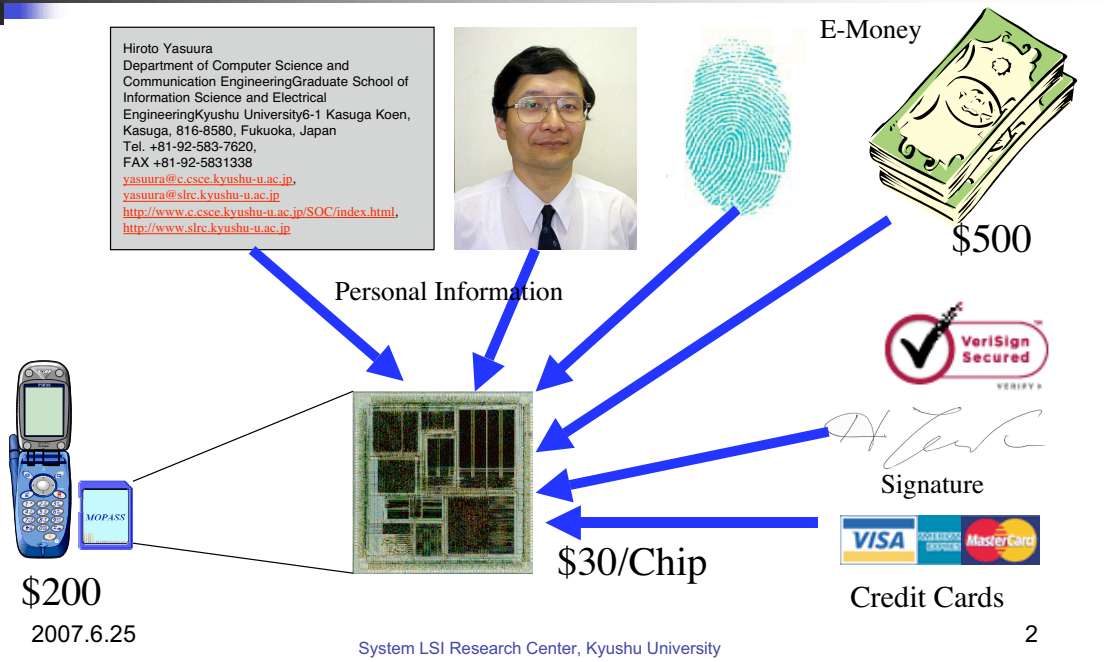
Dependability of MPSoC for Applications in Social Information Infrastructure

Hiroto Yasuura
System LSI Research Center
Kyushu University

Values and Credit on a Chip

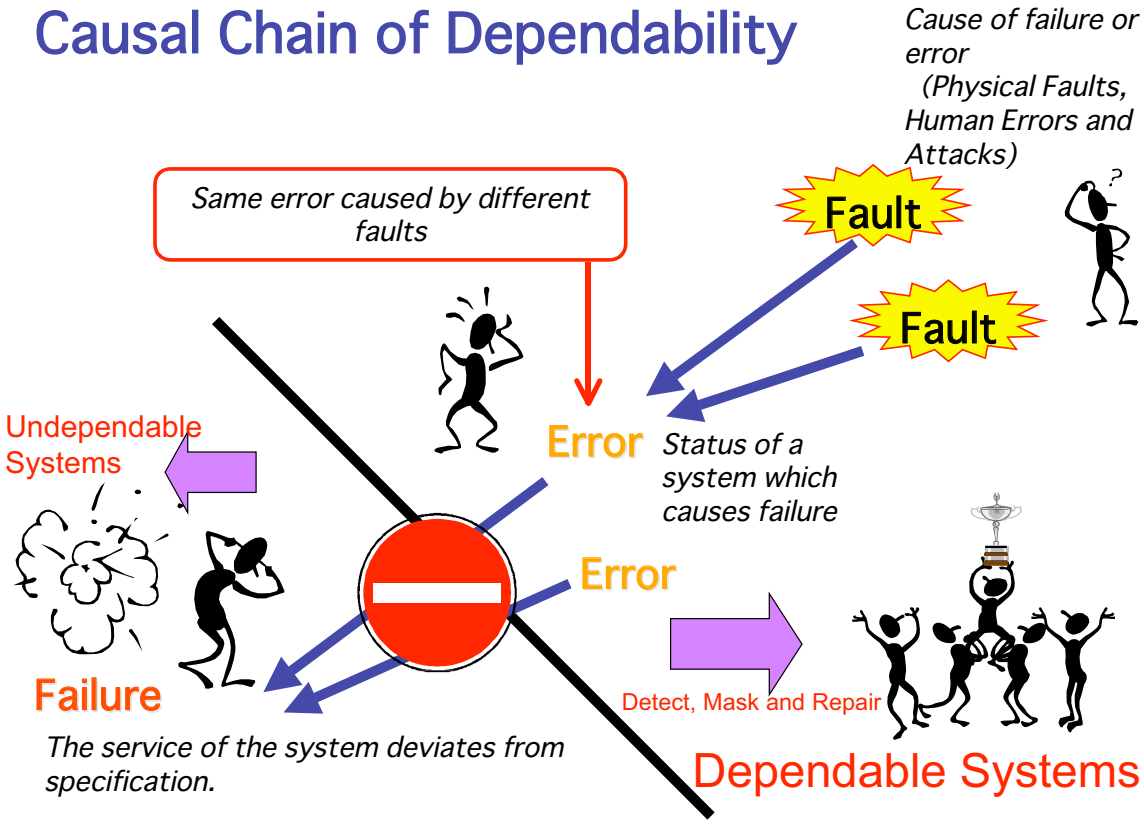
Our daily lives are heavily depends on SoCs.



