SICE Annual Conference 2007
Sept. 17-20, 2007, Kagawa University, Japan

Throwing a Bridge between Risk Assessment and Functional Safety

Yoshinobu Sato

Faculty of Marine Technology
Tokyo University of Marine Science and Technology, Tokyo, Japan
(Telephone : +81-3-5245-7421; E-mail: yoshi@kaiyodai.ac.jp)

Abstract: Risk assessment must be established for reasonable operation of functional safety. So far, the relationships between the risk frequency, i.e., hazardous event rate, and the safety integrity of safety-related systems have not been clear for the general demand modes of operation. Then, the present paper describes the new formulations of hazardous event rate (*HER*) as well as the risk reduction ratio (*RRR*) for the general demand modes of operation, and proposes the method how to determine safety integrity levels of SRS using *HER*, *RRR*, Table 2 and 3 in the standard of IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.

Keywords: Functional safety, Risk assessment, Safety integrity, Safety integrity level, Hazardous event rate.

1. INTRODUCTION

An electrical/electronic/programmable electronic safety-related system (**SRS**) is assumed to implement a safety function(s) in order to reduce and/or mitigate a risk(s) of harm in an overall system [1]. Safety integrity level (**SIL**) to be allocated to SRS is determined by taking account of both random hardware failures and demands on a safety function(s) of SRS to prevent a hazardous event(s) from occurring. Then, it is necessary to estimate the risk frequency, i.e., ***hazardous event rate*** for reasonable determination of SIL(s) to be achieved by SRS.

In order to estimate the ***hazardous event rate***, it is important that mathematical models should be established for formulation of the relationships between the failures and the demands. Fault-tree and Markov as well as Event-tree techniques would be very useful for such formulation. Usually an SRS has a complex architecture for functional redundancy involving common cause factors.

However, here, one of the simplest systems, in which an SRS with a constant failure rate implements a safety function and no other protection layer than that SRS exists, is taken for modeling of the relationships between the failures of SRS and the demand put on the SRS, then the ***hazardous event rate*** is formulated by use of Markov techniques [2].

2. TWO HAZARDOUS EVENT LOGICS

At first, there are two logics of occurrence of hazardous event, given that the failures of SRS and the demands on the safety function of SRS are mutually-statistically independent. In Fig. 1, the two logics are described by use of fault trees with priority AND-gates, i.e., sequential failure logics [3]. The logics are:

a) - A hazardous event occurs when the SRS is in a fault (i.e., a failed-state, see Fig. 2) and a demand arises in the overall system (namely, failure-first and demand-later logic), and

b) - A hazardous event occurs when the overall system is in a demand state and the SRS fails its safety function (i.e., demand-first and failure-later logic).

Here, the fault, dangerous failure and recovery (or restoration) are defined as the state of SRS where its safety function(s) can not be implemented, the start of the fault and the termination of the fault, respectively. Similarly the demand state, demand and completion are the state where the implementation of safety function is continuously required, the start of demand state and the termination of the demand stated, respectively.

The statistical parameters regarding to demands and failures of SRS are modeled as shown in Fig. 2 and they are defined as follows [4]:

Constant dangerous (fail-to-dangerous) failure rate λ_D [1/hour]: probability that a dangerous (fail-to-dangerous) failure occurs per unit time at time t, given it is not in a fault at time t, i.e., $1/\lambda_D$ is the mean time between a restoration and the next failure in Fig. 2,

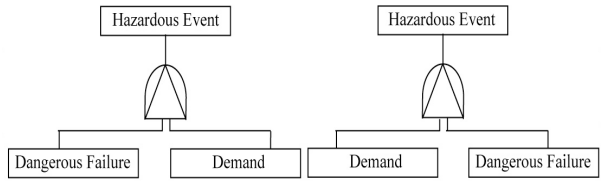
Constant restoration (repair) rate μ_D ($=2/T$ [1/hour], if dangerous failures are undetected by self-diagnoses and if the dangerous-undetected failure is completely restored at each proof test of interval T and the maintenance time is negligible comparing to the proof test interval [5]): probability that a restoration (a recovery) occurs per unit time at time t, given it is in a fault at time t, i.e., $1/\mu_D$ is the mean time between a failure and the restoration (see Fig. 2),

