Smart Environments:

Technologietrends und mögliche Konsequenzen für die informationelle Selbstbestimmung

Dirk Timmermann

Institut für
Angewandte Mikroelektronik und Datentechnik
FB Elektrotechnik u. Informationstechnik
Universität Rostock

Agenda

- Trends der Basistechnologien
- Was sind die wirklichen Limits ?
- Smart Labels und *ihre* Randbedingungen
- Energie und Informationelle Selbstbestimmung

Zur Natur von Vorhersagen

- **Vorhersage möglich, ohne sich in 10 Jahren zu einem Narren gemacht zu haben ?** **Horowitz: The future will happen and you will be wrong**
  - Prinzipiell unmöglich .....
  - Zumindest diese Folien nicht auf einen Webserver legen ☺
  - Klon nötig aus
    - Mathematiker (Chaostheorie)
    - Physiker
    - Ingenieur, Informatiker
    - Betriebswirt, Marketingspezialist
    - Unternehmer
    - Trendforscher, Philosoph
    - Durchschnittskonsument
- **Zwei Ansätze**
  - Pessimistisch: Erwarte Begrenzungen, beschäftige dich mit ihnen
  - Optimistisch: Schreibe derzeitige Trends konservativ fort

Trends der Basistechnologien

- postuliert 1968 von Gordon Moore

IC Technologie

DRAM
SRAM

Die Kapazität von Halbleiterspeichern nimmt alle 1,5 Jahre um den Faktor 2 zu

Verallgem. Moore‘sches Gesetz

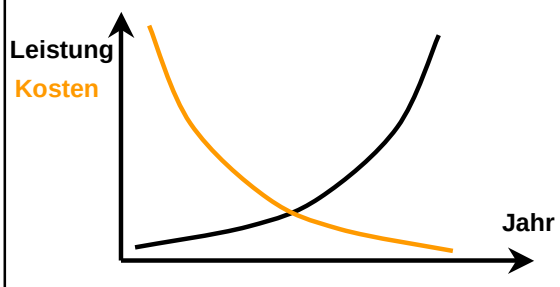
Prozess-Technologie

IC-Technologie
Magnetspeicher
Optische Speicher
Bandbreite
Software
etc.

Alle charakteristischen Parameter der Informationstechnologie verbessern sich alle 1 bis 3 Jahre um den Faktor 2

Escherichia Coli verdoppelt sich alle 20 Minuten

Preis-/Leistungsverhältnis



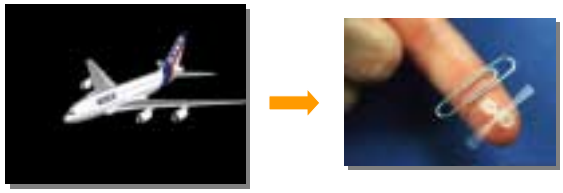
Schrumpfungsprozess

- Festplatten

- Embedded Internet

Perspektive ?

- Luftfahrzeuge



Was nützt es uns ?

- Verallgemeinertes Moore'sches Gesetz
  - Exponentielle Verbesserung der Technologie
- Das Gesetz des technologischen Nutzens:

Der Nutzen aus diesen Technologien wächst nur logarithmisch mit ihnen:

Nutzen = log (Technologie)

➔ **Nutzen entwickelt sich zeitlich nur linear**

Inverses Gesetz

Technologie = exp (Nutzen)

Um Probleme des täglichen Lebens zu lösen, braucht man (u.a. !) eine Unmenge neuer Technologien

- Verkehrsstaus
- Ökologie und Umwelttechnik
- Medizintechnik

Konsequente Extrapolation

- Theoretisch schnellster Computer [Seth Lloyd, MIT]
- Ausgangspunkt: aktueller Laptop 10^{10} Ops/s @ 10^{10} Bits Speicher @ 1 dm^3 @ 1 kg Gewicht
  - **Geschwindigkeit:**
  - Jedes Teilchen in Energie verwandelbar: Spez. Relativ.theorie + $E=mc^2$ → 25 MWh
  - Quantenmechanik -> **max. 10^{51} Ops/s**
  - **Speicher:**
  - Jedes Teilchen als Speicher, benutze alle Zustände des Spin, Geschwindigkeit, Richtung → Speicher im Zustand max. Entropie
  - Speicherkapazität von **max. 10^{31} Bits**
- Und was sagt Moore dazu ?
  - **in nur 250 Jahren erreicht ....**

Etwas konkreter, bitte

- SIA Roadmap 1998

Jahr	1999	2002	2005	2008	2011	2014
Strukturgröße (nm)	180	130	100	70	50	35
Logiktrans./cm^2	6.2M	18M	39M	84M	180M	390M
Kosten/Trans (mCent)	1.735	.580	.255	.110	.049	.022
Takt [MHz]	1250	2100	3500	6000	10000	16900
Chipgröße [mm^2]	340	430	520	620	750	900