Requirements for SoC in SII

- SII: Social Information Infrastructure
  - Life: Intelligent Transportation System, Health Care System, Life-line Systems
  - Property: e-Commerce, e-Banking, e-Money
  - Privacy: Authentication System, Communication System
- SII should be dependable for users
  - Secure and reliable operation
  - Stable operation in many years
  - Failure free operation with allowance of some performance degradation
  - Easy to maintenance
  - Gradual and sustainable improvements

Causal Chain of Dependability



A Mathematical Model of Money System

(Inenaga, Oyama and Yasuura 2007)

H A set of Holders

An accumulation type system is more difficult to detect counterfeits than a bill type system.

V A set of Values

n

0

Amount of Value
(1$, ..., 1000$,..., $n$$)

$K^t : M^t \rightarrow H^t$

A set of Media

M

$I^t : M^t \rightarrow V^t$

01001....110

Ownership Function
A mapping from M to H.
Show an owner holder of each medium at time *t*.

Value Function *I*
A Mapping from M to V.
Show value which each medium carries at time *t*.

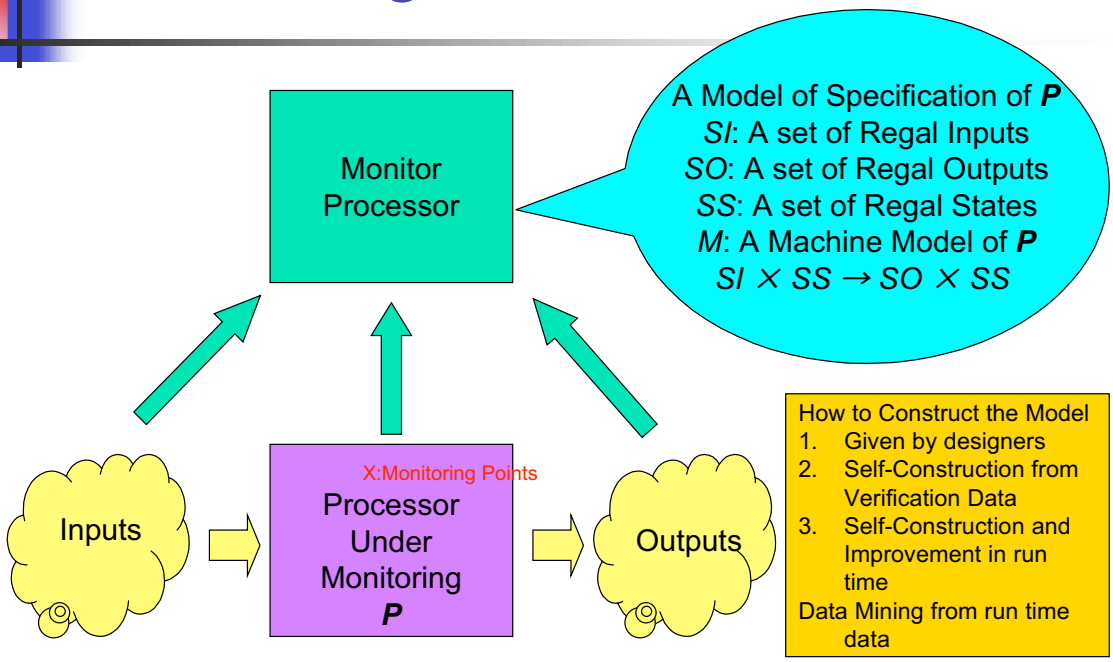
Threats in SoC for e-Money System

	Natural Threats	Human Errors	Attack
Plan		•Bug in Specification	•Theft of Plan
Design		•Design Bugs •Errors in Assumptions	•Theft of Design, •Insertion of Illegal Circuit (IPs)
Fabrication	•Process Variation	•Errors in Fabrication	•Illegal Sale of Extra Products
