A Concept of a Trust Management Architecture to Increase the Robustness of Nano Age Devices

Thilo Pionteck

University of Lübeck
Institute of Computer Engineering
Lübeck, Germany

Werner Brockmann

University of Osnabrück
Institute of Computer Science
Osnabrück, Germany

Outline

- **Motivation**
  - Problem Statement
  - Related work
- **The SMART Approach**
  - Lack of Informational Trust
  - System Model
- **Trust Management**
  - Trust Level Determination and Processing
  - Generic Module Architecture
- **Summary & Outlook**

Motivation

Technology scaling leads to an increase in

- **Process variation**
  - **Systematic effects**
    spatial correlation between transistors
    - Primary source: lithographic irregularities
      → effects effective channel length L_{efff}
  - **Random effects**
    individual transistors
    - Primary source: varying dopant concentrations
      → effects threshold voltage V_T

- **Device degradation / aging**
  → Wear-out effects:
  - Gate oxide breakdown
  - Negative bias temperature instability
  - Electromigration
  - Hot carrier injection

Motivation

Characteristics:

- **Process variation**
  - fixed parameter fluctuations = **static**
  - can be determined after fabrication and before shipping
- **Device degradation / aging**
  Depends on operation conditions = **dynamic**
  - Temperature
  - Workload

Classical compensation technique: design for ***worst case scenario***

→ will result in an unacceptable low yield and/or performance

→ huge hardware and/or timing overhead
(usage of classical redundancy schemes for compensation of SEUs and SETs and worst case timing, resp.)

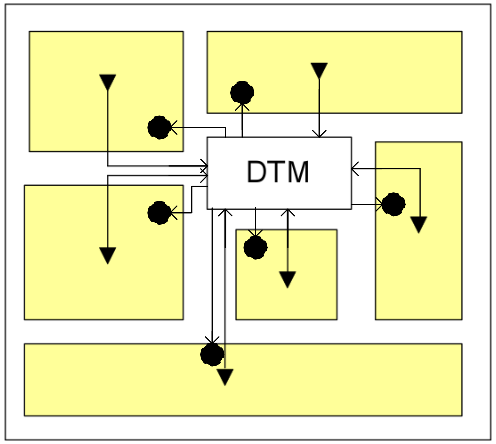
Solution: ***adjust system parameters dynamically*** to

- external requirements
- device dependent parameters

} already done for **dynamic thermal management (DTM)**

Dynamic Thermal Management

- **Temporal**
  - Dynamic Frequency Scaling (DFS)
  - Dynamic Voltage Scaling (DVS)
  - Clock gating
- **Spatial**
  - Thread migration
  - Load balancing



Problems:

- Spatial effects are not considered adequately
- Within-die variations
- Fast dynamic effects and long-term aging
- Accuracy of
  - Sensors
  - Actors setting system parameters
- Aging

Uncertainties for system management:

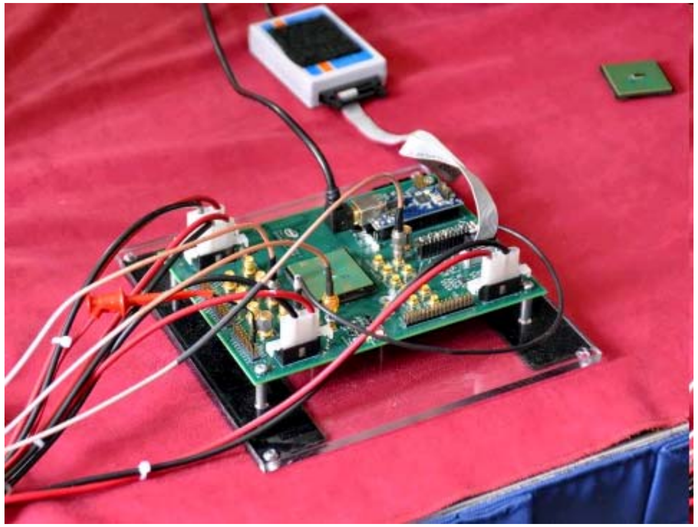
- correctness and trustworthiness of sensor information
- correct and trustworthy operation of actors

