Current Research Activities on Dependable Computing and other Dependability Issues in Japan

Yoshihiro Tohma[1] and Masao Mukaidono[2]

1) Tokyo Denki University, tohma@sie.dendai.ac.jp
2) Meiji University, masao@cs.meiji.ac.jp

Aim

- To introduce researches on dependable computing and the related issues currently conducted in Japan
- Comprehensive survey not intended, simply depending on the authors' view

Outline

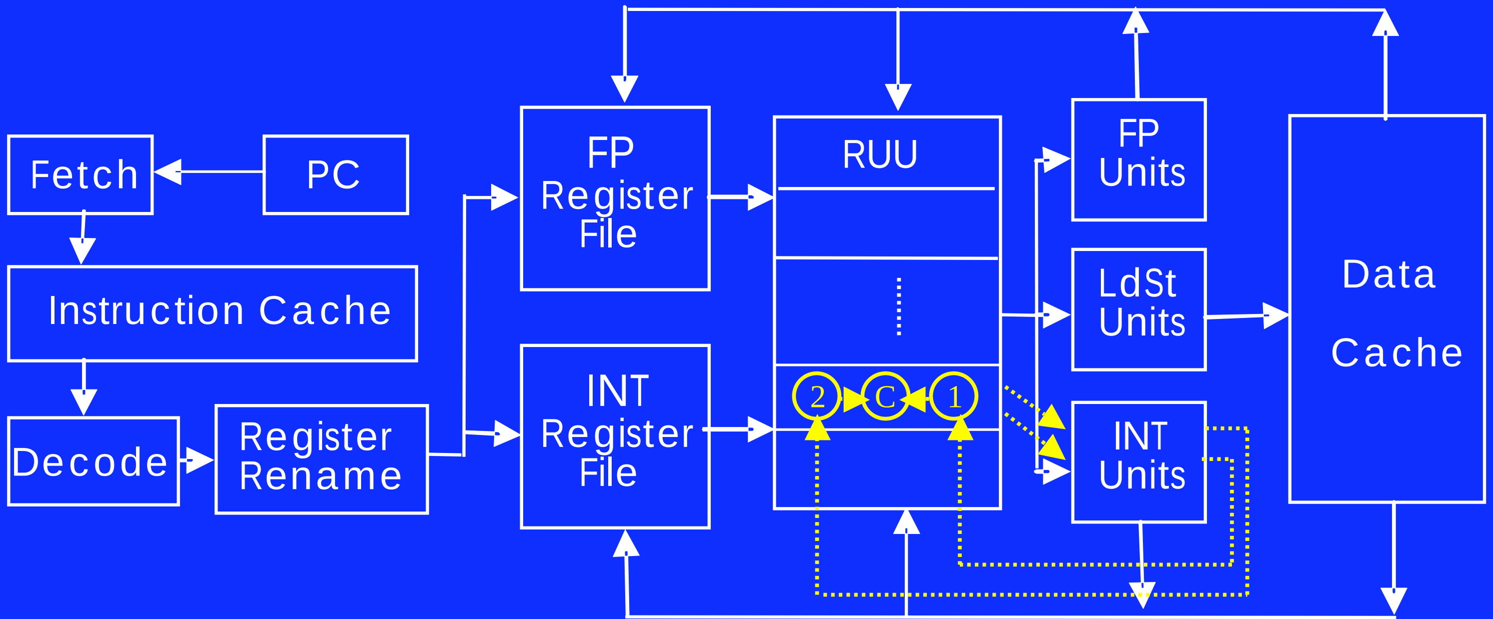
- New Paradigms of dependable computing
  - Mobile computing (Sato, 2003)
  - Use of COTS for Internet services (Mishima and Akaike, 2003)
  - Grid computing (Tohma, 2003)
  - New frontier (Yokogawa et al, 2003)
- Extension of dependability concept to other world
  - Safety Mandara (Mukaidono, 2002)
  - Stadardisation on safety of machinery (Mukaidono, 2002)

Fault Tolerance in Mobile Computing

- Microprocessors in mobile computing platforms such as cellular phone, PDA, etc.
  - Small size, light weight, high speed clock
  - Produced by sub-micron fabrication technologies
  - Vulnerable to radiation
  - Transient error
  - real-time and continuous services mandatory

- Fault tolerance against transient error
  - Duplication-comparison and retry
    - Serial two times execution of an instruction and comparison
    - Instruction reissued upon mismatch
  - Superscalaring
    - Concurrent execution of multiple instructions
    - Time penalty for two times execution of an instruction alleviated

