HITACHI
Inspire the Next

Research Report
– My Recent Events and Activity on IEC 61508

2011/07/04

Nobuyasu Kanekawa
Hitachi Research Laboratory,
Hitachi, Ltd.

HRL Hitachi Research Laboratory

HITACHI
Inspire the Next

Contents

1. New Book Published
2. Earthquake on 11 Mar., 2011
   Absence from IFIP TC. 10. Meeting
3. IEC 61508 Ed. 2.0 Issued

HRL Hitachi Research Laboratory

HITACHI
Inspire the Next

Contents

1. New Book Published
2. Earthquake on 11 Mar., 2011
   Absence from IFIP TC. 10. Meeting
3. IEC 61508 Ed. 2.0 Issued

HRL Hitachi Research Laboratory

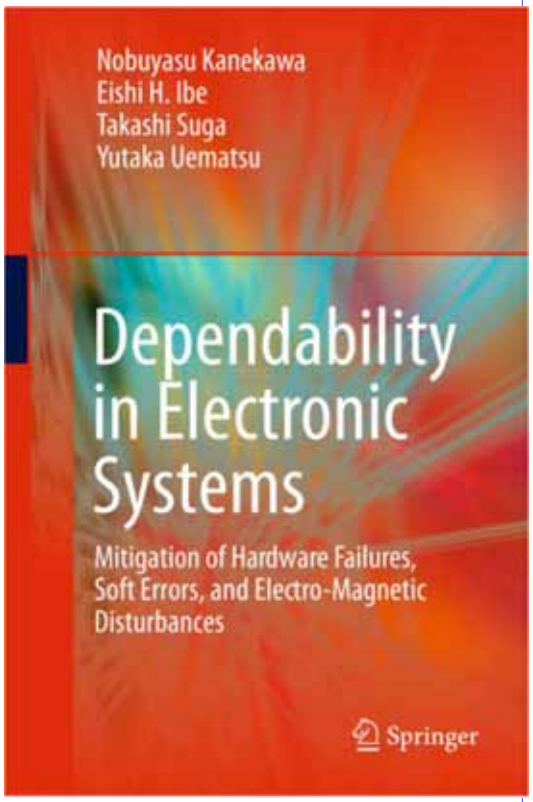
New Book Published

HITACHI
Inspire the Next

Contents

1. Introduction
2. Terrestrial Neutron-Induced Failures
   Semiconductor Devices and Relevant Systems and Their Mitigation Techniques
3. Electromagnetic Compatibility
4. Power Integrity Design
5. Fault-Tolerant System Technology

Presented yesterday.