Langfristig

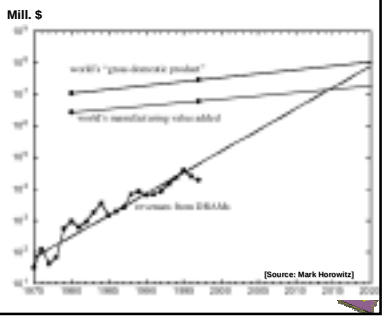
- **Kein exponentieller Anstieg hält ewig**
- **Technologien nach dem Siliziumzeitalter:**
  - Neue Schalter
    - Ein-Elektron-Transistor
    - Organische / optische Computer
  - Nano-Technologie
    - Molekulare Schalter
    - Kohlenstofffaser-Leitungen
  - Quantencomputer

- **Beobachtungen:**
  - Das einzige, was sich ändert, sind die Namen der Nachfolgetechnologien....
  - Die meisten wollen etwas verbessern, was nicht das Problem ist: **Schaltgeschwindigkeit**
  - Das Problem sind die **Verbindungsleitungen**, sprich Kommunikation

Die echten Limits

- **Silizium wird weiterentwickelt, skaliert, solange die nächste Generation billigere Schaltungen erlaubt als die aktuelle**
- **Es gibt keine Grenzen, außer ...**

  ökonomische
- **Entweder steigt BSP - oder - Technologie-entwicklungs-kurve verflacht**



Agenda

- **Trends der Basistechnologien**
- **Was sind die wirklichen Limits ?**
- **Smart Labels und *ihre* Randbedingungen**
- **Energie und Informationelle Selbstbestimmung**

Technik in Smart Environments

- **Ausgangspunkt:**
  - ***aktive* Smart Labels**
  - **miniaturisiert < 1 mm³**
  - **allgegenwärtig**
  - **kommunizieren per Funk**

  Erfolgversprechend nur ohne Steckdose (LAN und 220V)
- **Probleme**
  - **User-Konfiguration**
  - **Biologische Verträglichkeit**
  - **Zuverlässigkeit**
  - **Informationelle Selbstbestimmung**
  - **Energieverbrauch, und damit**
    - **Interaktions-Reichweite → Communication**
    - **Funktionalität → Computation**

Anforderungen an Smart Labels

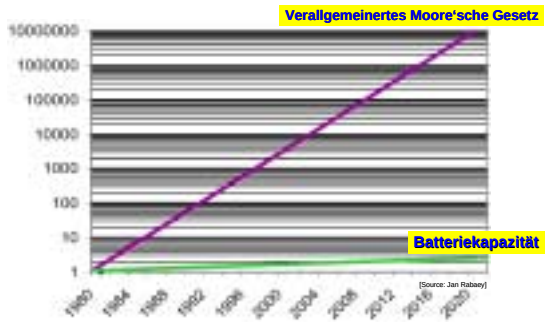
- **Größe**
  - mm³ - cm³
- **Energieverfügbarkeit**
  - ~1J/mm³
- **Mindestlebensdauer**
  - 5-10 Jahre
- **Datenraten**
  - Bits/s .... KBits/s
- **Reichweite**
  - 5-50 Meter
- **Räumliche Dichte**
  - 0.1 Knoten/m² .... 20 Knoten/m²

Beispiele für autarke, aktive Knoten

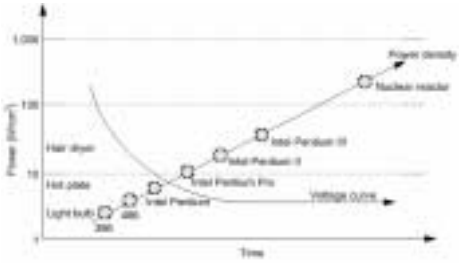
Smart Dust **Picoradio** **WINS**

Das gemeinsame Problem: **Energieversorgung**

Nicht alles gehorcht Moore



Trend Leistungsdichte



[Herring, MICROPROCESSORS, MICROCONTROLLERS, AND SYSTEMS IN THE NEW MILLENNIUM, IEEE Micro, vol. 20, no. 6, Nov/Dez. 2000]

Fakten eines Mobilitätsszenarios

- Rechner
  - Rechnerperformance und –leistungs-verbrauch steigt exponentiell nach Moore
- Kommunikation
  - Sendeleistung steigt mit zunehmender Entfernung und Bitrate exponentiell an

- Batteriekapazität steigt aber in 5 Jahren nur um 30-50%

Außerdem
- Kosten, Größe, Kühlung, ...
- Umwelt (Elektronikanteil derzeit 10% am Gesamtenergieverbrauch USA)

Agenda

- **Trends der Basistechnologien**
- **Was sind die wirklichen Limits ?**
- **Smart Labels und *ihre* Randbedingungen**
- **Energie und Informationelle Selbstbestimmung**

