Functional Safety of Safety Related Systems with Safe Shutdown

Hitoshi MUTA*,

Koichi SUYAMA, and

Yoshinobu SATO

Tokyo University of Marine Science and Technology,

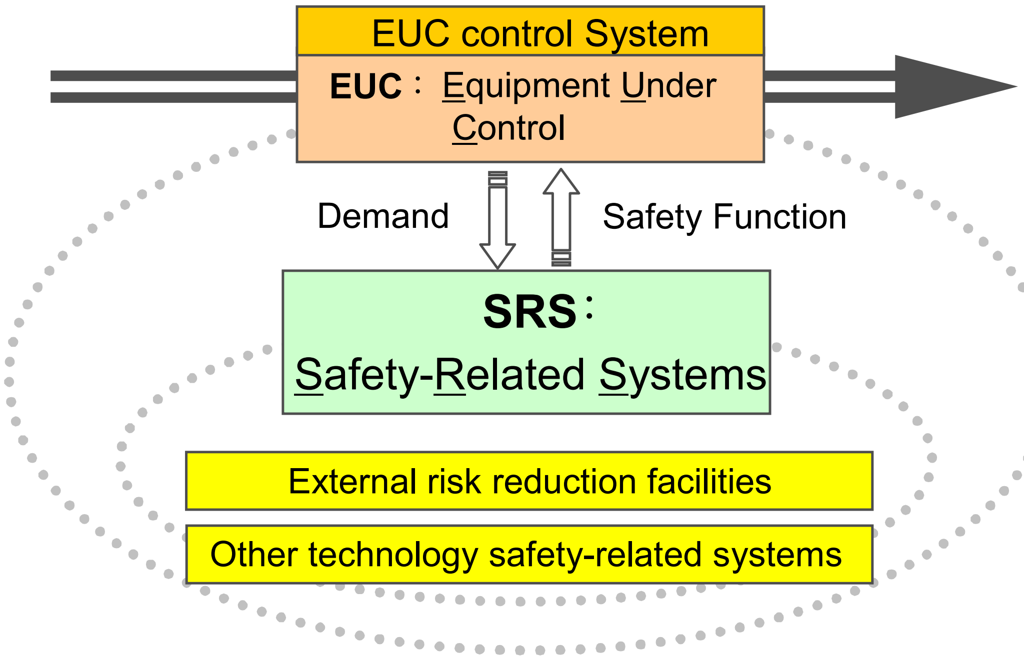
Tokyo, Japan

Contents

1.Forewords

- These days, systems equipped with computers have been used to implement safety functions in several industrial fields.
- Embedded software systems are increasingly utilized for advanced control of robot, space as well as automotive.
  - Requirement of critical safety is increasing
- IEC 61508 for functional safety of electric, electronic and programmable electronic safety related systems (E/E/PE SRS) was published in 2000 and now under the first revision.
  - In Japan, this standard was translated into Japanese as to publish JIS C 0508
- One of the most important features of this standard is to require quantitative safety integrity levels (SILs) for the random hardware failures of the SRS.

2. Definition of "Overall system" in IEC 61508



3.Safety requirements of IEC 61508

- The standard says that functional safety will be achieved by …
  - Conforming with the overall safety lifecycle requirements
  - Involving the SIL requirements
    - The SIL is to be determined using a target risk reduction and the failure probability of a safety function by SRS.
- However, the relationship between the risk reduction and the failure probability is not necessarily clear yet for implementation of the standard.