Motivation

Handling uncertainties: Intel's Palisades processor

→ Resilient Processor Design / Self-Tuning Processor

- Elimination of margins for voltage droop, temperature, and critical path activation
- **Tunable replica circuits (TRC)** can be used to detect timing errors
  digital delay sensor which can be tuned at test time to match the delay of a critical path in the circuit.
- Error correction:
  - Parameter adjustment
  - Pipeline flush
- Power reduction of 21% or performance improvement of 41%



Source: www.golem.de

Motivation

Weak point of all approaches:

Vagueness and uncertainty of data / Lack of informational trust

1. Dynamic behavior is not completely predictable
2. Trustworthiness of sensor readings
3. Uncertainty of actor operation
4. Significance of a temperature measured at a single spot
5. Environmental effects
6. Accuracy of thermal models
7. Adaptation to time-variant parameters based on fixed rule-sets

➔ **For optimal performance and trustworthy operation, dynamically changing uncertainties must explicitly taken into consideration at runtime.**

Outline

- **Motivation**
  - Problem Statement
  - Related work
- **The SMART Approach**
  - Lack of Informational Trust
  - System Model
- **Trust Management**
  - Trust Level Determination and Processing
  - Generic Module Architecture
- **Summary & Outlook**

The SMART Approach

SMART: System-on-Chip with Modular Adaptation for Robustness and Trust

System requirements:

- Guaranteed system lifetime
- Robust and trustworthy operation
- Autonomous on-chip and online operation
- Timely reaction
- Low hardware overhead, low power dissipation
- Universal applicability, independent of technology
- Scalability
- Easiness to engineer
- Complementariness to classical fault tolerance

SMART: System-on-Chip with Modular Adaptation for Robustness and Trust

General Concept: Modeling and integrating uncertainty information explicitly into device management

Trust Management

- Complementary to normal system operation
- Increases robustness
- Allows for performance optimization without sacrificing lifetime

Trust-Level:

- Uncertainty represented by specific attribute
- Normalized value between 0 and 1
- Represents the trustworthiness of information:

  1 = trusty, safe; 0 = untrusty, unsafe, no information

Trust Management

Trust-Level as additional attribute for

- **Sensors (*R-Sensors*)**

  → Trust level models e.g. ambiguity, lack of information

- **Internal variables (*R-Variables*)**

  → Trust level represents trustiness of calculations

- **Actors (*R-Actors*)**

  → Trust level models the uncertainty of actor operation caused by

  - Process variation
  - Degradation
  - Operating conditions
  - . . .

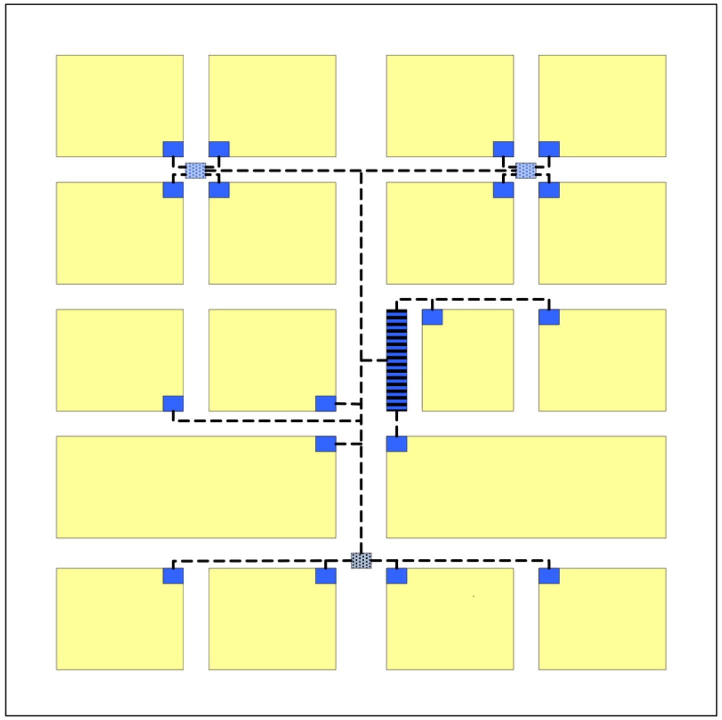
General Architecture

Functional Units (FUs) are complemented by Robustness Units (RUs)

- Additional functionality for device management
- Integrates uncertainty handling:
  - Trust-level determination (in software)
    - Plausibility check
    - Combination of sensor information
  - Reaction on uncertainties