Informationelle Selbstbestimmung

- **Masse der in Smart Environments erfassbaren Informationen erfordert zwingend u.a.**
  - Individuelle Konfiguration der preiszugebenden Daten durch den Nutzer
  - **Anonymisierung und Verschlüsselung von Daten** zur Vermeidung einer **ungewollten Profilerstellung**
- **Ungleiche Ausgangssituation:**
  - **Smart Labels: wenig Rechenleistung, wenig Energie**

  - **Datensammler: praktisch unbegrenzte Rechenleistung und Energie**

Energiekosten der Sicherheit

- **Leistungsverbrauch *P***
- **Schlüssellänge *n*, Sicherheit ~ *n***
- **Symmetrisches, secret key Verfahren:**
  - Beispiel DES: $P_{DES} = O(n)$
- **Asymmetrisches, public key Verfahren:**
  - Beispiel RSA: $P_{RSA} = O(n^3)$
- **Energie = Leistung * Zeit**
  - Schlüssellänge bei RSA >> DES
  - Anderseits: Symmetrische Verfahren häufiger benötigt als asymmetrische Verfahren
- **Energieverbrauch für Sicherheit abhängig vom Szenario**

Energie sammeln unumgänglich

- **Nutzen der Umgebungsenergie für Smart Environments**
  - 

  - Solarzelle, empfindlich gegen Abdeckung
  - Mechanische Vibration 10 µW
  - Piezo-Drucksensoren
  - Radio-Wellen
  - .....

- **Ausreichend für Elektronik + Funk ?**

Ausweg

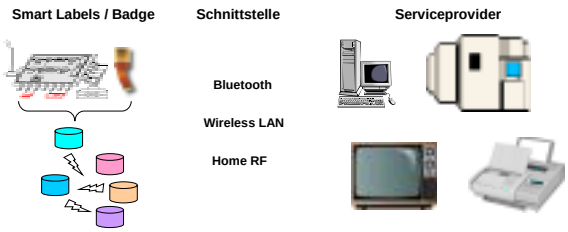
- **„Ingenieurmäßiger Ansatz“ bei allen gezeigten Beispielen:**

  Kompromiss Energieverbrauch ⇔ Qualität

- **In Smart Environments:**

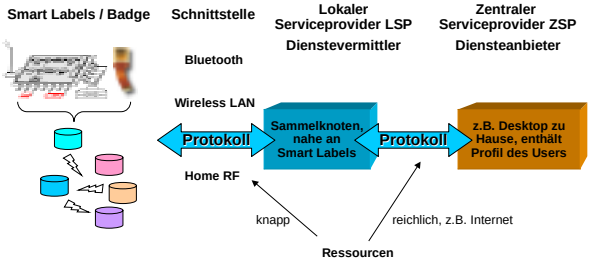
  Kompromisse auf Kosten der Informationellen Selbstbestimmung ?

Zweistufige Architektur für Mobilität



- **Eigenschaften**
  - **Knappe Ressourcen: Größe, Performance, Stromverbrauch, Bandbreite, Reichweite**
  - **Jini zu „schwer“**
  - **Konsequenzen für Konfigurierbarkeit, Anonymität, Sicherheit**

Mehrstufige Architektur für Mobilität



- **Smart Label/Badge sehr einfach**
- **Enthält nur IP- # oder URL und ausreichend (!) Kryptofähigkeit**
- **Systemarchitektur für mobile Sicherheit**
- **mehrstufiges Konzept nutzt jeweils verfügbare Ressourcen**
- **vgl. NINJA, UC Berkeley, Prof. Katz**

Informatisierte Zukunft ?

Ihr Mann ist gestorben, aber hier ist sein Smart Label

Fazit

- **Technologie macht fast alles möglich**
- **Smart Environments technisch machbar**
- **Minimales Energiebudget tangiert Informationelle Selbstbestimmung**
- **Spannende Forschungsfragen:**
  - Architektur ? Wie viele Hierarchiestufen angemessen ?
  - Smart Labels/Protokolle/Interaktionen/Architekturen/Kommunikation mit minimalem Energieverbrauch und maximaler „Privacy“
  - Welcher Grad an „Privacy“ ist soziologisch/politisch/... unabdingbar ?

Quellen

- **enthält Bilder und Anregungen aus Vorträgen und Veröffentlichungen von:**
  - Jim Gray, Microsoft, Turing award lecture
  - Anantha Chandrakasan, MIT
  - Bob Brodersen, Randy Katz, Jan Rabaey, UC Berkeley
  - Mark Horowitz, Stanford
  - Hugo de Man, IMEC
  - Clemens Cap, Universität Rostock
  - Seth Lloyd, MIT, Department of Mechanical Engineering, „Ultimative physical limits to computation“, Nature, 31. August 2000