ISBN 978-1-4419-6714-5

HITACHI
Inspire the Next

Contents

1. New Book Published
2. Earthquake on 11 Mar., 2011
   Absence from IFIP TC. 10. Meeting
3. IEC 61508 Ed. 2.0 Issued

HRL Hitachi Research Laboratory

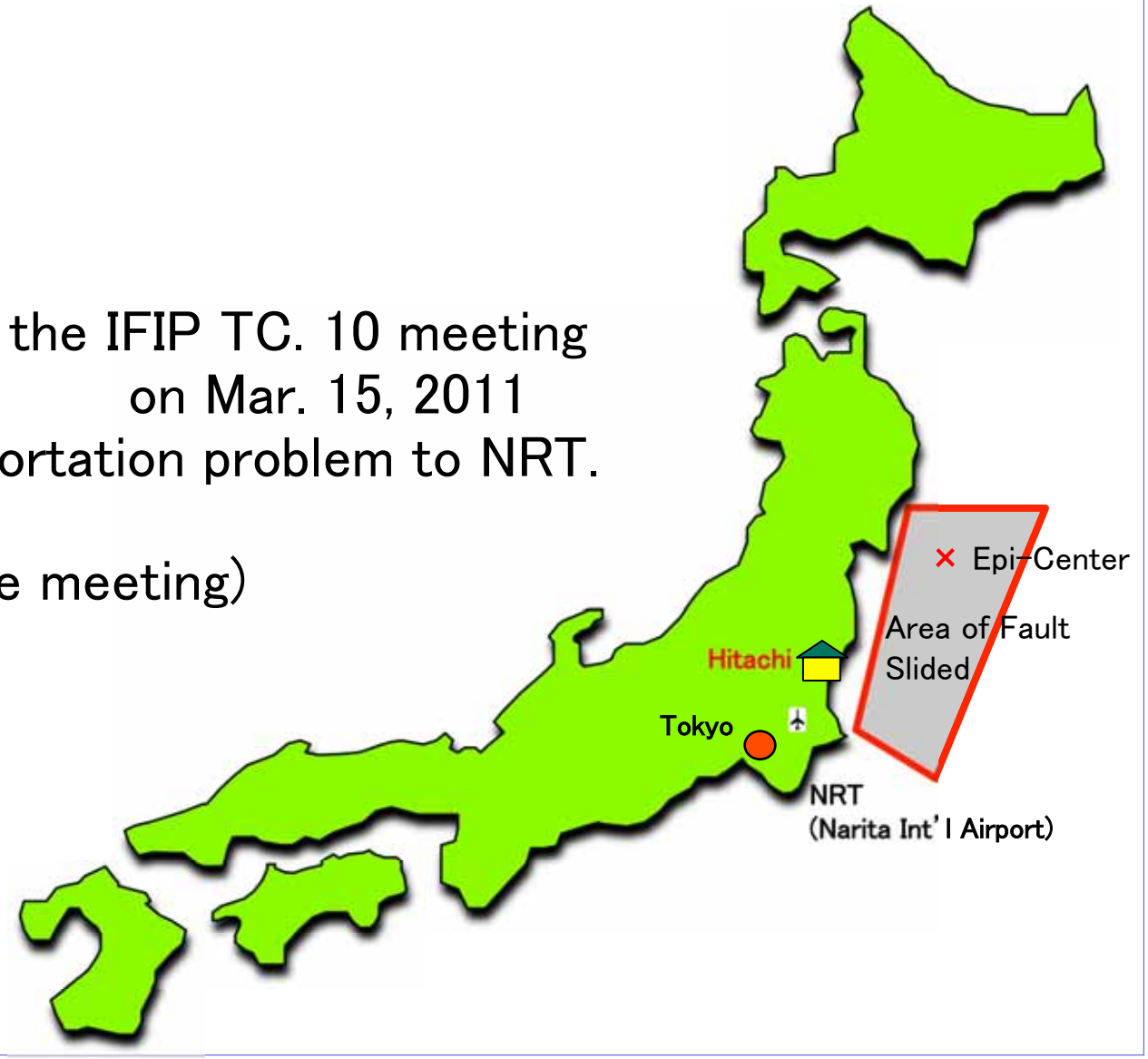
Earthquake on Mar. 11, 2011

HITACHI
Inspire the Next

- I have survived.

- But ...
  I could not attend the IFIP TC. 10 meeting
  on Mar. 15, 2011
  because of transportation problem to NRT.

- (Rick attended the meeting)