Constant demand rate λ_M [1/hour]: probability that a demand occurs per unit time at time t, given it is not in a demand state at time t, i.e., $1/\lambda_M$ is the mean time between a completion and the next demand (see Fig. 2), and

Constant completion rate μ_M [1/hour]: probability that a completion occurs per unit time at time t, given it is in

PR0001/07/0000-2484 ¥400 © 2007 SICE
Authorized licensed use limited to: Fachhochschule FH Offenburg. Downloaded on May 31, 2009 at 13:46 from IEEE Xplore. Restrictions apply.

a demand state at time *t*, i.e., $1/\mu_M$ is the mean time between a demand and the next completion (see Fig. 2).



a) Fault and demand **b)** Demand state and failure

Fig. 1 Two hazardous event logics

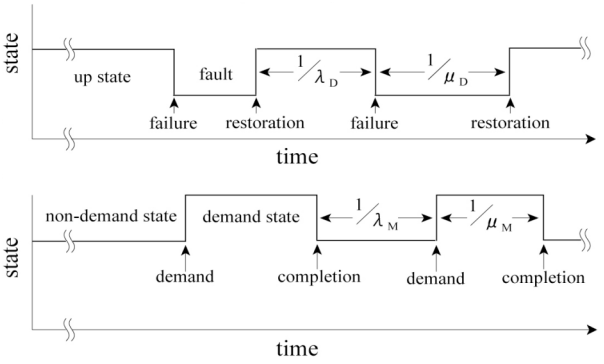


Fig. 2 Modeling of statistical parameters

3. SYSTEM WITHOUT COMMON CAUSE BETWEEN DEMANDS AND FAILURES

Figure 3 is a Markov model equivalent to Fig 1, which describes the relationships between demand rate λ_M, completion rate μ_M, dangerous (i.e., fail-to-dangerous) failure rate λ_D, and restoration (repair) rate μ_D, given that demands and failures of SRS occur statistically-independently [5], [6].

The states of the figure are:

(0, 0); the initial state where SRS is normal and the overall system is not in any demand state,

(1, 0); SRS is in a fault and the overall system is not in any demand state,

(0, 1); SRS is normal and the overall system is in a demand state where implementation of the safety function is required, and

(1, 1); the final absorption state where the overall system is in harm and is not recovered.

The harm is the state in which the overall system is fatally damaged and a hazardous event is the start of harm according to the figure.

In Fig. 3 the state transitions from ***(0, 0)*** to ***(1, 0)*** and from ***(0, 1)*** to ***(1, 1)*** are dangerous failures of SRS. Similarly, the state transitions from ***(0, 0)*** to ***(0, 1)*** and from ***(1, 0)*** to ***(1, 1)*** are demands. Moreover, the state transitions from ***(1, 0)*** to ***(0, 0)*** and from ***(0, 1)*** to ***(0, 0)*** are a restoration and a completion, respectively.

The state transitions from ***(1, 0)*** to ***(1, 1)*** and from ***(0, 1)*** to ***(1, 1)*** materialize the failure-first and demand-later logic, as well as the demand-first and failure-later logic, respectively.

According to Fig. 3, ***hazardous event rate***, ω*, is defined as

$$\omega^* = 1/(\textbf{\textit{average absorption time}}) \text{ [1/hour]}. \quad (1)$$

The ***average absorption time*** is the statistically expected time until the initial state ***(0, 0)*** reaches the final absorption state ***(1, 1)***, i.e. the harm.

On the other hand, Fig. 4 describes the Markov model where the renewal transition from state ***(1, 1)*** to state ***(0, 0)*** takes place instantaneously. In the figure, ***hazardous event rate***, ω**, in its steady state, is defined as [6]

$$\omega^{**} = \lambda_M \, Pr(1, 0) + \lambda_D \, Pr(0, 1) \text{ [1/hour]}, \quad (2)$$

where *Pr(x, y)* is the probability that the overall system is in state ***(x, y)***.

Then, in general,

$$\omega^* = \omega^{**} (= \omega) \quad (3)$$

becomes true [6].

