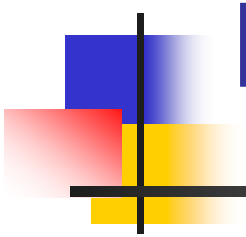
Dependability of VLSI Systems(MPSoC)

安浦, 寛人
九州大学大学院システム情報科学研究院 | 九州大学システムLSI研究センター

出版情報：SLRC プレゼンテーション, 2006-08-15. 九州大学システムLSI研究センター
バージョン：
権利関係：

Dependability of VLSI Systems(MPSoC)

Hiroto Yasuura
System LSI Research Center
Kyushu University

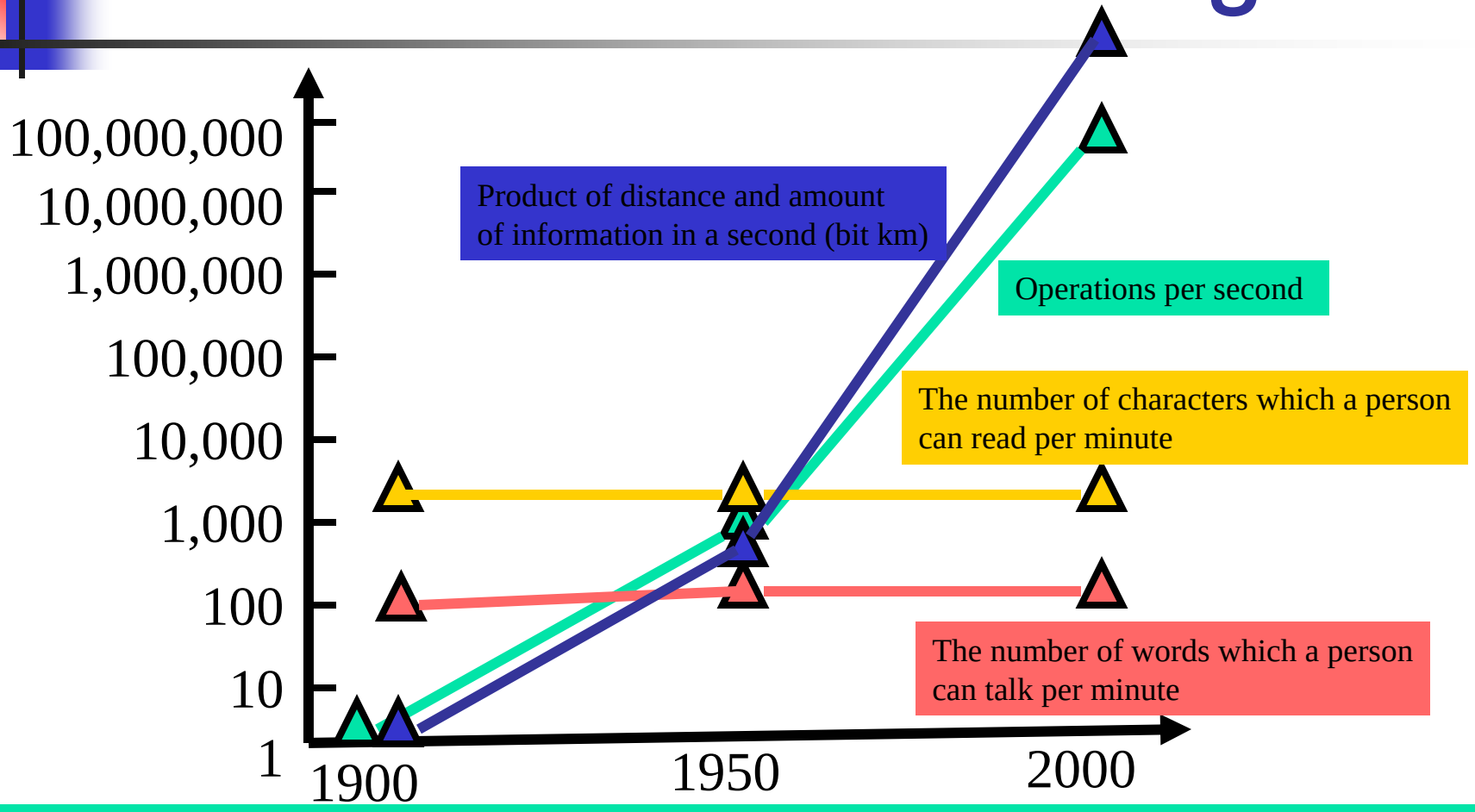


Backgrounds

Rapid Progress of IT Changed Time Constants

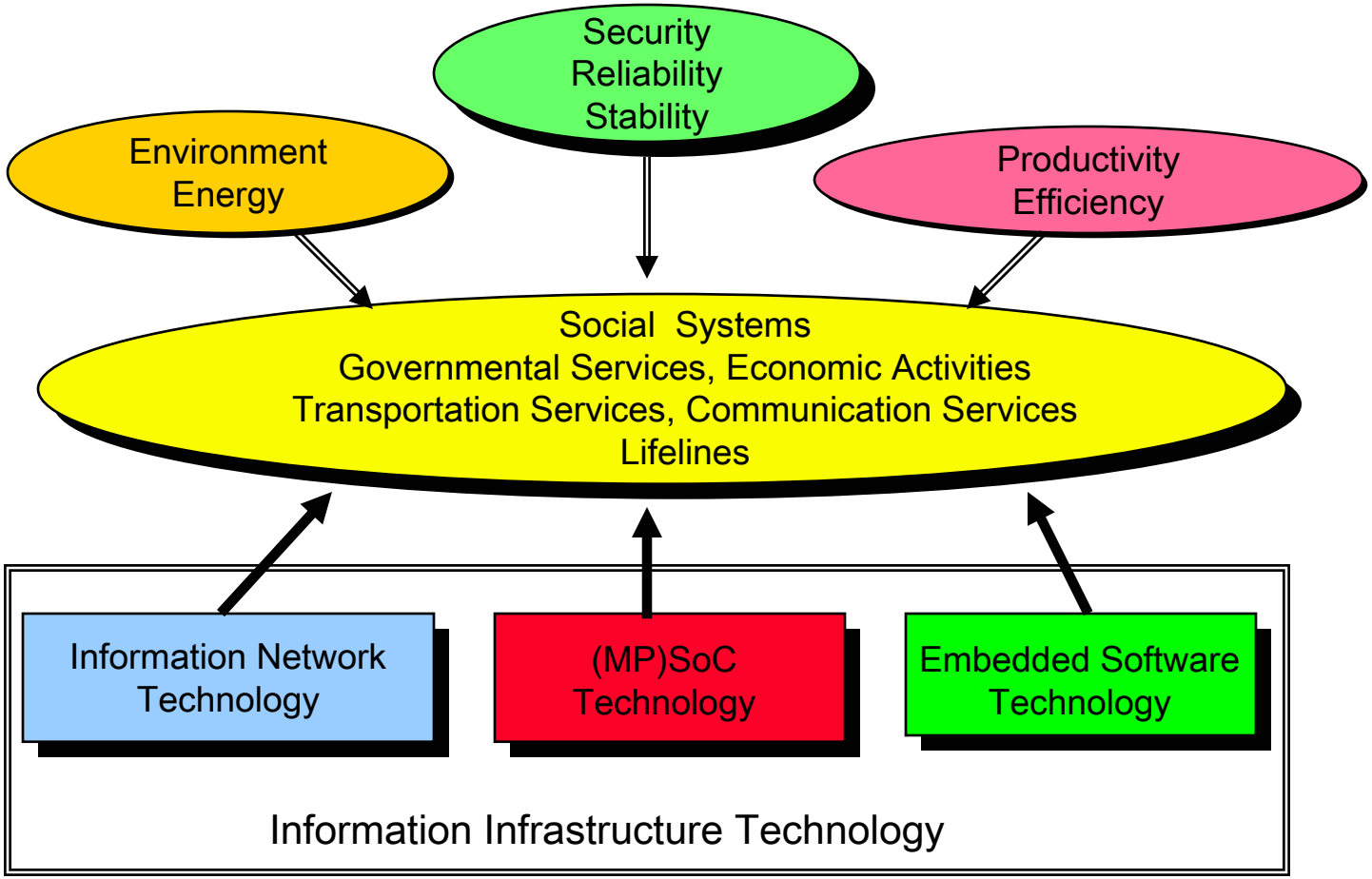
- Time of information transfer and processing has been shortened drastically by IT.(x10^{-6}-10^{-9})
- Basic design of social systems was not supposed the speed-up of information spreading. Time constants of the social systems are completely changed and the stability of the systems is not guaranteed.
  - Stock and foreign exchange markets
  - e-commerce, e-government, e-education,…