- Architecture

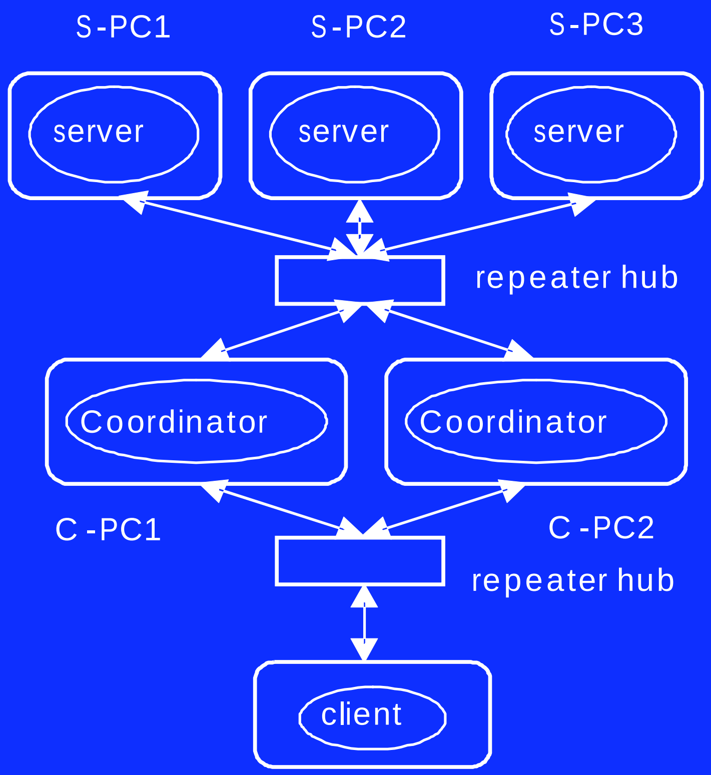


- Performance penalty
  - Benchmark programs
    - SPEC200 and MediaBench
  - Incease of execution cycles (in average) in 8 way superscalaring
    - 44.2% for SPEC2000 and 44.7% for MediaBench
- Improvement
  - Earlier speculative update of branch prediction
  - Elimination of redundant memory (data cache) access
  - about 30% overhead attained

Use of COTS for Internet Services

- Requirements
  - Low cost
  - Fault tolerance by proprietary OS such as voting and/or fault isolation inappropriate
  - Real-time operation
- Approach
  - Use of commodity HW and SW not modified, nor recompiled, nor vendor-specific
  - Fault tolerance of server emphasized

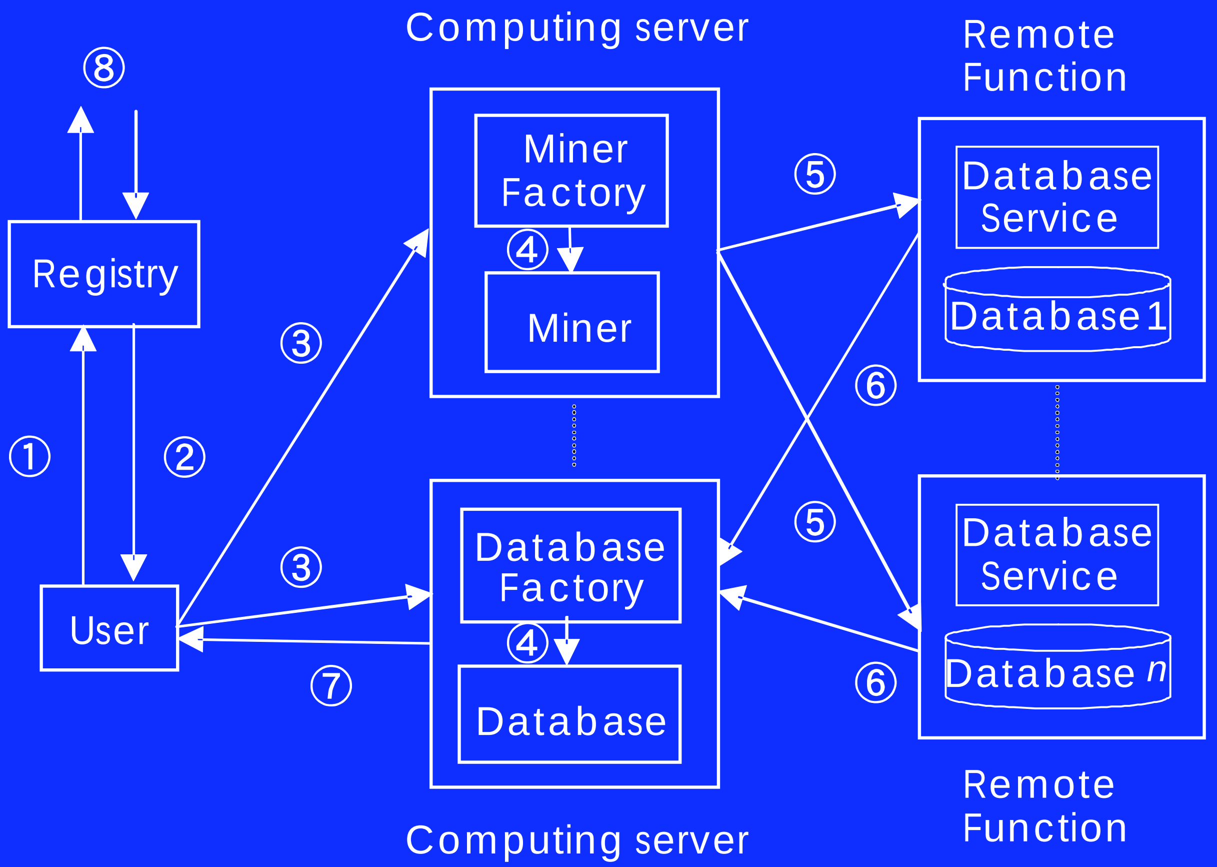
  - Primary-backup inappropriate for server
    - Active replication
- Architecture
  - Server: TMR
  - Coordinator
    - Making server's fault tolerance transparent to users, modification of HW and SW unnecessary
    - Interchange of IP addresses
    - Primary-backup