Moreover, **risk reduction ratio**, ***RRR***, achieved by SRS is defined as

$$RRR = \omega^*/\lambda_M = \omega^{**}/\lambda_M = \omega/\lambda_M. \quad (4)$$

3.1 SRS with self-diagnosis functions

When SRS has self-diagnosis functions that can detect all dangerous failures in the SRS and alarm maintenance personnel to repair the malfunction, then the dangerous failures become dangerous detected-failures (DD failures) of which rate is defined as DD failure rate, λ_{DD}.

Here, it is assumed that the restoration made by the maintenance personnel follows an exponential distribution with a constant restoration (repair) rate, μ_D.

Then, simultaneous equations are obtained from Fig. 4 in order to estimate ***hazardous event rate***, ω (=ω*=ω**), which results in the following formulations:

(1) If $\lambda_{DD} << \lambda_M + \mu_{DD}$ and $\lambda_{DD} << \mu_M$, then ω (=ω*=ω**) and ***RRR*** are given as [6]

$$\omega \cong (1-Q_M)\lambda_{DD}\omega_M / \{(1-Q_M)\mu_{DD} + \omega_M\} + Q_M \lambda_{DD} \text{ [1/hour]}, \quad (5)$$

$$RRR \cong (1-Q_M)^2 \lambda_{DD} / \{(1-Q_M)\mu_{DD} + \omega_M\} + \lambda_{DD}/(\lambda_M + \mu_M). \quad (6)$$

Here, $Q_M = \lambda_M/(\lambda_M+\mu_M)$, and $\omega_M = \lambda_M\mu_M/(\lambda_M+\mu_M)$ [3].

(2) Moreover, if $\lambda_M << \mu_{DD}$ and $\lambda_M << \mu_M$ (i.e., low demand rate and short demand duration mode of operation), Eq. (5) and (6) give

Authorized licensed use limited to: Fachhochschule FH Offenburg. Downloaded on May 31, 2009 at 13:46 from IEEE Xplore. Restrictions apply.

$$\omega \cong \lambda_{DD}\lambda_M/\mu_{DD} \text{ [1/hour]}, \quad (7)$$

$$\boldsymbol{RRR} \cong \lambda_{DD}/\mu_{DD}. \quad (8)$$

(3) Then, if $\mu_{DD} << \omega_M$ (high demand frequency mode of operation) or $\mu_M << \lambda_M$ (continuous mode of operation), similarly

$$\omega \cong \lambda \text{ [1/hour]}, \quad (9)$$

$$\boldsymbol{RRR} \cong \lambda_D/\lambda_M. \quad (10)$$

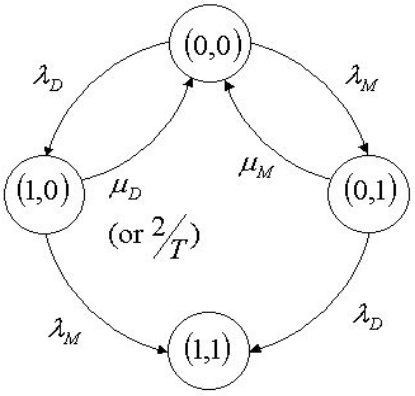


Fig. 3 Markov model with an absorbing state

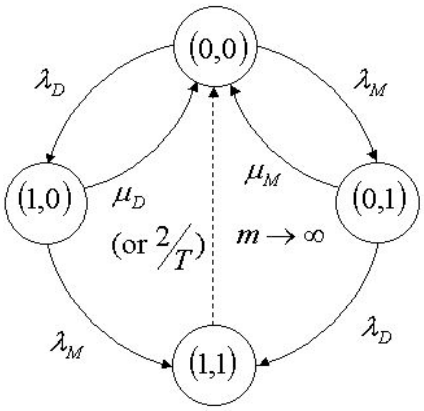


Fig. 4 Markov model with instantaneous renewal

The ***RRR*** of Eq. (8), λ_{DD}/μ_{DD}, and the ***hazardous-event rate*** of Eq. (9), λ_{DD}, are called as the *probability failure on demand* (***PFD***) and the *probability of failure per hour* (***PFH***), and refer to Table 2 and 3 in IEC 61508-1 [1], respectively.