Increase of Information Transfer and Processing

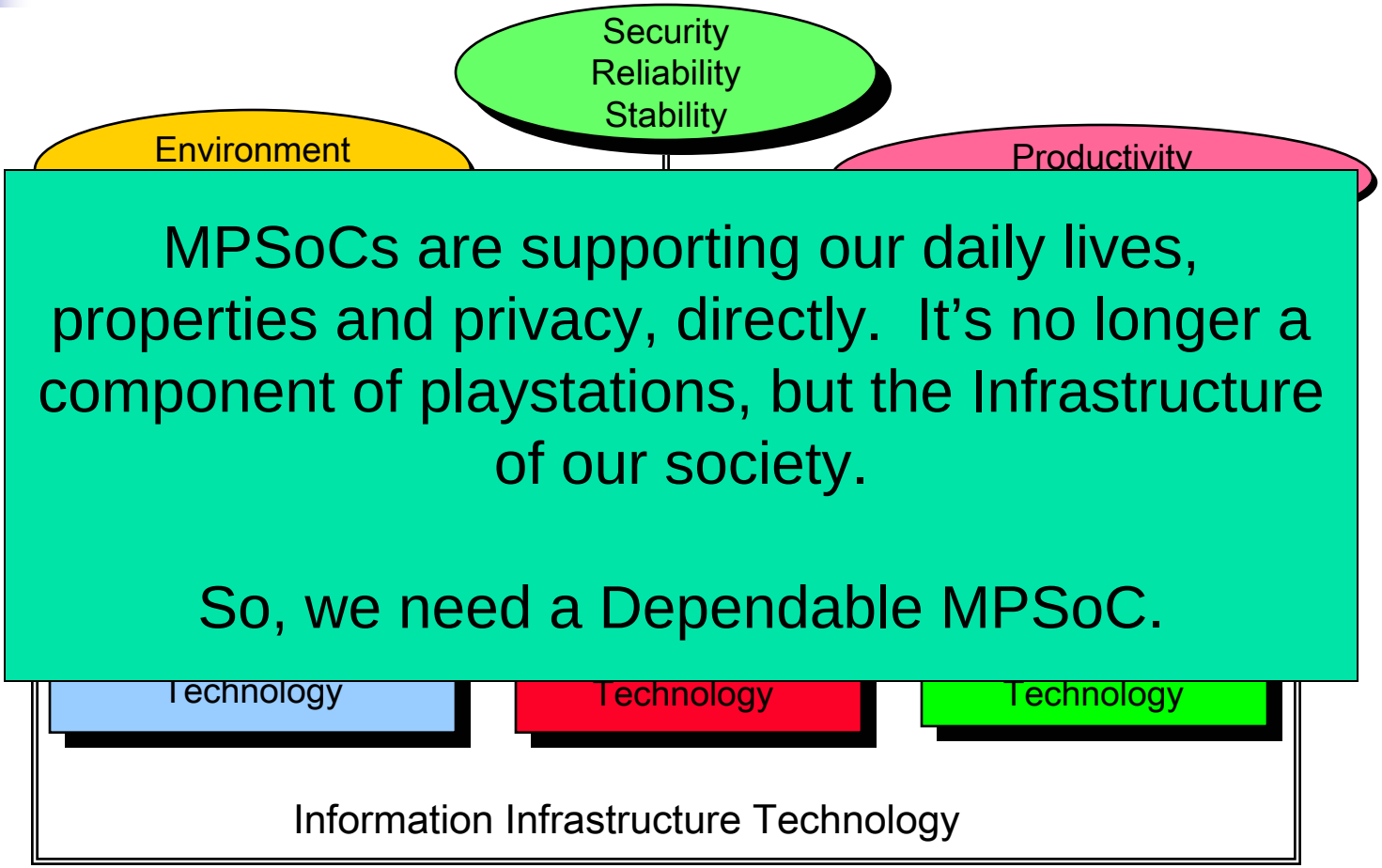


Speed of talking and reading is not improved, but we can now process and transmit huge amount of information using IT.

Information Infrastructure Technologies

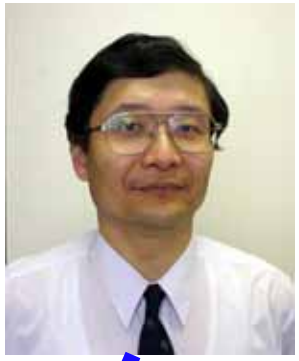


Information Infrastructure Technologies



Values and Credit on a Chip

Hiroto Yasuura
Department of Computer Science and Communication EngineeringGraduate School of Information Science and Electrical EngineeringKyushu University6-1 Kasuga Koen, Kasuga, 816-8580, Fukuoka, Japan
Tel. +81-92-583-7620,
FAX +81-92-5831338
yasuura@c.csce.kyushu-u.ac.jp,
yasuura@slrc.kyushu-u.ac.jp
http://www.c.csce.kyushu-u.ac.jp/SOC/index.html,
http://www.slrc.kyushu-u.ac.jp