FT in New Computation Paradigm

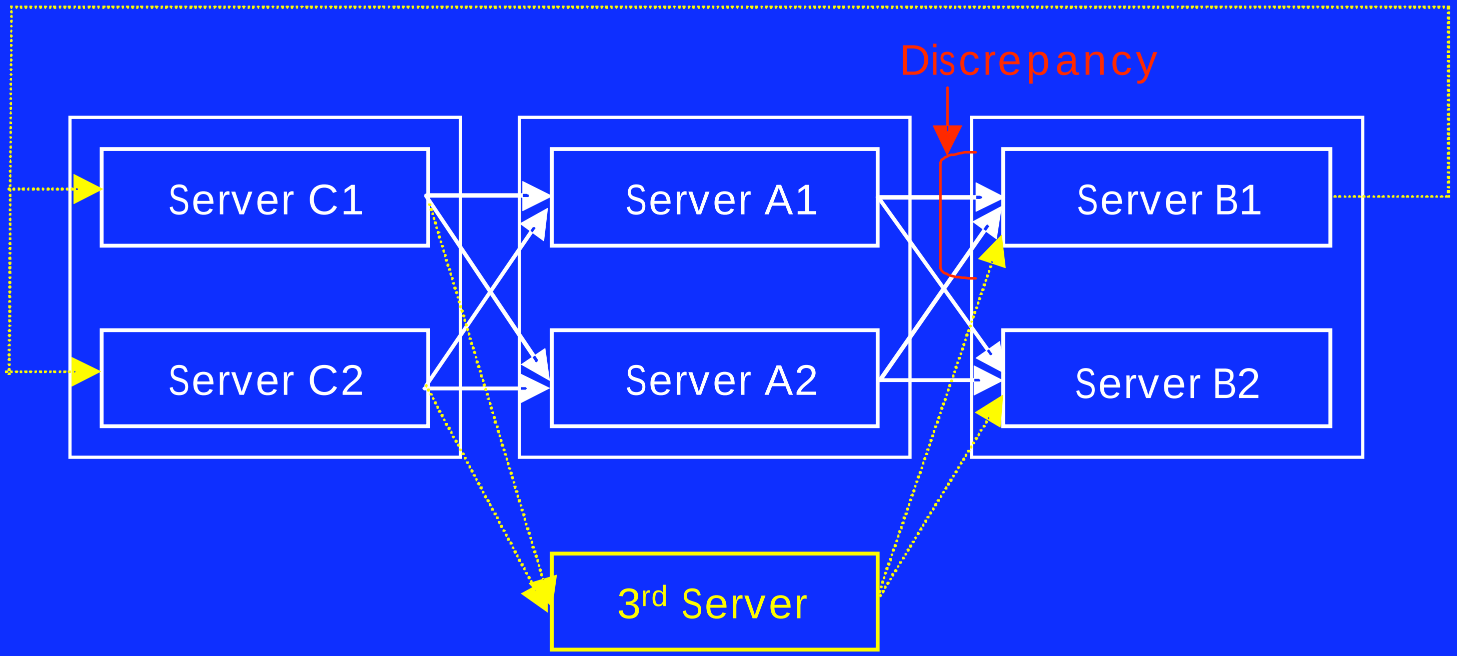
- Characteristic to current computing systems
  - Giant
    - Fault-prone
  - Networked
    - Spread of abnormity
  - Continuous expansion of system configuration with non-stop services
    - Centralized management difficult
- New approach
  - Distributed over network(s)
  - Autonomous without centralized management

- Model


Computing server
Remote Function
⑧
Miner Factory
Database Service
⑤
④
Registry
Miner
Database1
③
⑥
①
②
⑤
Database Factory
Database Service
③
User
④
Database n
⑦
⑥
Database
Remote Function
Computing server

- Ease and difficulty of fault tolerance
  - Ease
    - Replacement of faulty servers easy
  - Difficulty
    - Registry
      - How to implement fault tolerance in its own
        - Stand-by spare imperative
      - How to maintain the health information of servers
    - Notification/Recognition of abnormity
      - During service operation after initial negotiation completed
      - Need robust error detection and communication components

- Alleviation of difficulty

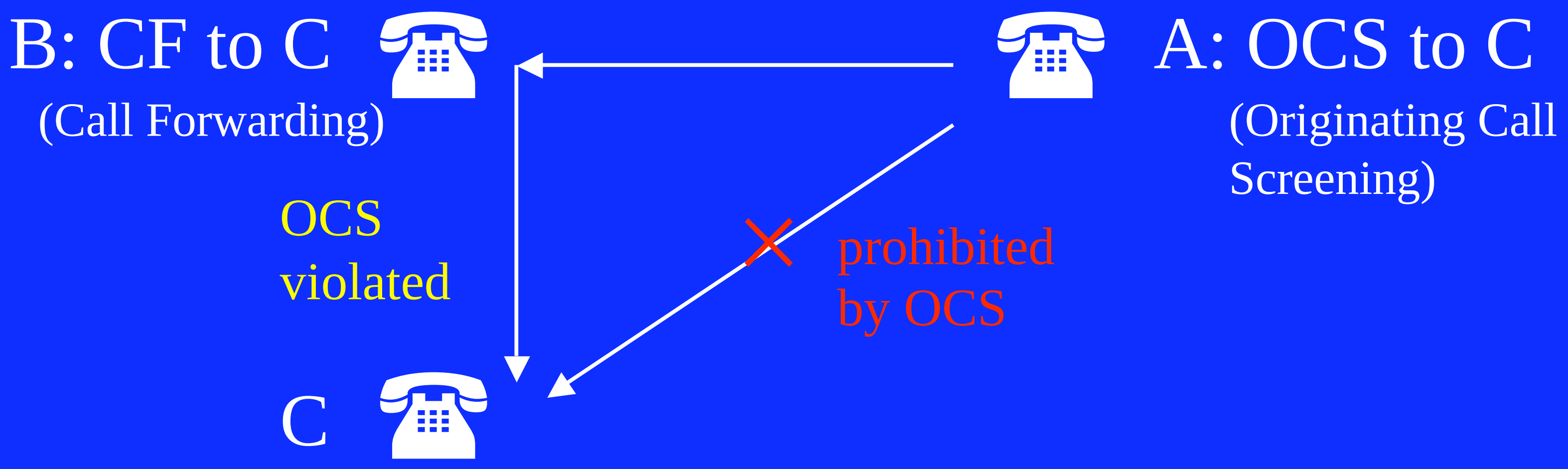


New Frontier of DC

- Functionality (feature) interaction
  - Caused by inadvertent augmentation of functionality
  - Disable some function(s) already installed
  - New challenge – detection of feature interaction
- Examples in telephony