As shown above, quantities, ***PFD*** and ***PFH***, have its own validity in the special domains of demand rate and / or completion rate only. Namely, it is now difficult to say that ***hazardous-event rate***, ω, is equal to ***PFH***, as well as ***RRR*** is ***PFD*** throughout the general domains of demand and completion rates.

Thus, naming of ***PFD*** and ***PFH*** should be changed generally into ***RRR*** and ***hazardous-event rate***, respectively. Here, it should be also reminded that which tables should be applied to the general domains of demand and completion rates is still not clear.

3.2 SRS without self-diagnosis functions

When SRS has no self-diagnosis functions, the dangerous failures become dangerous undetected-failures (DU failures) of which failure rate is defined as DD-failure rate, λ_{DU}.

DU failures must be detected and repaired by maintenance personnel at a proof test that is implemented periodically.

Here, it is assumed DD failures are completely restored at each proof test of interval T and the time necessary for the maintenance is negligible comparing to the proof-test interval. Thus, since the mean down time of SRS between two proof tests is $T/2$ it is assumed that the restoration made by the maintenance personnel follows approximately an exponential distribution with the constant restoration (repair) rate of $2/T$ [5], [7].

In general, there are two types of implementation of the proof test. Namely, one is the proof test being practiced under the situation where equipment under control (EUC) that is the source of hazards in the overall system is stopped in order to prevent any demand from arising. The other is that practiced under the situation where EUC is in operation, given that some bypassing is taken instead of the safety function of SRS during its proof testing.

The main difference between two types of implementation of the proof test is: although the state transition model described in Fig. 4 gives simultaneous equations for the estimation of constant ω for the latter type, the former type requires simultaneous differential equations for the estimation of variable, $\omega(t)$, and time-average hazardous event rate, ω, is obtained by calculating the time-average of $\omega(t)$ during two proof tests.

Thus, analyses of hazardous event rate for the two types give the results shown in Section (1) (a)~(f) and (2) (a)~(f) as follows [8], [9]:

(1) Proof-test by making EUC stationary

(a) Low occurrence & short duration mode:
($\lambda_M << 1/T$ *and* $\mu_{DU} >> 1/T$)

$$\omega \cong 0.5\lambda_{DU}\lambda_M T \qquad \boldsymbol{RRR} \cong 0.5\lambda_{DU}T$$

The above ***RRR*** is called as the *probability failure on demand* (***PFD***) and shall be refer to Table 2 in IEC 61508-1.

(b) Low occurrence & intermediate duration mode:
($\lambda_M << 1/T$ *and* $\mu_{DU} \cong 1/T$)

Authorized licensed use limited to: Fachhochschule FH Offenburg. Downloaded on May 31, 2009 at 13:46 from IEEE Xplore. Restrictions apply.

$\omega \cong 0.87\lambda_{DU}\lambda_M T$ $\quad$ $\boldsymbol{RRR} \cong 0.87\lambda_{DU} T$

(c) Low occurrence & long duration mode: ($\lambda_M << 1/T$ *and* $\mu_{DU} << 1/T$)

$\omega \cong \lambda_{DU}\lambda_M T$ $\quad$ $\boldsymbol{RRR} \cong \lambda_{DU} T$

(d) Intermediate occurrence & short duration mode: ($\lambda_M \cong 1/T$ *and* $\mu_{DU} >> 1/T$)

$\omega \cong 0.37\lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong 0.37\lambda_{DU}/\lambda_M$

(e) Intermediate occurrence & duration mode ($\lambda_M \cong \mu_{DU} \cong 1/T$)

$\omega \cong 0.57\lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong 0.57\lambda_{DU}/\lambda_M$

(f) Intermediate occurrence & long duration ($\lambda_M \cong 1/T$ *and* $\mu_{DU} << 1/T$), high occurrence & short duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} >> 1/T$), high occurrence & intermediate duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} \cong 1/T$), or high occurrence & long duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} << 1/T$) modes:

$\omega \cong \lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong \lambda_{DU}/\lambda_M$

The above $\omega \cong \lambda_{DU}$ is called as the *probability of failure per hour* (***PFH***) and shall be referred to Table 3 in IEC 61508-1.