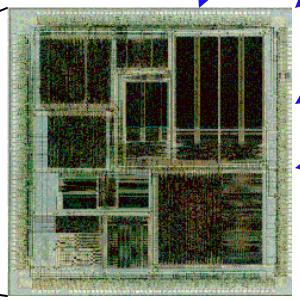


E-Money

$500

Personal Information

$200



$30/Chip

Signature

Credit Cards

Risks and Definitions

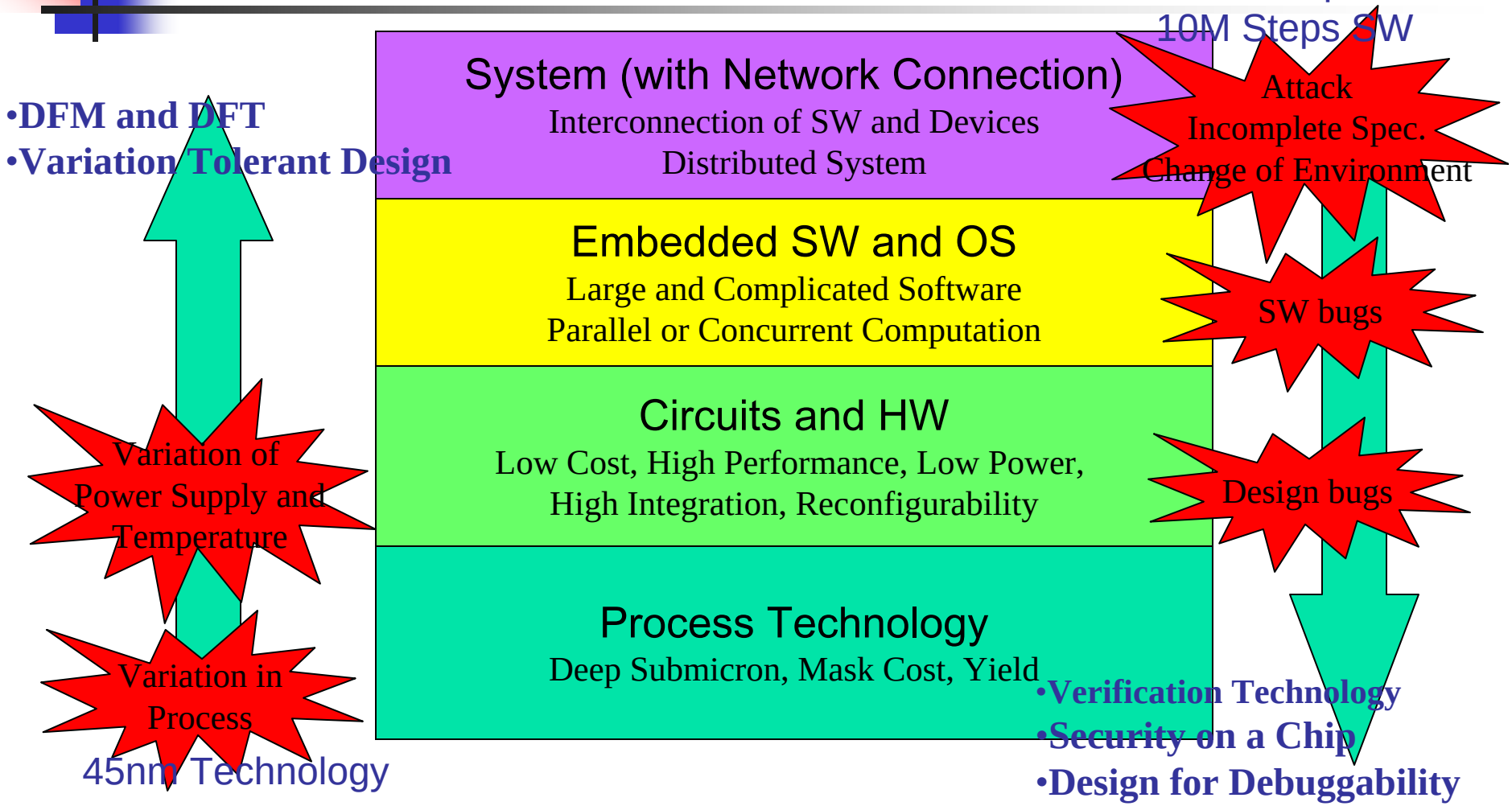
Risks in MPSoC

- Increase of Leakage Current
- Process Variation
- Variation of Supply Voltage
- Variation of Temperature
- Soft Errors by particles
- Cross Talks
- Design Bugs in Logic Circuits and SW
- Complicated Computation on Multi-Processor System (Programmability and Debuggability)
- Incomplete Specification and Misunderstanding of Semantics
- Attacks

- Natural Phenomena
- Human Errors
- Human Attacks

Increase of Variation and Uncertainty

Internet Connection
1GTr. Chip
10M Steps SW



- **DFM and DFT**
- **Variation Tolerant Design**

45nm Technology

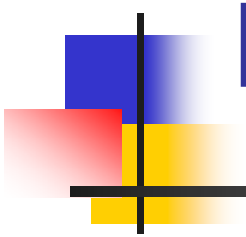
- **Verification Technology**
- **Security on a Chip**
- **Design for Debuggability**

Dependability of System

- Ability to deliver service that can justifiably be trusted
- Dependability contains
  - Availability: Readiness for usage
  - Reliability: Continuity of service
  - Safety: Absense of catastrophic consequences on the user(s) and the environment
  - Confidentiality: Absence of unauthorized disclosure of information
  - Integrity: Absense of improper system alternations
  - Maitainability: Ability to undergo repairs and evolutions
    - Security contains Availability, Confidentiality and Integrity
- IFIP WG10.4 “Dependable Computing and Fault Tolerance” (1980)
- A.Avizienis, J.-C. Laprie, B.Randel, C.Landwehr: ”Basic concepts and taxonomy of dependable and secure computing”, IEEE Trans. on dependable and secure computing. Vol.1. No.1 (Jan. - March 2004)