OCS vs CF

(Originating Call Screening) (Call Forwarding)



B: CF to C

(Call Forwarding)

A: OCS to C

(Originating Call Screening)

OCS violated

prohibited by OCS

C

- Detection of feature interaction
  - Rule-based definition of functions
  - Definition of state transition
  - Reachability check to state(s) of feature interaction

- Formal representation
  - Service SVC

$$\text{SVC} = (U, V, P, E, R, s_{init})$$

Example

U : Set of users $= \{A, B\}$

V : Set of variables $= \{x, y\}$

P : Set of predicates $= \{idle(x), dialltone(x), busytone(x), calling(x, y), talk(x, y)\}$

E : Set of events $= \{onhook(x), offhook(x), dial(x, y)\}$

R : Set of rules $= \{r : pre-condition \lfloor event \rfloor post-condition\}$

s_{init} : Initial state $= \{idle(A), idle(B)\}$

– Rules (examples)

$r_1 : idle(x)[offhook(x)]dialtone(x)$

$r_2 : dialtone(x)[onhook(x)]idle(x)$

$r_3 : dialtone(x), idle(y)[dial(x,y)]calling(x,y)$

$r_4 : dialtone(x), \neg idle(y)[dial(x,y)]busyone(x)$

$r_5 : calling(x,y)[onhook(x)]idle(x), idle(y)$

$r_6 : calling(x,y)[offhook(y)]talk(x,y), talk(y,x)$

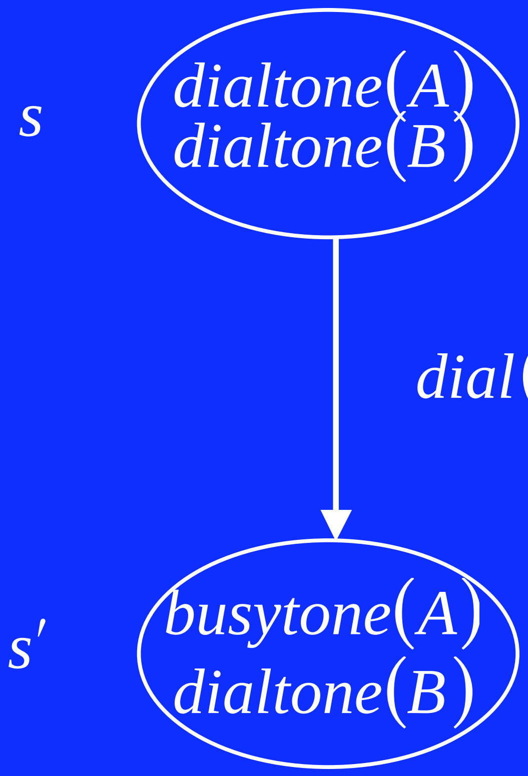
$r_7 : talk(x,y), talk(y,x)[onhook(x)]idle(x), busytone(y)$

$r_8 : busytone(x)[onhook(x)]idle(x)$

$r_9 : dialtone(x)[dial(x,x)]busytone(x)$

– State transition

- s : state, a set of predicates



s

$dialtone(A)$
$dialtone(B)$

s'

$busytone(A)$
$dialtone(B)$

$$\left.\begin{matrix} r_2 \\ r_4 \\ r_9 \end{matrix}\right\} \text{enabled at } s$$

$$dial(A,B) \in r_4$$

$$s \setminus Pre[r_4(x = A, y = B)]$$

$$\{dialtone(A), dialtone(B)\} \setminus \{dialtone(A), \neg idle(B)\}$$

$$\cup\, Post[r_4(x = A, y = B)]$$

$$\{busytone(A)\}$$

- Example of interaction
  - Non-determinism
    Two or more rules activated by the same event at a state
  - Invariant violation
    Unable to decide by reachability check to state(s) where the invariant holds

$$\bigcup_{\{r_i,r_j\} | r_i,r_j \in R} \; \bigcup_{\{\theta_i,\theta_j\} | e[r_i\theta_i]=e[r_j\theta_j]} E_{r_i\theta_i} \wedge E_{r_j\theta_j}$$

$$f_G(s) = \neg Inv(s)$$

- Example of detecting feature interactions
  - 7 features

    CW : allows receiving the second incoming call while talking
    CF : allows forwarding incoming calls to another address
    OCS : allows specifying outgoing calls to be restricted or permitted
    TCS : allows specifying incoming calls to be restricted or permitted
    DO : allows disabling any call from the terminal. Only terminating calls permitted
    DT : allows disabling any calls terminating at the terminal. Only originating calls permitted
    DC : so-called hot-line service. The specified address is called simply by off-hooking

  - 11 combinations result in non-determinism
  - 9 combinations result in violation of invariant

Findings

- Importance of fault tolerance ever increases in any circumstances.
- Fault tolerance technology never saturates.
- We are facing new challenge at any time.