(2) Proof-test by remaining EUC operating

(a) Low occurrence & short duration mode: ($\lambda_M << 1/T$ *and* $\mu_{DU} >> 1/T$)

$\omega \cong 0.5\lambda_{DU}\lambda_M T$ $\quad$ $\boldsymbol{RRR} \cong 0.5\lambda_{DU} T$

The above ***RRR*** is called as the *probability failure on demand* (***PFD***) and shall be refer to Table 2 in IEC 61508-1.

(b) Low occurrence & intermediate duration mode: ($\lambda_M << 1/T$ *and* $\mu_{DU} \cong 1/T$)

$\omega \cong 1.5\lambda_{DU}\lambda_M T$ $\quad$ $\boldsymbol{RRR} \cong 1.5\lambda_{DU} T$

(c) Low occurrence & long duration mode: ($\lambda_M << 1/T$ *and* $\mu_{DU} << 1/T$)

$\omega \cong Q_M\lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong \lambda_{DU}/(\lambda_M + \mu_{DU})$

(d) Intermediate occurrence & short duration mode: ($\lambda_M \cong 1/T$ *and* $\mu_{DU} >> 1/T$)

$\omega \cong 0.37\lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong 0.37\lambda_{DU} T$

(e) Intermediate occurrence & duration mode: ($\lambda_M \cong \mu_{DU} \cong 1/T$)

$\omega \cong 0.68\lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong 0.68\lambda_{DU} T$

(f) Intermediate occurrence & long duration ($\lambda_M \cong 1/T$ *and* $\mu_{DU} << 1/T$), high occurrence & short duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} >> 1/T$), high occurrence & intermediate duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} \cong 1/T$), or high occurrence & long duration ($\lambda_M >> 1/T$ *and* $\mu_{DU} << 1/T$) modes:

$\omega \cong \lambda_{DU}$ $\quad$ $\boldsymbol{RRR} \cong \lambda_{DU}/\lambda_M$

The above $\omega \cong \lambda_{DU}$ is called as the *probability of failure per hour* (***PFH***) and shall be referred to Table 3 in IEC 61508-1.

4. HOW TO DETERMINE SIL

Currently in the standard, the way how the demand is put on SRS is assumed as either one of the following two situations: **1) Impulse-shaped demand** where although λ_M can be arbitrary values, $1/\mu_M$ is always assumed to be nearly zero, i.e., demand durations are always sufficiently short; or **2) Continuous demand duration** where μ_M is always assumed to be nearly zero, i.e., demand durations are always sufficiently long.

Thus, the current standard does not have the concept of intermediate demand durations where neither μ_M nor $1/\mu_M$ is estimate as null, although the reality requires the intermediate demand durations (see Fig. 2).

In addition, the standard categorizes the demand modes of operation into two modes only: the low demand mode and the high demand/continuous mode. For the former, the target failure measure of SRS is defined as the average probability of failure to perform the design function on demand, i.e., the *probability failure on demand* (***PFD***). For the latter, the target failure measure of SRS is the probability of a dangerous failure per hour, i.e., the *probability of failure per hour* (***PFH***) [1], [10].

Moreover, in accordance with the standard, SIL shall be referred to Table 2 and 3 in IEC 61508-1 for the SRS in a low demand mode of operation and for that in a high demand / continuous mode of operation, respectively [1], [10].

As shown in the precedent sections, it is not necessary clear which Table 2 or 3 in IEC 61508-1 should be applied to the general cases of overall systems where the demand and continuous modes are mixed up together, i.e., to those of intermediate demand durations, and the safety performance of SRS depends not only its failure rate but also such factors as the proof-test interval T, demand rate λ_M, completion rate μ_M as well as the architecture of SRS. Namely, it would be no longer reasonable to pre-determine the table to be chosen for SIL allocation based on the conventional definitions of modes of operation give in the standard.

Authorized licensed use limited to: Fachhochschule FH Offenburg. Downloaded on May 31, 2009 at 13:46 from IEEE Xplore. Restrictions apply.

Then, the following procedure is proposed for the determination of SIL:

1) Both of ***risk reduction ratio***, ***RRR***, and ***hazardous event rate***, **ω**, regarding the safety function should be estimated,

2) Two values of SIL form Table 2 and 3 in IEC 61508-1 are obtained based on the ***RRR*** (refer to Table 2) and **ω** (refer to Table 3), respectively, and

3) The lower value is to be formally allocated as the SIL with the table to the safety function of SRS.