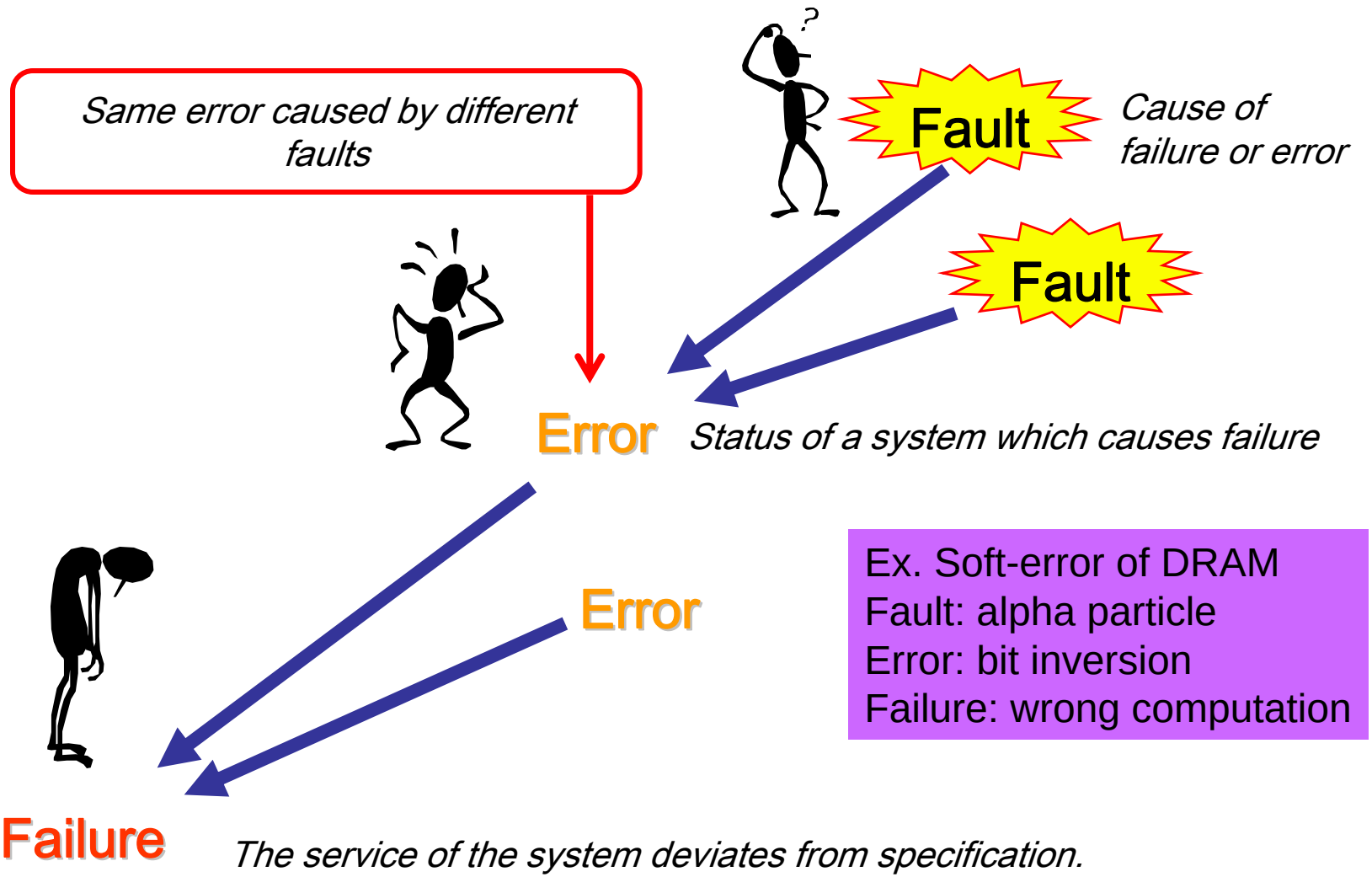
Dependability is

- Concept of User's View.
- Ability to deliver expected services of the system in acceptable range under the circumstances with unexpected events.
  - Basic property to define reasonably limited liability
  - There are several systems requested unlimited liability: Nuclear generation system, Airplane, Governmental systems.
- The biggest problem is that there is no general metrics of dependability.
  - MTBF, MTTR, BER… still not a metrics of Dependability!
  - Comparison with reference systems
  - Absolute standard by social request - privacy etc.
  - Difference of liability - Human life, properties and privacy



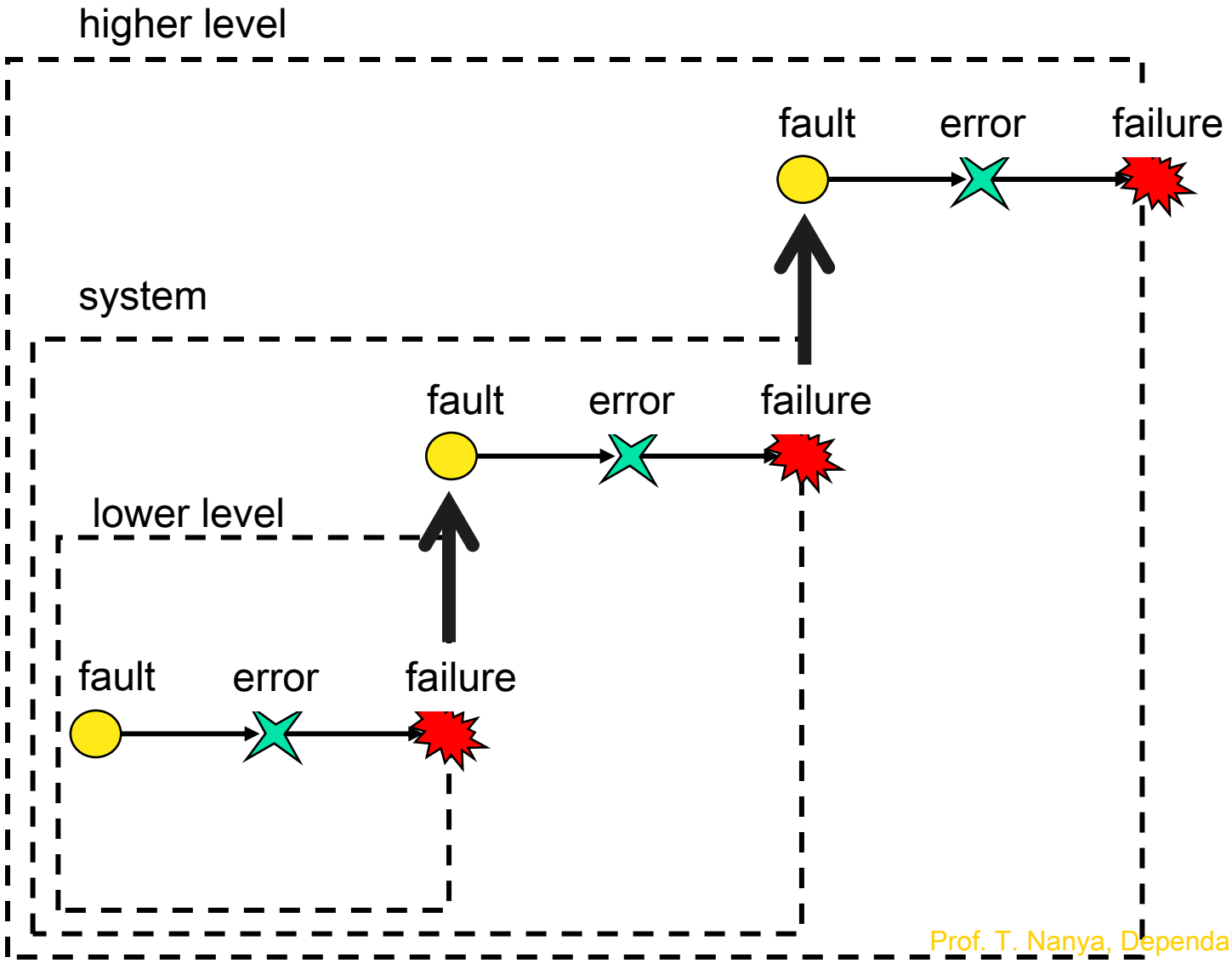
Dependability Chain

Causal Chain of Dependability



Ex. Soft-error of DRAM
Fault: alpha particle
Error: bit inversion
Failure: wrong computation