Extended Application of Dependability Concept to Other Worlds

Two activities on safety issues in Japan

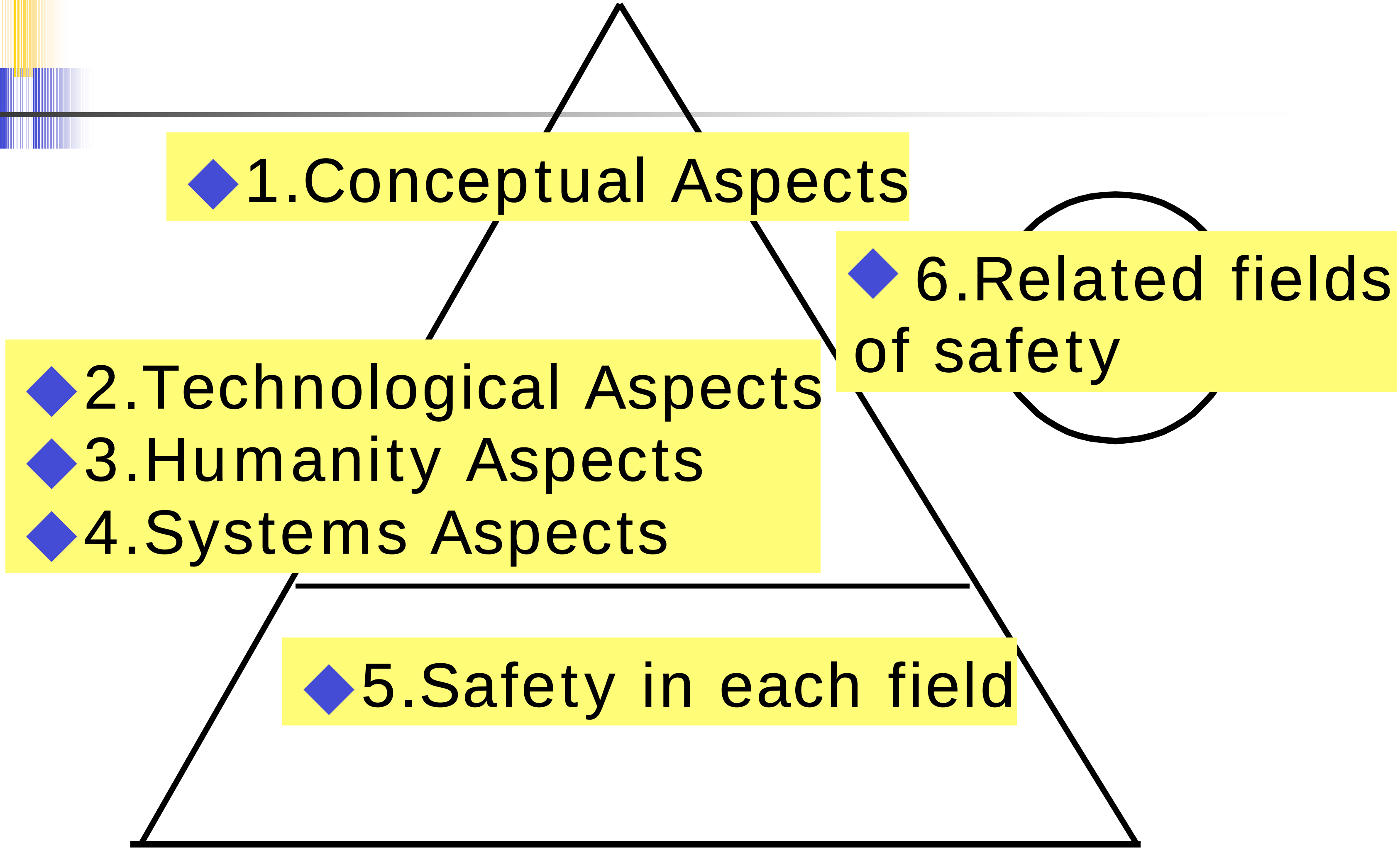
- Attempt to construct **Map on Safety**: systematizes the safety concepts and safety technologies

- **Safety standard** of machinery in Japan with international safety standards.

Map on Safety or Safety Mandala

- An attempt toward establishing a new overall discipline on safety (“safenology”?) by unifying safety engineering and safety science with social and humanity sciences.
- For the first step, list up many key words concerning or related to safety and cluster them into categories of hierarchal levels

◆Map on Safety



◆1.Conceptual Aspects

◆2.Technological Aspects
◆3.Humanity Aspects
◆4.Systems Aspects

◆5.Safety in each field

◆ 6.Related fields of safety

Conceptual Aspects

- **What is safety?**: Definitions of safety, risk, tolerable risk, --
- **A sense of values in safety**: Responsibility, safety versus cost/efficiency/ ethics, safety culture,--
- **Humanity in safety**: Mistakes, habit, human's reliability,--
- **Structure of safety**:

  Defend what, from what, how, under what name ?

Technological Aspects

- evaluation,
- prevention
- maintenance
- damage reduction
- inherent safety design
- fault tolerance
- fail safe
- fail soft
- fool proof

Humanity Aspects

- Human machine interface
- Miss uses
- Ergonomics
- Education
- Peace in mind

Systems Aspects

- Management
- Assessment
- Standardization
- Regulation and norm
- Certification