Here, ***RRR*** and **ω**, for the two extremes of low demand rate and short demand duration mode of operation (or low occurrence & short duration mode) as well as of continuous mode of operation (or case (f) in the precedent sections) correspond to ***PFD*** and ***PFH*** of the current standard, respectively.

Thus, this procedure should be a fundamental rule for the determination of SIL.

5. CONCLUSIONS

Risk assessment must be established for reasonable operation of the standard of functional safety. So far, the relationships between the risk frequency, i.e., hazardous event rate, and the safety integrity of SRS have been not clear for the general demand modes of operation.

Then, in the paper, first, two hazardous event logics are established by use of fault trees with priority AND-gates, i.e., sequential failure logics. Next, Markov state-transition diagrams for the hazardous event logics are developed and analyzed in order to estimate risk-reduction made by a safety function of SRS quantitatively. Thus, the relationships between the hazardous event rate and the safety integrity of SRS are formulated for several types of overall systems. Finally, a procedure how to define SIL for a safety function of SRS is proposed to be a formal rule under general situations of overall systems.

The conventional method for evaluation of *PFD* and *PFH* sometimes gives us dangerous and/or unreasonable estimation of risk frequency, i.e., hazardous event rate. The approach described in the present paper will contribute toward solving such problems.

In this paper, only *1-out-1* systems architecture is taken for SRS, since it is assumed that the common cause failure rate for redundant channels of SRS is not negligible and rather dominant. However, if small and negligible, then the effect of independent failures of the redundant channels on the risk frequency becomes overriding and therefore must be taken into account for the risk assessment [5]. In addition, the modeling of occurrence of demands here could be applied with a slight error to the overall system where the demands are periodical rather than random [7].

REFERENCES

[1] IEC 61508-1, Functional safety of electrical/ electronic/programmable electronic safety-related systems-Part 1: General requirements, IEC, Geneva, 1998.

[2] IEC 61165, Application of Markov techniques, IEC, Geneva, 2006.

[3] Y. Misumi and Y. Sato, "Estimation of average hazardous-event-frequency for allocation of safety-integrity levels", *Reliability Engineering and System Safety*, Vol. 66, pp.135-144, 1999.

[4] E. Kato and Y. Sato, "Safety integrity levels for IEC 61508 – examination of modes of operation", *IEICE Trans. on Fundamentals*, Vol. E83-A, No. 5, pp. 863-865, 2000.

[5] T. Shimodaira, Y. Sato and K. Suyama, "Estimation of hazardous event rate for repairable *1-out-of-2* safety-related systems based on state transition models", *Trans of the Institute of Electronics, Information and Communication Engineers*, Vol. J88-A, No. 8, pp. 962-973, 2005 (*in Japanese*).

[6] T. Kawahara, A. Ichitsuka and Y. Sato, "State-transition model of safety-related systems with automatic diagnoses and its formulation for functional safety assessment", *Trans of the Institute of Electronics, Information and Communication Engineers*, Vol. J86-A, No. 3, pp. 241-249, 2003 (*in Japanese*).

[7] H. Shimizu, Y. Sato and T. Fukuda, "Evaluation of functional safety of protection devices for electric heaters", *Trans of the Institute of Electronics, Information and Communication Engineers*, Vol. J85-A, No. 12, pp. 1380-1387, 2002 (*in Japanese*).

[8] I. Yoshimura and Y. Sato, "Formulation for determining SIL using sequential failure logics", *Trans of the Japan Society of Mechanical Engineers* (C), Vol. 70, No. 691, pp. 879-885, 2004 (*in Japanese*).

[9] T. Shimodaira, Y. Sato and K. Suyama, "Estimation of average hazardous-event rate for steady-state demands and determination of SIL", *Trans of the Japan Society of Mechanical Engineers* (C), Vol. 72, No. 715, pp. 953-959, 2006 (*in Japanese*).

[10] IEC 61508-4, Functional safety of electrical/ electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, IEC, Geneva, 1998.

Authorized licensed use limited to: Fachhochschule FH Offenburg. Downloaded on May 31, 2009 at 13:46 from IEEE Xplore. Restrictions apply.