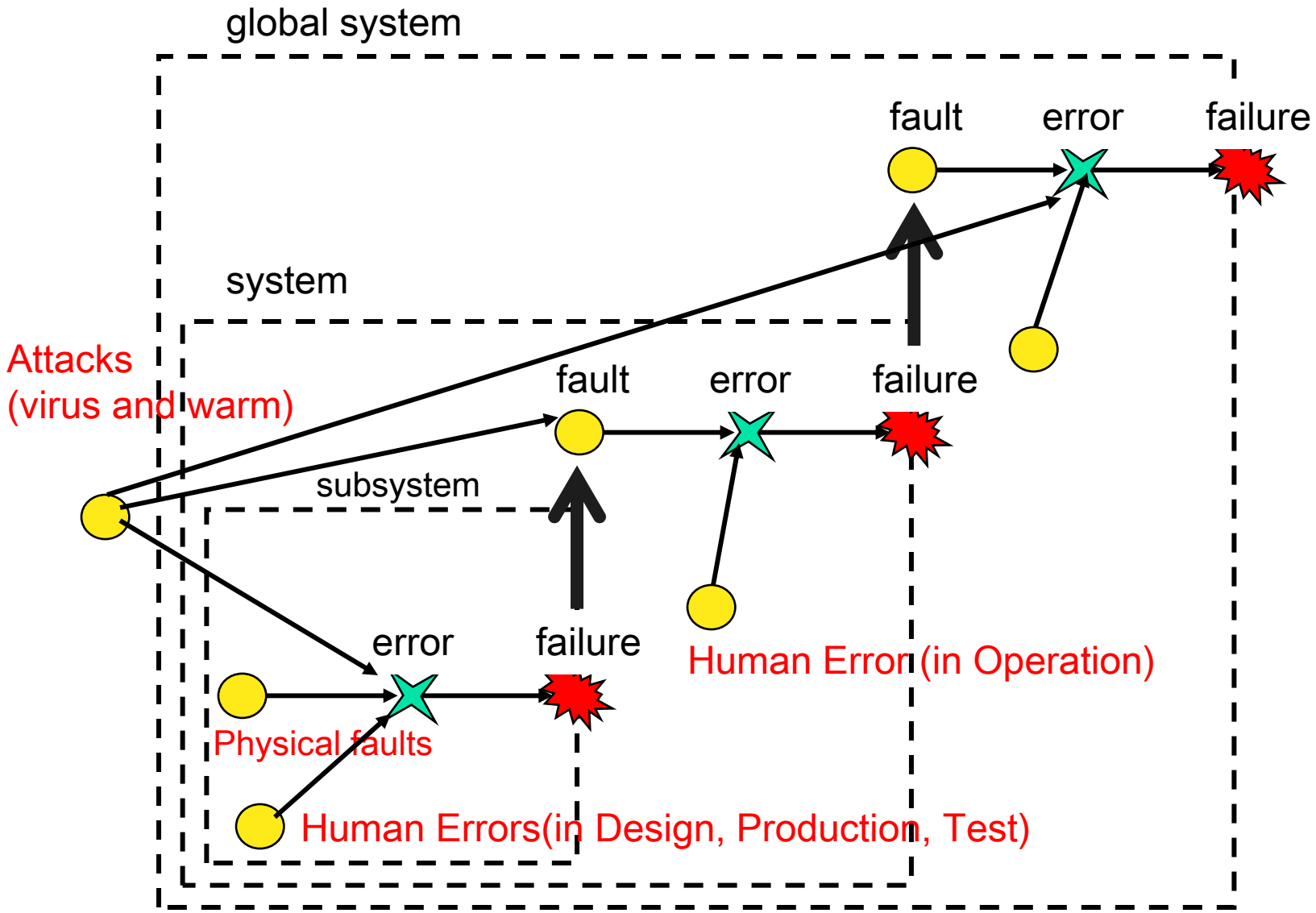
Classical Fault Model: Recursion



Modern Problems on Dependability

- Diversification of Faults
  - Natural Threats, Human Errors and Attacks

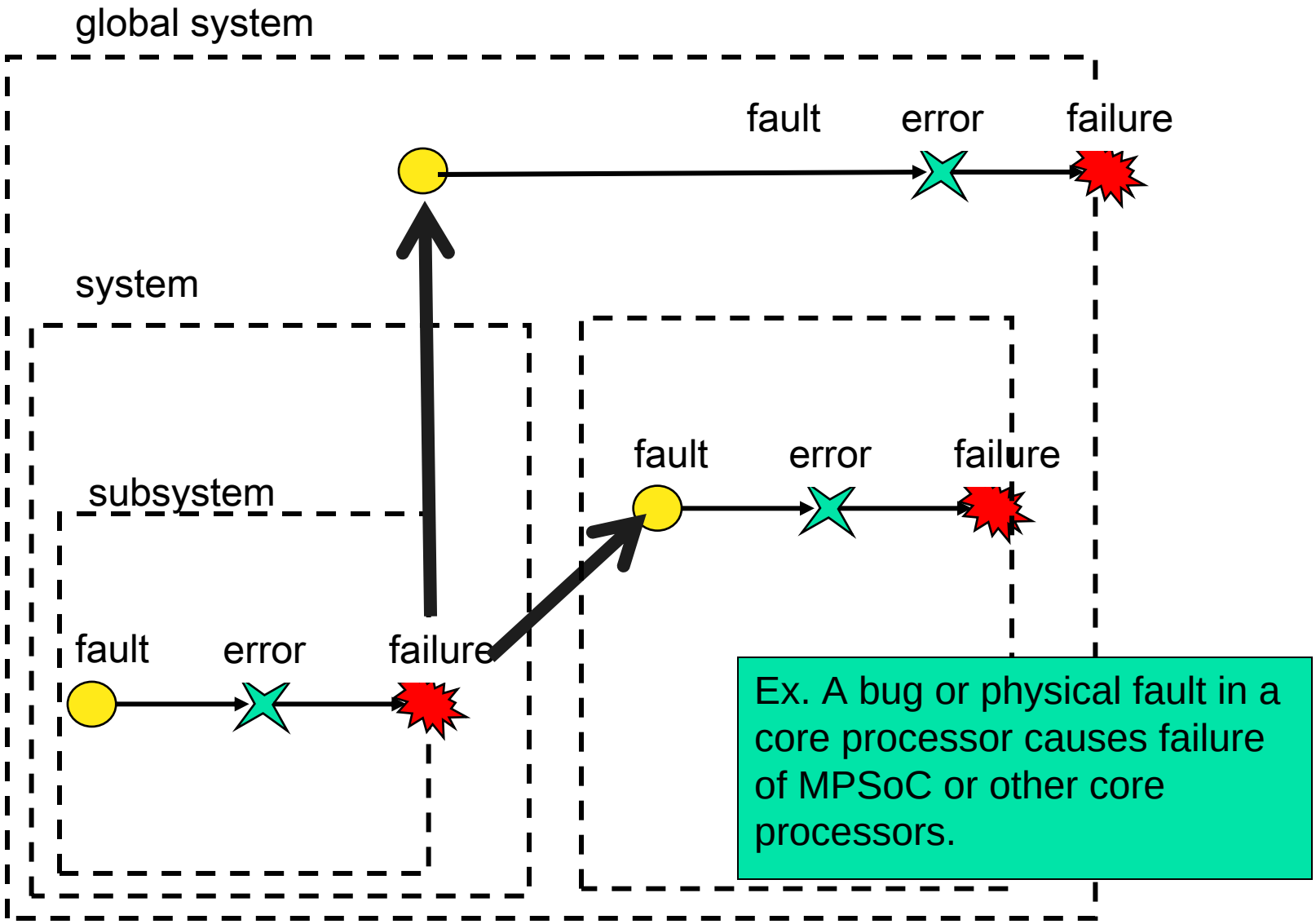
Modern Fault Model: Diversification of Faults