Safety in each field

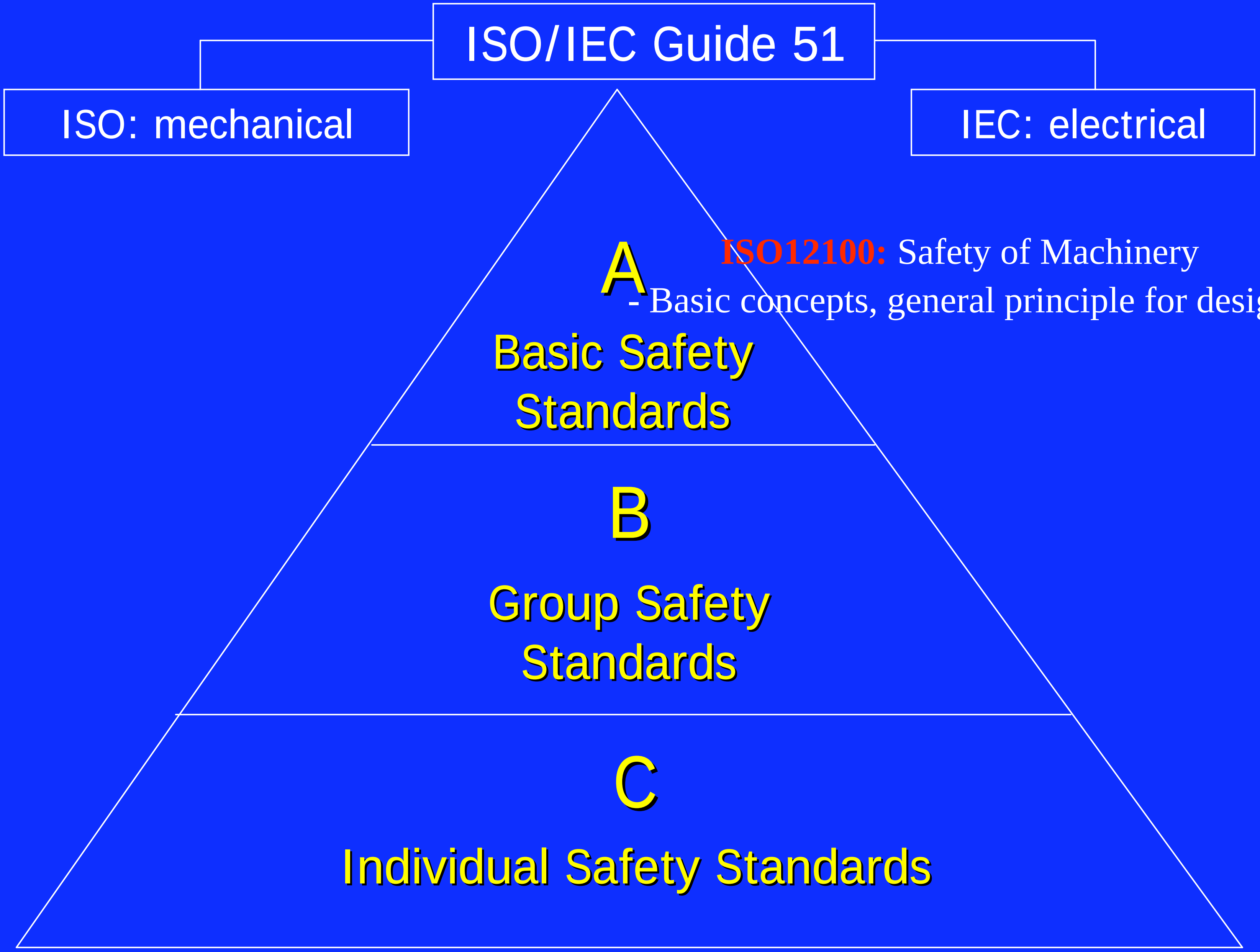
- Machine safety
- Nuclear power safety
- Traffic safety
- Chemical safety
- Product safety
- Food safety
- Material safety
-

Related fields of safety

- Crisis management
- Security
- Insurance
- Court systems
- Law
-

Recent activities in standardisation on safety of machinery in Japan

- **1989** (Europe) EC Machine directives
- **1990** (International) ISO/IEC guide 51: Safety Aspects - Guidelines for their inclusion in standards
- **1991** (Europe) EN292: Safety of Machinery - (International) ISO/TC199: Safety of Machinery
- **1992** (International) ISO/TR12100: Safety of Machinery - Basic concepts, general principle for design
- **1995** (Japan) Declaration to harmonize JIS (Japan Industrial Standard) with ISO, IEC within 5 years, under TBT (Technical Barriers to Trade) agreement
- **1998** (Japan) TR B 0008, 0009 (corresponding to ISO/TR12100)
- **2001** (Japan) Guideline for comprehensive safety norm on Machinery (corresponding to ISO/TR12100) into effect by Ministry of Labour, Health and Welfare
- **2003** (International) ISO12100: Safety of Machinery - Basic concepts, general principle for design
- **2004** (Japan) JS B 9700 (corresponding to ISO12100) will be published