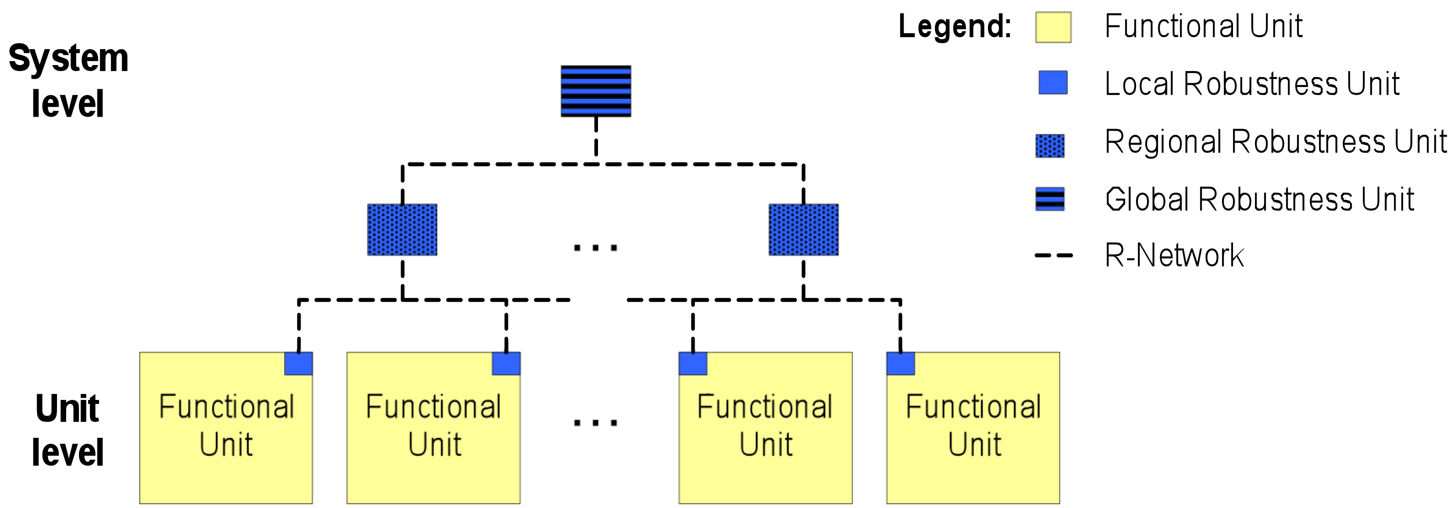
Legend:

- Functional Unit
- Local Robustness Unit
- Regional Robustness Unit
- Global Robustness Unit
- R-Network



The SMART Approach

- RUs form a separate hierarchy for device and trust management
  - Local RUs
  - Regional RUs
  - Global RU
- Communication via a (virtual) Robustness network (*R-network*)