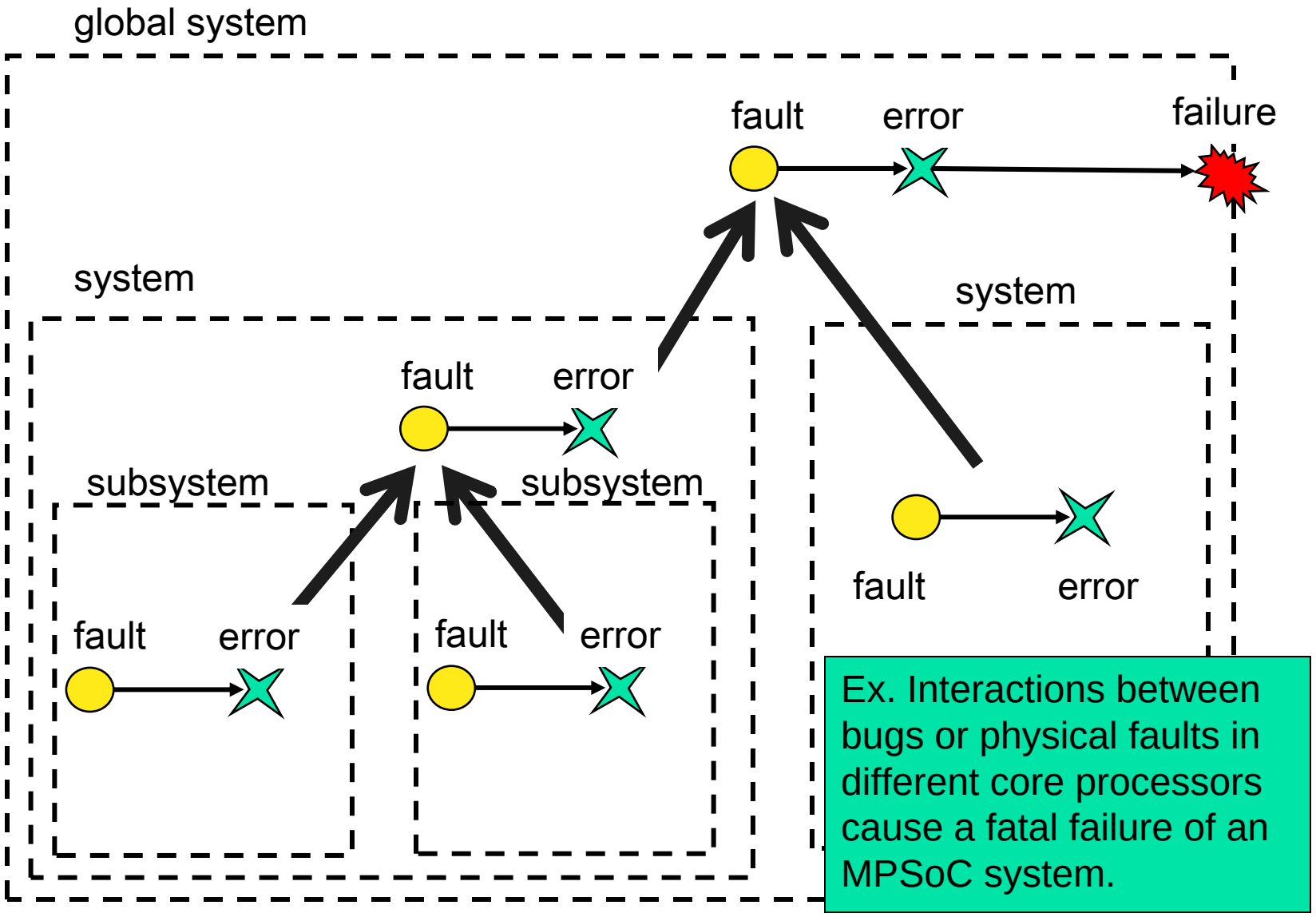
Modern Problems on Dependability

- Diversification of Faults
  - Natural Threats, Human Errors and Attacks
- Diversification of Relations between Fault and Failure
  - Skipping layers and system boundaries
  - Interaction of several Faults

Modern Fault Model: Skipping layers and boundaries



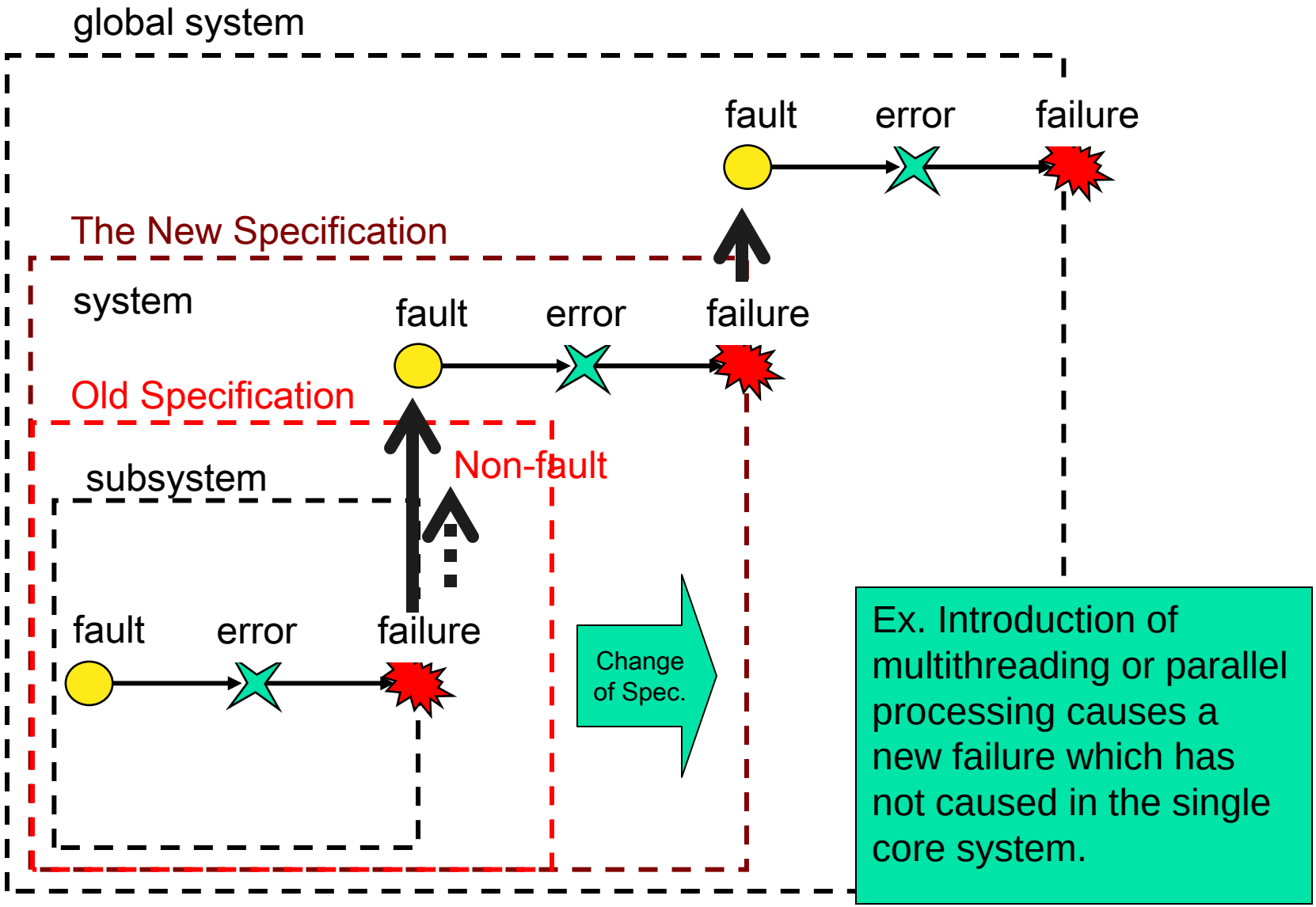
Modern Fault Model: Interaction

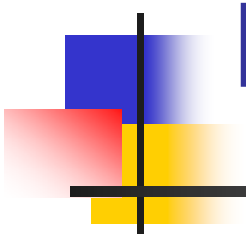


Modern Problems on Dependability

- Diversification of Faults
  - Natural Threats, Human Errors and Attacks
- Diversification of Relations between Fault and Failure
  - Skipping layers and system boundaries
  - Interaction of several Faults
- Definition of Failure
  - Dynamic Change of System Specification

Modern Fault Model: Change of Specification





Faults in MPSoC

Classification of Faults

- Natural Threat
  - Noises: Electro-Magnetic, Vibration, Power Supply, Temperature, Particles
  - Faults in Device: Ageing, electronic Migration,
  - Process Variation
- Human Errors
  - Errors in specification and design
  - Errors in fabrication process and testing
  - Errors in SW
  - Errors in system operation
- Human Attacks
  - Attacks in design phase, foundry, test and operation
- Interaction of various faults
  - System-to-system, system-to-human, and human-to-human
  - Parallel computation on multi-processor system
  - It becomes difficult to define “specification”!!!