ISO/IEC Guide 51

ISO: mechanical

IEC: electrical

A

Basic Safety Standards

ISO12100: Safety of Machinery

- Basic concepts, general principle for design

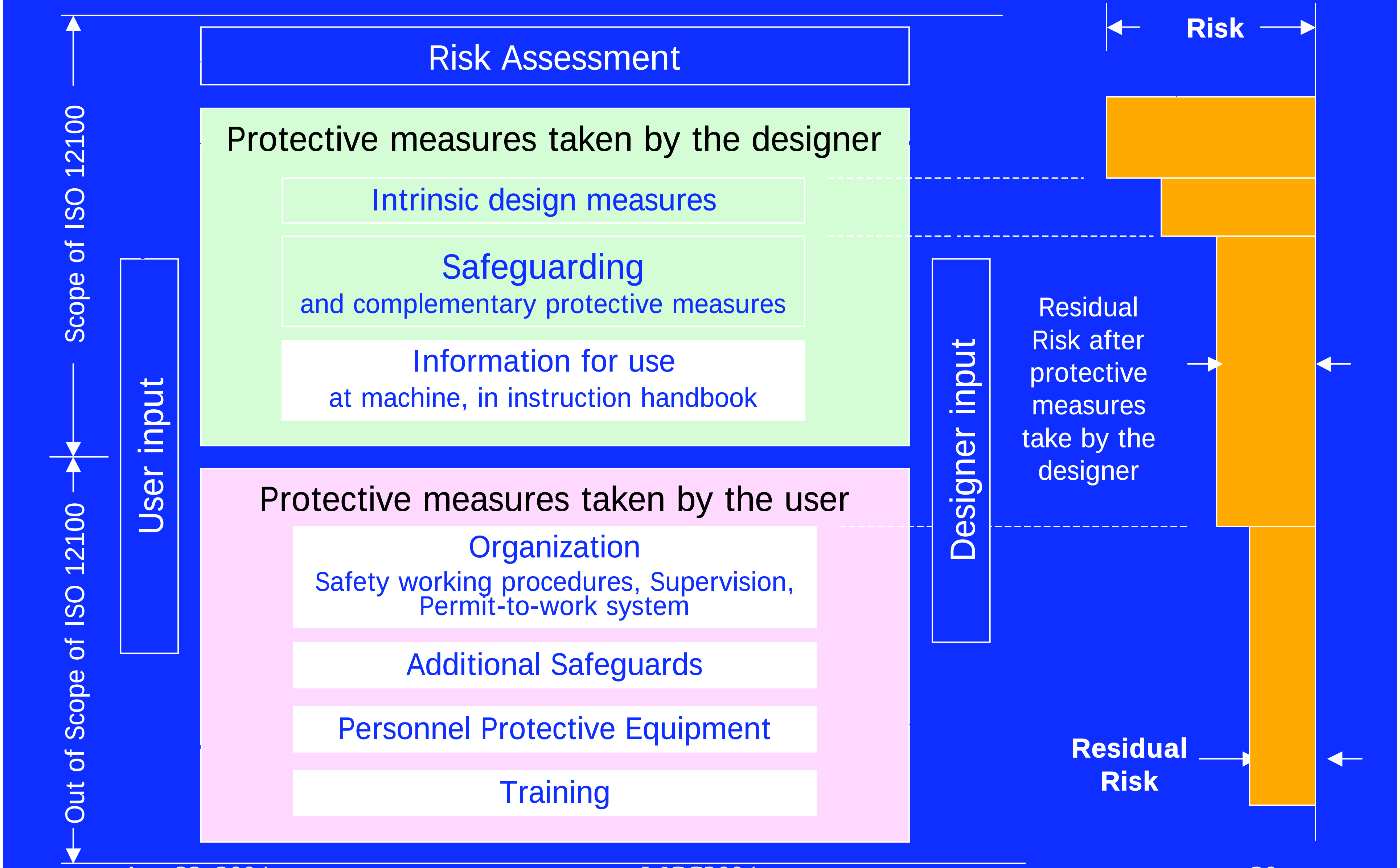
B

Group Safety Standards

C

Individual Safety Standards

Risk reduction process from the point of view of the designer



Scope of ISO 12100

Out of Scope of ISO 12100

User input

Risk Assessment

Protective measures taken by the designer

Intrinsic design measures

Safeguarding
and complementary protective measures

Information for use
at machine, in instruction handbook

Protective measures taken by the user

Organization
Safety working procedures, Supervision,
Permit-to-work system

Additional Safeguards

Personnel Protective Equipment

Training

Designer input

Risk
Residual Risk after protective measures take by the designer
Residual Risk

Source: ISO DIS 12100-1

We can extend the concept of dependability into many other worlds

Application fields of

Modern Dependable Computing(Reliability, Maintainability, Safety, Evaluation, --------)

- From online real time control systems (Chemical process, Manufacture, Aerospace,etc.) To business information systems (Financial, data communications, etc.)
- From (Traditional) computing and structural systems To (New) social and human systems such as organizations and inspections.
- Dependability has potentially huge application fields in the real world.

- Logic (binary) expression
  - Binary variables to instances of predicates

$$\begin{array}{ccccccc} \{idle(A), & idle(B), & dialtone(A), & dialtone(B), & busytone(A), & \cdots, & talk(B,B)\} \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & ,\cdots, & \updownarrow \\ b_1 & b_2 & b_3 & b_4 & b_5 & ,\cdots, & b_{14} \end{array}$$

$$s\ \{dialtone(A), dialtone(B)\} = (00110\cdots0) \leftrightarrow b_3 b_4$$

  - state transition:

$$T_r(s,s') = \prod_{p_i \in Pre[r]} b_i \wedge \prod_{p_i \in Pre[r]} \neg b_i \wedge \quad \text{(activation of a rule at } s\text{)}$$

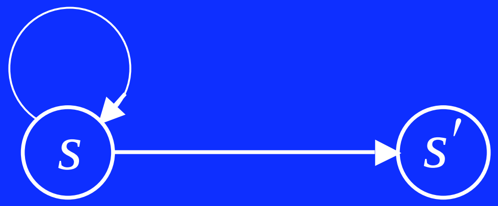
$$\prod_{p_i \in Post[r] \setminus Pre[r]} b'_i \wedge \prod_{p_i \in Pre[r] \setminus Post[r]} \neg b'_i \wedge \quad \text{(new variables)}$$

$$\prod_{p_i \in P \setminus (Post[r] \setminus Pre[r] \cup Pre[r] \setminus Post[r])} (b_i \leftrightarrow b'_i) \quad \text{(unchanged variables)}$$

- Extension

$$D_r(s,s') = T_r(s,s') \vee \prod_{p_i \in P} (b_i \leftrightarrow b_i')$$

$D_r(s,s') = 1$ when s changes to a truly new s' or s remains unchanged. $(s = s')$



– Reachability

$$
\begin{aligned}
& I(s_0) \\
& \wedge D_{r_1}(s_0, s_1) \wedge D_{r_2}(s_1, s_2) \wedge \cdots \wedge D_{r_n}(s_{n-1}, s_n) \\
& \wedge D_{r_1}(s_n, s_{n+1}) \wedge D_{r_2}(s_{n+1}, s_{n+2}) \wedge \cdots \wedge D_{r_n}(s_{2n-1}, s_{2n}) \\
& \vdots \\
& \wedge D_{r_1}\left(s_{(k-1)n}, s_{(k-1)n+1}\right) \wedge D_{r_2}\left(s_{(k-1)n+1}, s_{(k-1)n+2}\right) \wedge \cdots \wedge D_{r_n}(s_{kn-1}, s_{kn}) \\
& \wedge f_G(s_{kn})
\end{aligned}
$$

$I(s_0) = 1$ iff s_0 is the initial state.