Test	•Intermittent Faults	•Errors in Test	•Illegal Sale of Good Products
Distribution	•Variation in Packaging	•Mixture of Defectives •Installation of Buggy Software	•Theft •Insertion of Illegal Software
Operation	•Ageing and Particles •Temperature and Supply Voltage Variation	•Errors and Misunderstanding in Usage	•Phishing、Virus •Tampering, • Tapping
Abandonment		•Mis-Arrangement in Replacement	•Theft of Logged Information

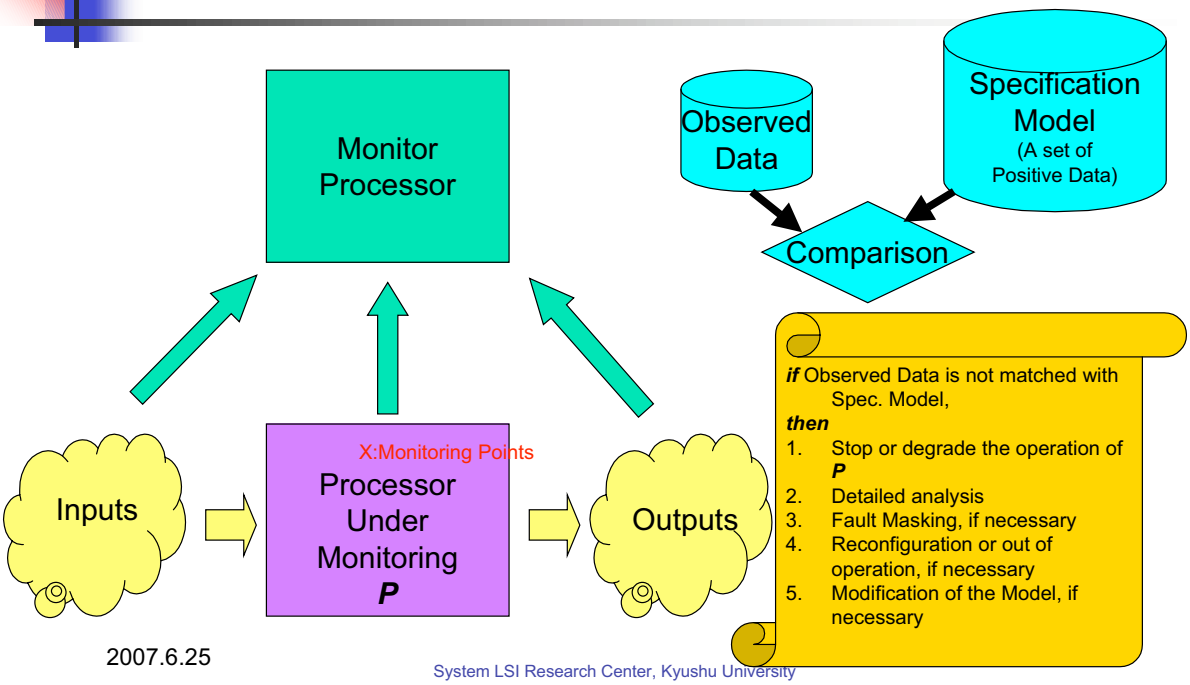
Solutions on MPSoC

- Self-Checking and Self-Detection of Malfunctions
- Fault/Error Masking
- Self-Reconfiguration and Self-Repair
- Autonomic Computing: Monitoring, Analysis, Planning, and Execution
- Adaptation to Change of Specification and Environment

Monitoring Processor Behavior



Checking Malfunctions



Concluding Remarks

- MPSoC is a key component of the social information infrastructure.
- Dependable MPSoC Technology
  - Automatic insertion of mechanisms mutual monitoring of processor cores and self-checking like DFT
  - General mechanism of Design for Dependability (DFD)
  - Application specific techniques
    - ID and Right/Authority management
    - e-money
- Technical Challenges
  - Specification Model Generation using Data Mining
  - Reduction of time and space complexity
  - Coverage of monitoring and masking tech.
  - Measure of Dependability
  - Total solution for various threats in all life cycles of chips