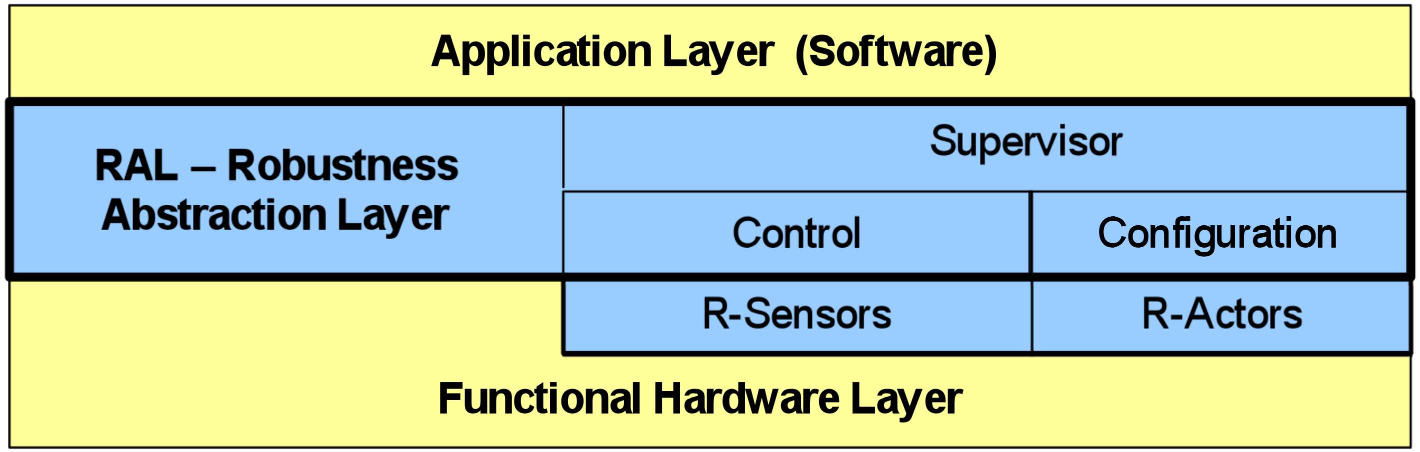


The SMART Approach

Layer Model

Robustness Abstraction Layer (RAL)

Hides uncertainty of lower layer to the application layer



Control: continuous data and control actions

Configuration: Discrete actions at discrete time points, e.g. altering operation modes, task migration, …

Supervisor

Local supervisor
- Coordinates actions of neighboring RUs

Global supervisor
- Reacts on outer requirements
- Interface to operating system
- Monitoring device lifetime

Outline

- **Motivation**
  - Problem Statement
  - Related work
- **The SMART Approach**
  - Lack of Informational Trust
  - System Model
- **Trust Management**
  - Trust Level Determination and Processing
  - Generic Module Architecture
- **Summary & Outlook**

Trust Level Determination (Examples)

Approaches for sensors:

- Noise amplitude
- Noise signal traces for comparison with known shape trends
- Noise + additional sensory information
- Noise amplitude of power and ground lines
- Consideration of dynamic changes (e.g. temperature) for assumption of system parameters between measuring points

Approaches for actors:

- Physical models
- Observation of past behavior to predict how a given value will cause the intended effect

Trust Level Processing

Based on fuzzy logic operators and techniques

- Easy to engineer
- Robust / do not require a precise formal model
- Different qualities of input variables can be combined harmonically
- Allows blending between different optimized controllers for trusty and untrusty system states

Example: internally generated signals (***R-variables***) based on *R-sensors*

- Trust level υ_{o_mult} depending on i uncertain inputs $\upsilon_{in,I}$:

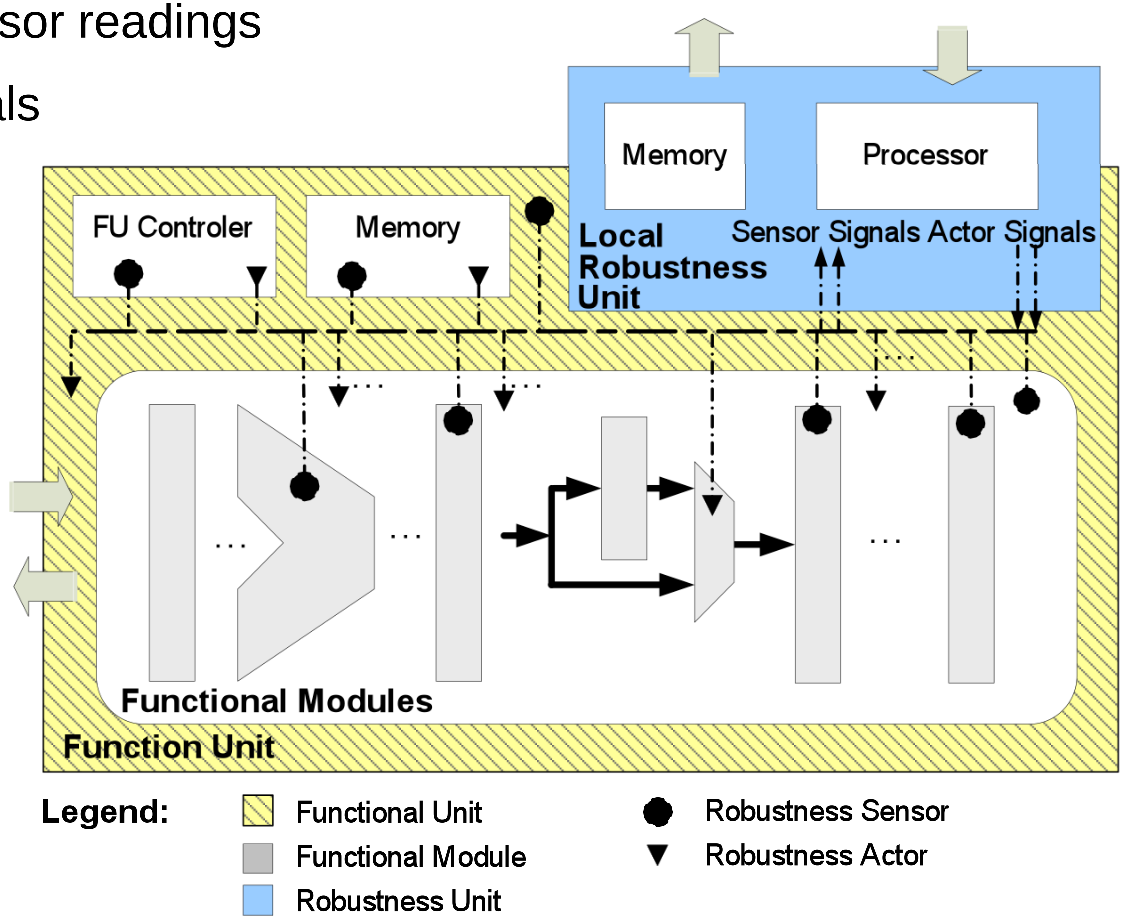
$$\upsilon_{o\_mult} \leq \min_i \upsilon_{in,i} \quad \forall i$$