$f_G(s) = 1$ iff s satisfies condition G.

The most critical application : **safety systems**

Safety has a strong relation with reliability but is fundamentally different concept from reliability

- “Reliability” targets to maintain the given functions
- “Safety” targets to avoid dangerous situations in which a sense of values of related person or current society is concerned.

Why
the Map on Safety

- Toward to establish a new overall discipline on safety
- Proposing to unify safety engineering and safety science with social science and humanity science
- Listing up many key words concerning or related to safety
- Clustering them into few categories which consist of hierarchal construction from concepts of safety to individual fields of safety.

Why
the Map on Safety(cont'd)

- The author believes that we have to start to construct the map on safety* for establishing a new overall discipline on safety including social science and humanity science with safety engineering and safety science

*This map is unfinished and constructioning now.

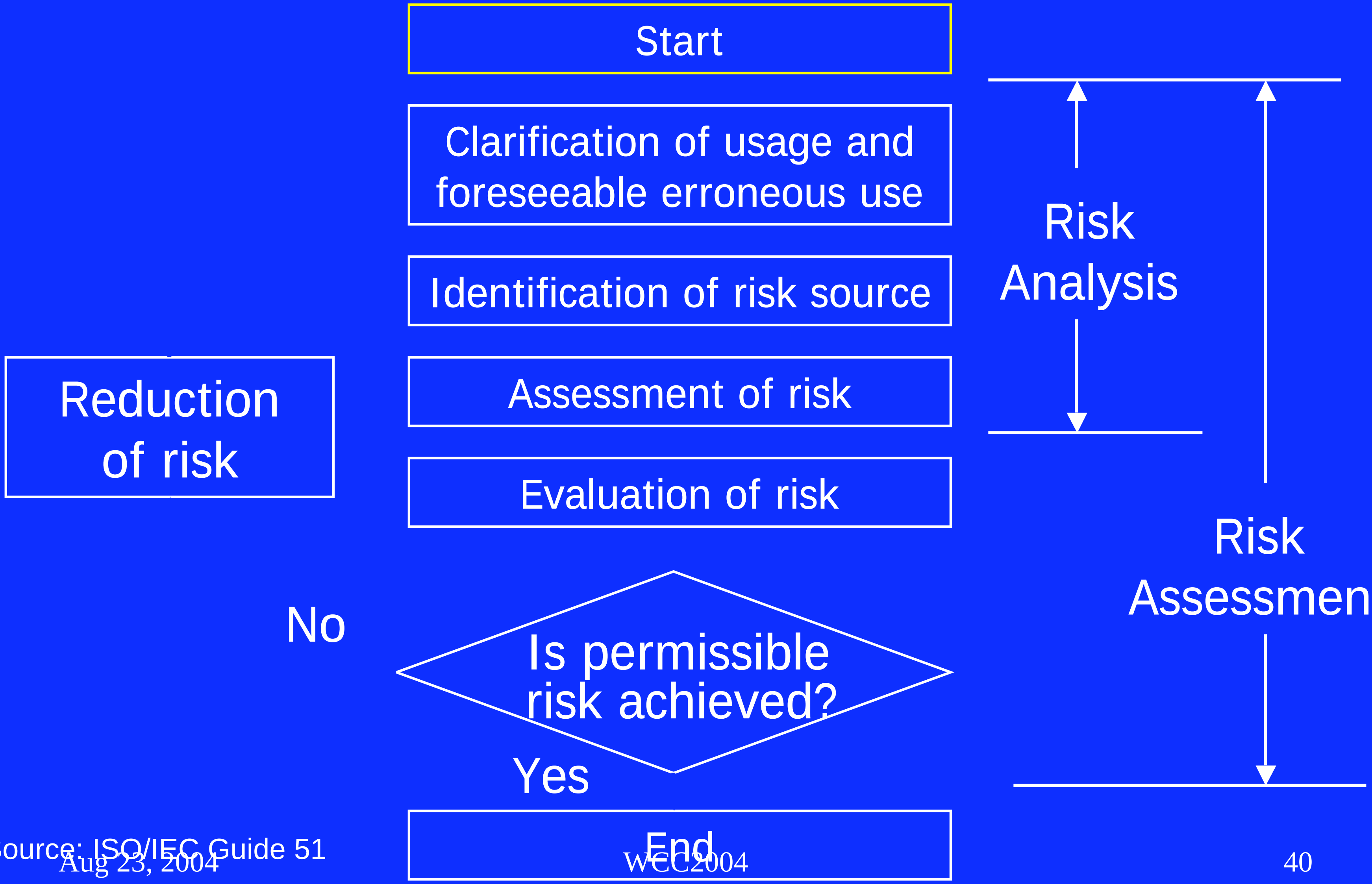
*At first I called this map as safety map, but I prefer rather to call it as safety mandala, where mandala is a word in Buddhism meaning a map illustrating the construction of conceptual essences.

（1） What is safety？

- Definition of safety
- What is risk?
- What is tolerable risk?
- Deterministic safety and probabilistic safety
- Absolutely safe?
- fail safe ?
- What is hazards?
- What is danger?

- Relation on safety and probability
- Relation on safety and reliability
- Relation on safety and security
- Relations on accident, disaster, incident, misfortune,---
- Relations on fault, failure, defect, ---

Procedure of Risk Assessment


Start
Clarification of usage and foreseeable erroneous use
Identification of risk source
Assessment of risk
Evaluation of risk
Is permissible risk achieved?
Yes
End
No
Reduction of risk
Risk Analysis
Risk Assessment

Source: ISO/IEC Guide 51