Life Cycle Stages of MPSoC

- Planning and Definition of Specification
- Design HW and SW
- Fabrication
- Test
- Distribution and Version-up of SW
- Operation
- Abandonment and/or Replace

Possible Faults : Chip on Automobile

	Natural Threats	Human Errors	Attack
Plan		•Bug in Specification	•Theft of Plan
Design		•Design Bugs, •Errors in Assumptions	•Theft of Design
Fabrication	•Process Variation	•Errors in Fabrication	
Test	•Intermittent Faults	•Errors in Test	•Mixture of Defectives
Distribution	•Variation in Packaging	•Mixture of Defectives and buggy SW	•Mixture of Counterfeits
Operation	•Ageing and Particles •Temperature and Supply Voltage Variation	•Errors of Drivers and Maintenance	•Attack by RF
Abandonment		•Mis-Arrangement in Replacement	•Theft of Logged Information

Possible Faults : Chip for Electric Commerce

	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	•Theft
Operation	•Ageing and Particles •Temperature and Supply Voltage Variation	•Errors and misunderstanding of Users	•Phishing、Virus •Tampering, • Tapping
Abandonment		•Mis-Arrangement in Replacement	•Theft of Logged Information

Dependability Measures

	Natural Threats	Human Errors	Attack
Plan	•Estimation of Lifetime •Expectation of Circumstances	•Complete Spec., •Expectation of Life Cycle	•Security Control •Expectation of Attacks
Design	•FTC, DFM, DFT • Measures for Noise •Embedded Monitors •Simple Architecture	•Design Verification, •Design Quality Control, •DFT •Increase of Operability	•Data Management •Anti-Tampering •Security-on-Chip
Fabrication	•Control of Variation	•Process Management	•Process Management
Test	•Increase of Test Accuracy, •Test under Bad Condition	•Test Management •Self Tests •Improvement of Test Accuracy	•Test Management •Monitoring
Distribution	•Control of Environment	•Management of Distribution	•Tracing
Operation	•Monitoring of Circumstances •On-line Self Test	•Log Monitoring •Education of Users	•Education of Users •Monitoring, Measures for Attacks
Abandonment	•Scheme for Self-Killing	•Automatic Erase	•Nullification

Dependability Measures

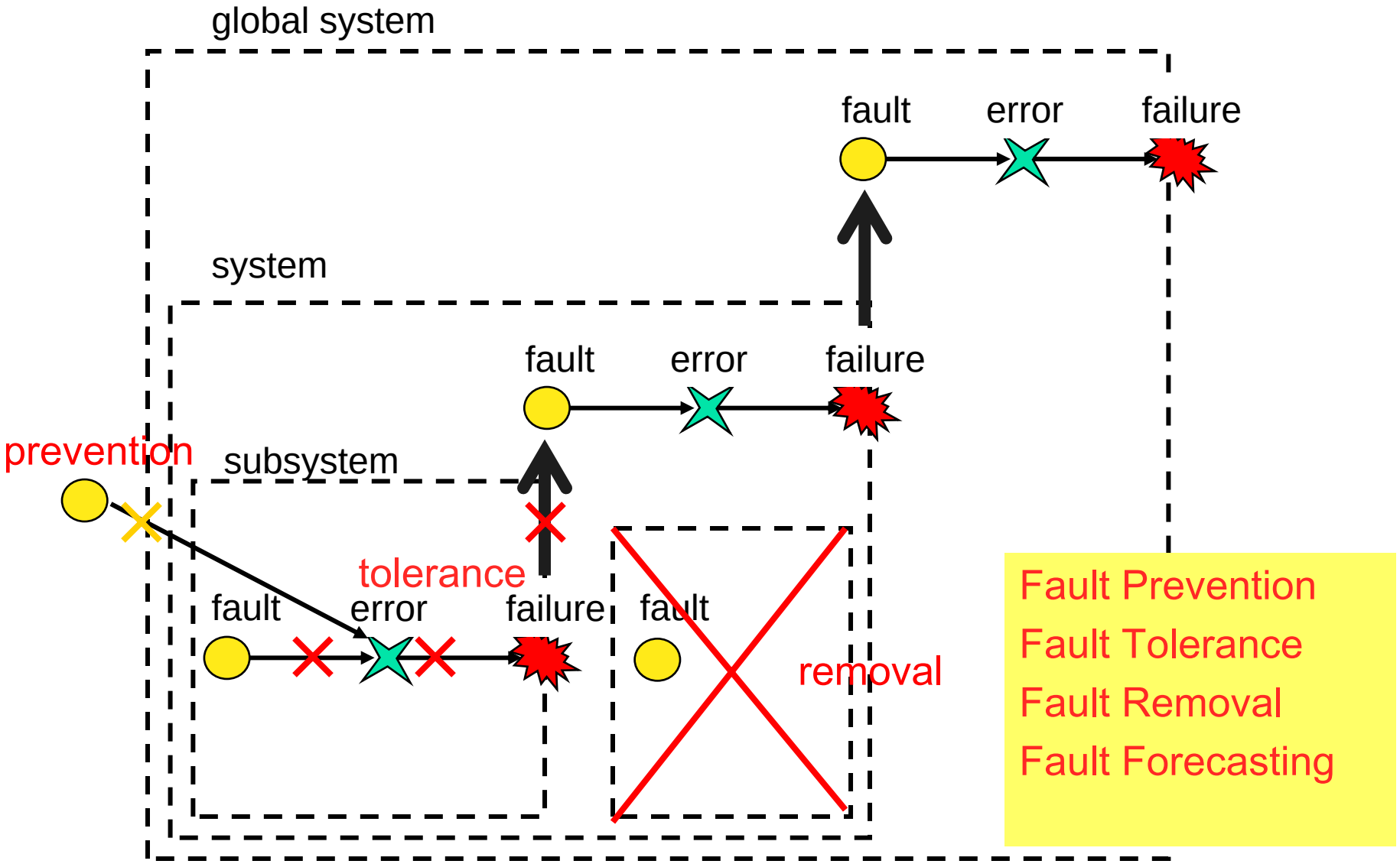
	Natural Threats	Human Errors	Attack
Plan	Estimation of Lifetime Expectation of Circumstances	Complete Spec., Expectation of Life Cycle	Security Control, Expectation of Attacks
Operation	Circumstances, Online Self Test	Log Monitoring Education of Users	Monitoring, Measures for Attacks
Abandonment	Scheme for Self-Killing	Automatic Erase	Nullification

We can share techniques and measures for different kinds of faults in different stages.