- Trust level υ_{o_red} when combining j redundant inputs $\upsilon_{in,j}$:

$$\upsilon_{o\_red} \geq \min_j \upsilon_{in,j} \quad \forall j$$

Generic Module Architecture

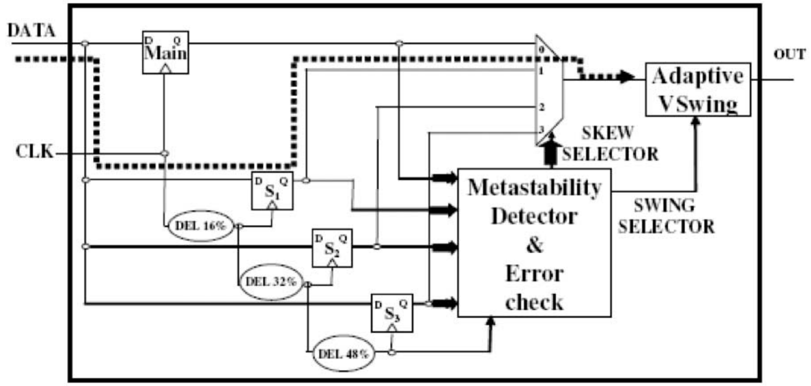
- FU contains sensors and actors
- Short term history of sensor readings
- RU generates trust signals
- RU communicates with
  - higher levels
  - operating system
- RU performs
  - trust management
  - device management



Exemplary scenario

System reaction on timing violations in pipelined FUs

- Detection: extended versions of the Razor flip-flop
- Uncertainties:
  - quantization errors (static factor)
  - significance of the path under test for the whole FU (dynamic factor)
    - Information has to be used to generate trust level



Taken from: M. Simone, M. Lajolo, D. Bertozzi „Variation tolerant NoC design by means of selfcalibrating links“

- System reaction
  Effect of each reaction has to be estimated by the RU (e.g. test mode)
  - Frequency adaption → *continuous*
  - Adding of pipeline stages → *discrete*
  - Time borrowing between pipeline stages → *continuous/discrete*

Outline

- **Motivation**
  - Problem Statement
  - Related work
- **The SMART Approach**
  - Lack of Informational Trust
  - System Model
- **Trust Management**
  - Trust Level Determination and Processing
  - Generic Module Architecture
- **Summary & Outlook**

Summary & Outlook

Summary

SMART approach (System-on-Chip with Modular Adaptation for Robustness and Trust)

- Concept for integrating uncertainty information explicitly into device management.

  Addressing: - within-die variation
  - dynamic operating conditions
  - device degradation

- Trust Management
  - Trust level attribute for representing uncertainty
  - Explicit modeling of uncertainties
  - Explicit consideration of uncertainties for discrete and continuous control actions

Outlook

- Concrete sensor and actor modeling
- Setting up a framework for the SMART architecture
- Use of safe online learning techniques for adaptation
- Formal modeling of trust management
- Long-term device management, e.g. dynamic life-time management, rejuvenation

Thank you for your attention