP teostab arvutuslikult nõudlikke operatsioone: diskreetne ja tagurpidi diskreetne koosinus teisendusi, liikumise arvutamist jms.

Trend: multiprocessor systems-on-a-chip (MPSoCs)



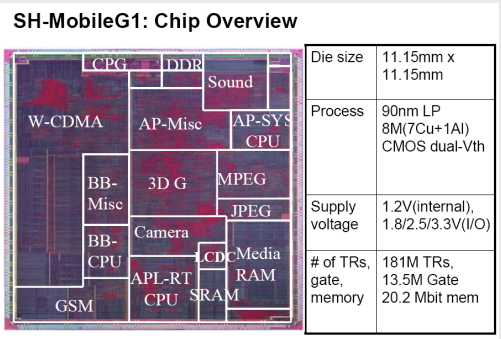
http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

MPSoCs



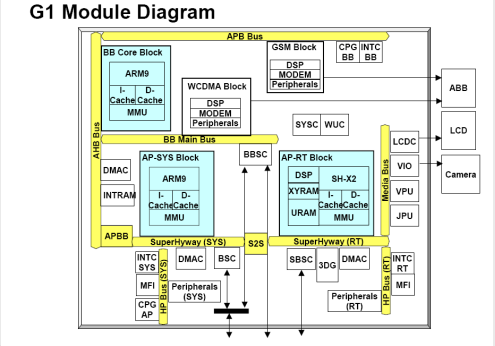
http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

MPSoCs



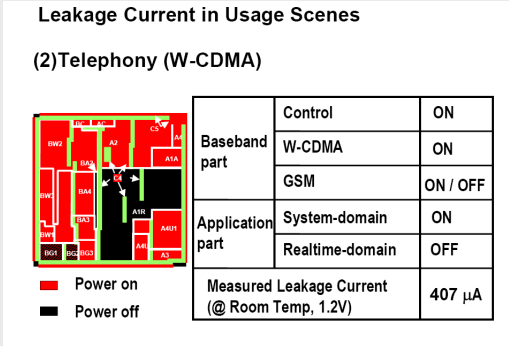
http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

MPSoCs



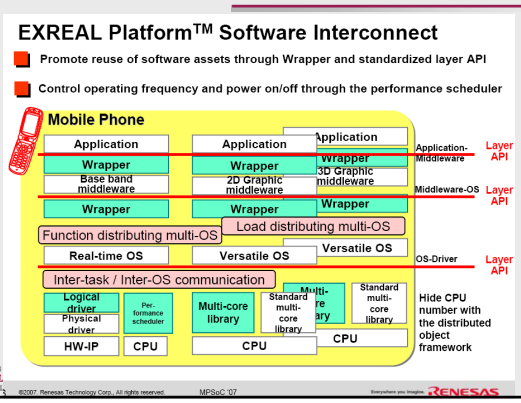
http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

MPSoCs



http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

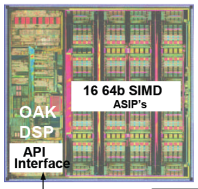
MPSoCs



http://www.mpsoc-forum.org/2007/slides/Hattori.pdf

MPSoCs

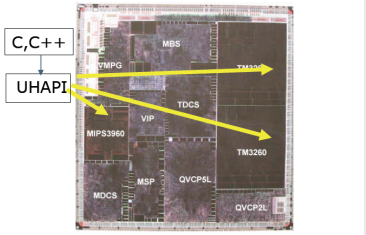
VIP for car mirrors Infineon



Hd Compiler ← VPL C

200MHz , 0.76 Watt
100Gops @ 8b
25Gops @ 32b

Nexperia Digital Video Platform NXP



1 MIPS, 2 Trimedia
60 coproc, 250 RAM's
266MHz, 1.5 watt 100 Gops

~50% inherent power efficiency of silicon

© Hugo De Man, IMEC, 2007

Kokkuvõte

- ✓ Sardüsteemid ja usaldusväärsus
- ✓ Arhitektuurid
- ✓ Võimsus- ja energiatarve
- ✓ Protsessorid
- ✓ Platvormid

- ✓ **NB! 11/12 loeng algab kell 15:30**

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY

Arvutitehnika instituut ati.ttu.ee

Küsimusi?

Gert Jervan
www.pld.ttu.ee/~gerje

Tallinna Tehnikaülikool
Arvutitehnika instituut