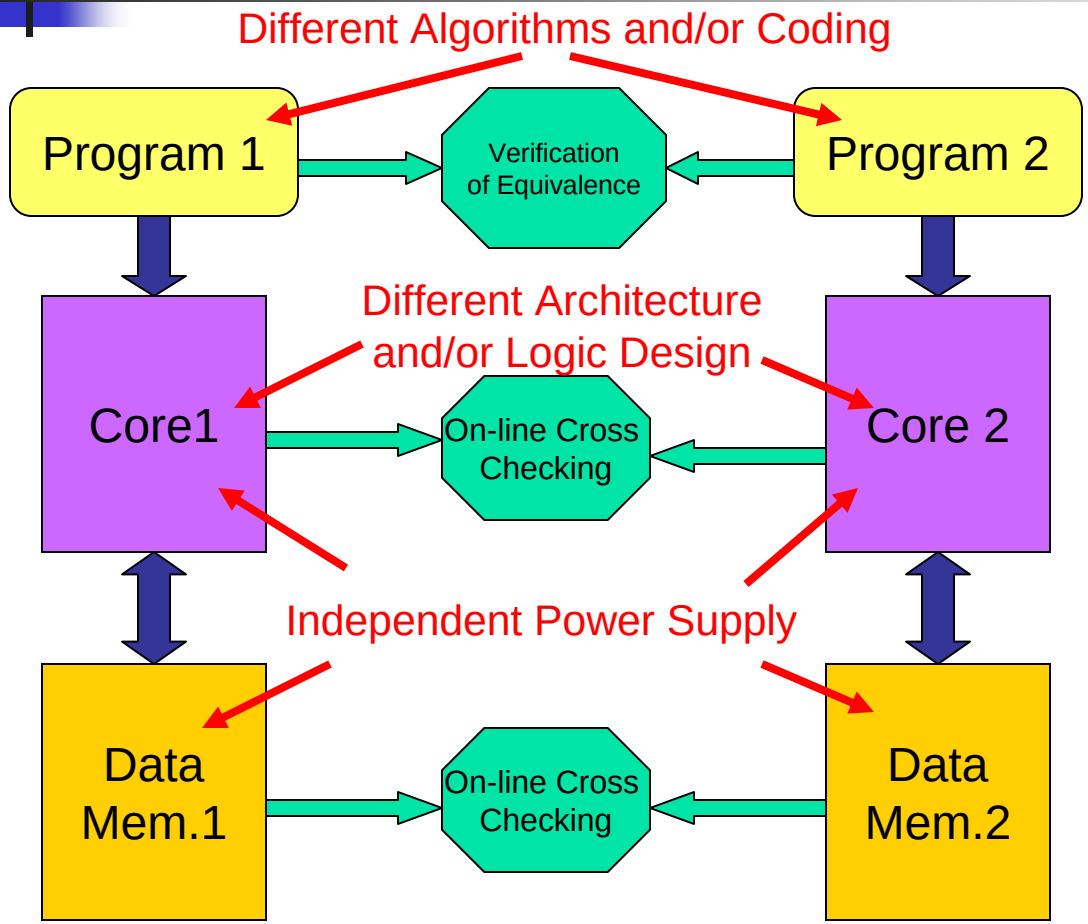
Interactions of various faults will cause unexpected system failures.

Measures for Dependability

How to Implement Dependability



Fault Tolerance in MPSoC
-Heterogeneous Redundancy-

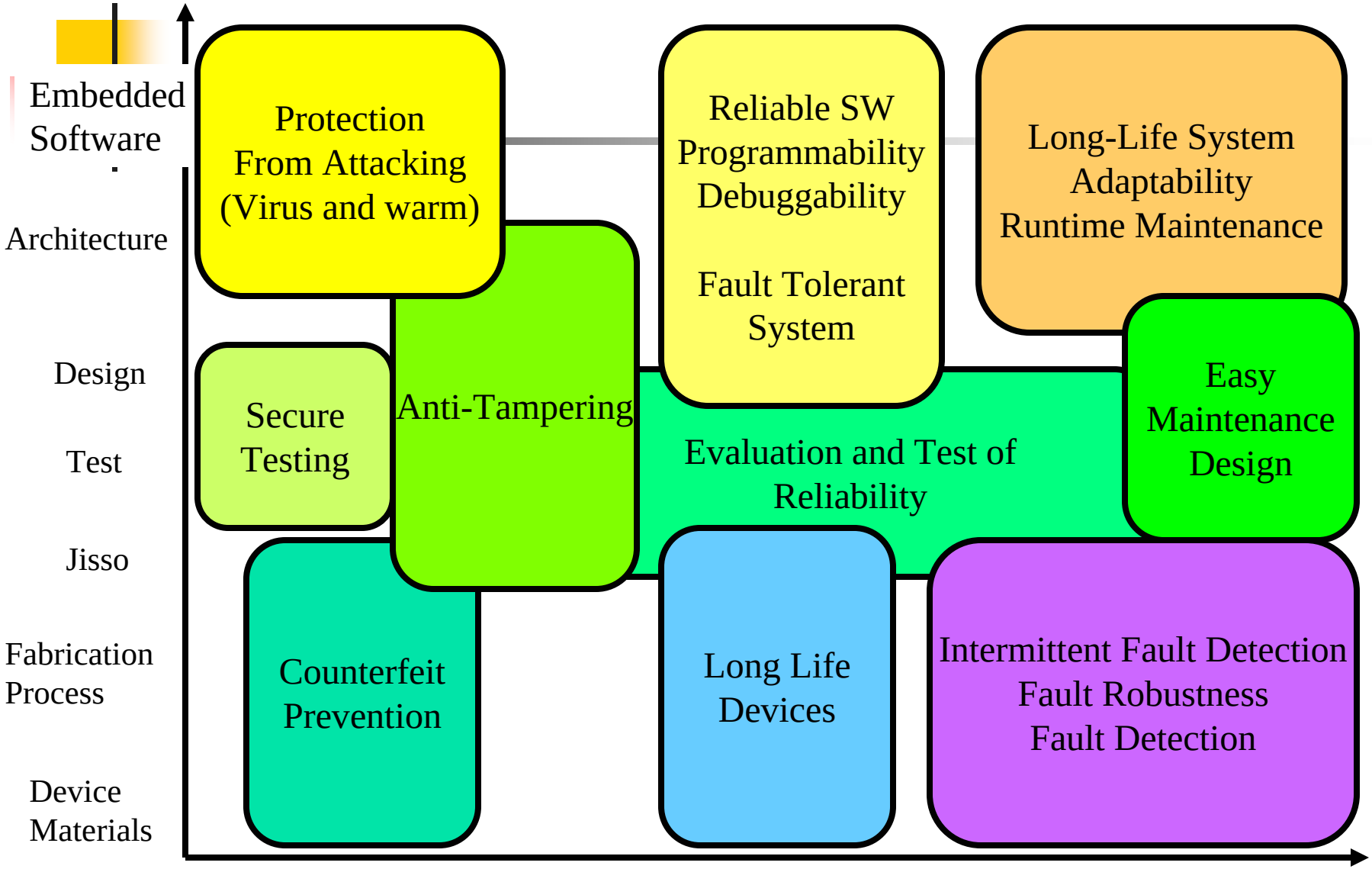


Redundancy of Algorithms and Programs
- •SW bugs
- •Attacking

Redundancy of Computation
- •Logic Design Errors
- •Physical Variations
- •Soft Errors
- •Attacks

Redundancy of Storage
- •Physical Variations
- •Soft Errors
- •Attacks

New SoC Technologies for Dependability



Conclusions

- MPSoC is a key component of the social infrastructure. Our daily lives are heavily depends on its dependability.
- Natural threat, Human errors and Attacks in all life stages of MPSoC should be considered as causes of system failures.
- Measures against various faults should be developed under collaboration of System designers, SW and HW designers, Test engineers, Operators/Users, and Service providers.

Dependable Computing in…

- VLSI / HW
- Operating Systems
- Embedded Software
- Communication Systems
- Social Infrastructures
- Quality, Reliability and Security