HITACHI
Inspire the Next

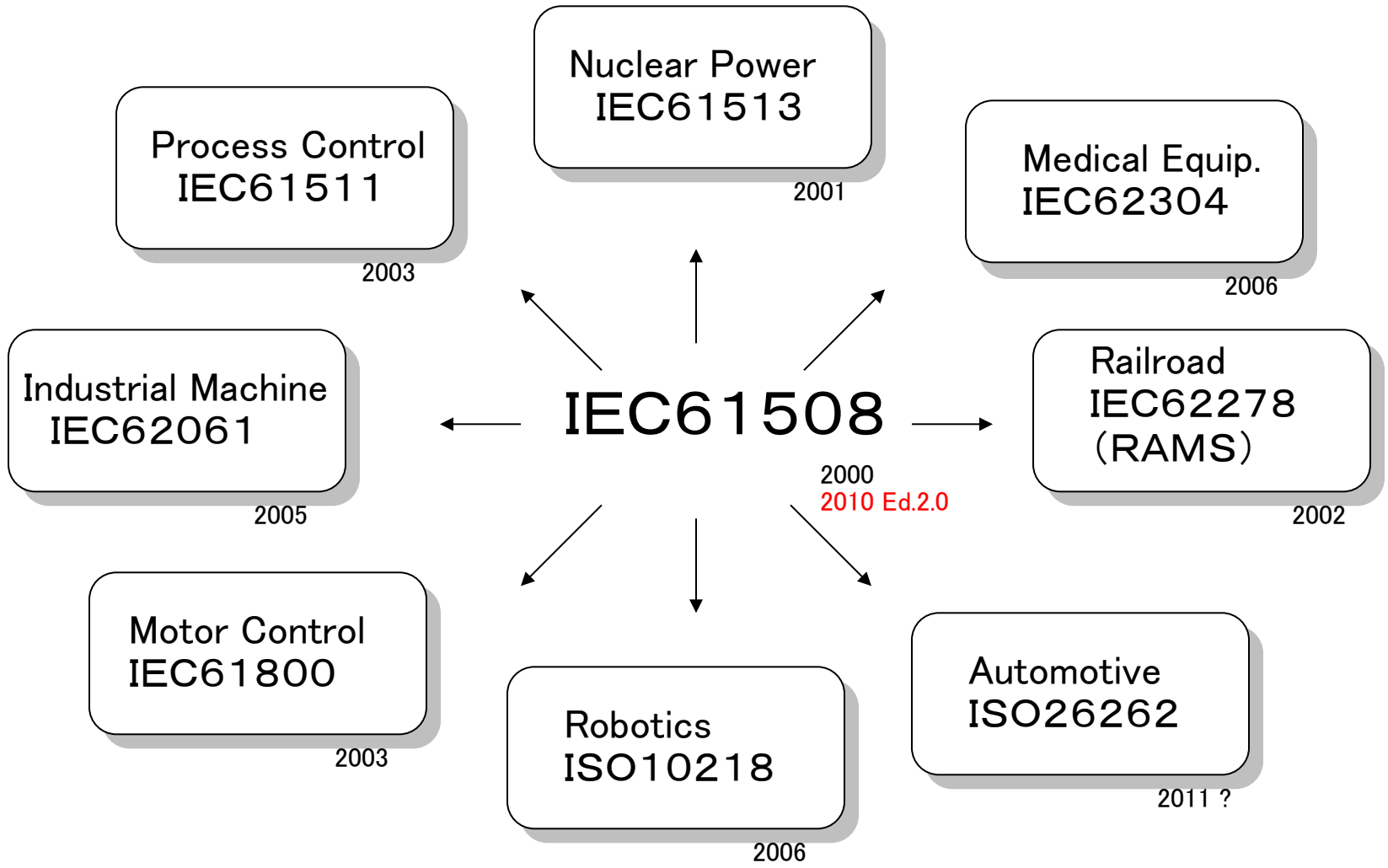
Contents

1. New Book Published
2. Earthquake on 11 Mar., 2011
   Absence from IFIP TC. 10. Meeting
3. IEC 61508 Ed. 2.0 Issued

HRL Hitachi Research Laboratory

Functional Safety Standards

HITACHI
Inspire the Next



SIL (Safety Integrity Level)

HITACHI
Inspire the Next

(a) low demand mode of operation

Safety Integrity Level (SIL)	Average probability of a dangerous failure on demand of the safety function
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

(b) high demand mode of operation or continuous mode of operation

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}]
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

IEC 61508 Ed. 2.0 Interpretation

HITACHI
Inspire the Next

(0) Interpretation on β_{IC} in IEC61508 Ed. 2.0 Part 2 Annex E
(Special Requirements for ICs with On-Chip Redundancy)

Initial Value: β_{B-IC}=33%
→ add according to Table E.1
→ subtract according to Table E.2
→ if β_{IC} < 25% then SIL 3

Annex D:
β_{IC}: Ratio of undetectable failures by CCF (Common Cause Failure)

$$\lambda_{D-CCF} = \beta_{IC} \cdot \lambda \qquad (1)$$

where,
λ_{D-CCF} : Failure rate of undetectable failures by CCF,
λ : Failure rate of the item.

Interpretation

Failure rate of the Chip λ = 400 [fit]

Dangerous failure rate for SIL 3 λ_{D-CCF} < 10^{-7}[hr.$^{-1}$]

→ β_{IC} < 0.25 according to eq. (1)

Proposals for IEC 61508 Ed. 3.0

HITACHI
Inspire the Next

(1) Upper bound of β_{IC}

Failure rate of the Chip λ is not always be 400 [fit]

Failure rate of the Chip λ = 200 [fit]
Dangerous failure rate for SIL 3 $\lambda_{D-CCF} < 10^{-7}[hr.^{-1}]$ ⟶ $\beta_{IC} < 0.5$

Failure rate of the Chip λ < 100 [fit]
Dangerous failure rate for SIL 3 $\lambda_{D-CCF} < 10^{-7}[hr.^{-1}]$ ⟶ $\beta_{IC} = 1.0$

⋮

proposal

Upper bound of β_{IC} shall be determined according to failure rate of the Chip λ ?

Proposals for IEC 61508 Ed. 3.0

HITACHI
Inspire the Next

(2) Others

Ed. 2.0 Part 2 Annex E mainly lists
Physical Protection Countermeasures (Signal Net Separation, Power Supply/GND Separation, etc.)
to guarantee Independence of Redundant Channels in a Chip.

Logical, Code-Theoretical Countermeasures (Redundant Codes, Alternative Codes, Specially Modulated Signals, etc.) should be added.

Many things to be improved.


HITACHI
Inspire the Next