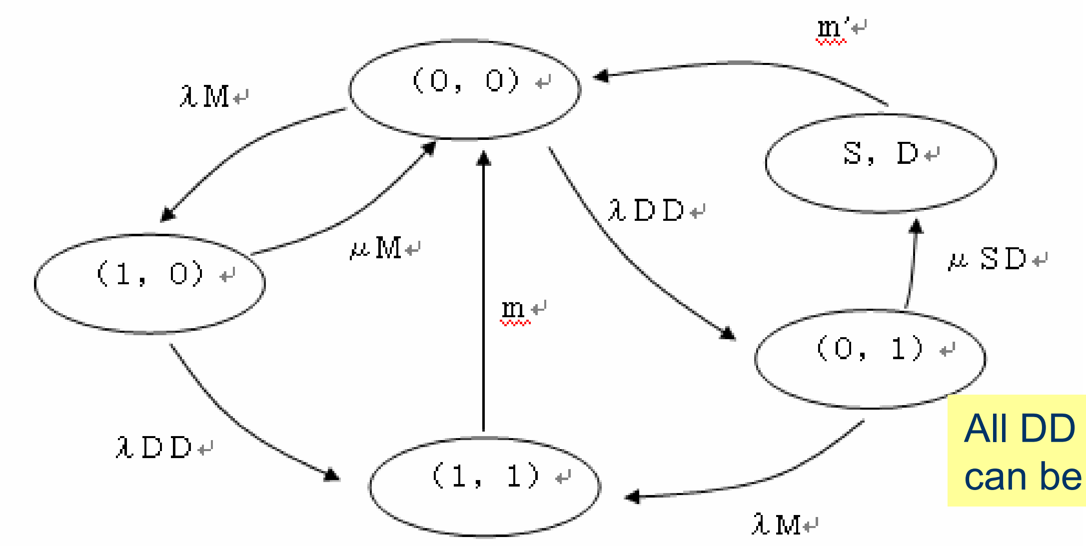
4.The relationship between SIL, frequency of demand and Dangerous event

- To solve this kind of issue….
  - To have formulated the relationship between the SIL and the frequency of dangerous event by using a fault-tree model ： KATO et al.
    - Where the SRS has no diagnostic function and can be repaired only by a proof-test
  - To have formulated the relationship for the SRS with a diagnostic function which can detect the fault for repair ： KAWAHARA et al.

5.The purpose of this study

- Chemical plants and nuclear power plants will be put into the safe shutdown state just after a detection of failure or AOT.
- So, this study focuses on the system equipped with a safe shutdown function and develops a quantitative model to evaluate the frequency of dangerous failure.
- A formulation will be developed for the dangerous event rate induced by the Dangerous Detectable (DD) failures based on a state transition model for a dangerous event.

6.Transition model(1)
- Markov Model -



All DD faults of SRS can be detected

λM: demand rate
λDD: dangerous detected-failure rate
μM: restoration (repair) rate
μSD: transition rate from a state where SRS is in a fault to a shutdown state

These parameters can be modeled by the exponential distribution

m: restoration rate from the state of harm to the initial state
m': restoration rate from the safe shutdown state to the initial state

6.Transition model(2)
- The simultaneous equations -

$$P(0,0)+P(1,0)+P(1,1)+P(0,1)+P(S,D)=1 \qquad (1)$$

$$\mu M\cdot P(1,0)+m'\cdot P(S,D)+m\cdot P(1,1)=\lambda M\cdot P(0,0)+\lambda DD\cdot P(0,0) \qquad (2)$$

$$\lambda M\cdot P(0,0)=(\mu M+\lambda DD)\cdot P(1,0) \qquad (3)$$

$$\lambda DD\cdot (1,0)+\lambda M\cdot P(0,1)=m\cdot P(1,0) \qquad (4)$$

$$\lambda DD\cdot P(0,0)=\lambda M\cdot P(0,1)+\mu SD\cdot P(0,1) \qquad (5)$$

$$\mu SD\cdot P(0,1)=m'\cdot P(S,D) \qquad (6)$$

6.Transition model(3)

- The real-average-dangerous-event rate -

- Calendar-time-averaged-dangerous-event rate defined as ω*hDD, then,

$$\omega^* hDD \cdot \Delta t = P^*(1,0) \cdot \lambda DD \cdot \Delta t + P^*(0,1) \cdot \lambda m \cdot \Delta t + o(\Delta t)$$

- Because P(1,1) and P(S,D) are the states of out of service, the real-average-dangerous-event rate is obtained by the following:

$$\omega^* = \frac{\omega^* hDD}{1 - P(1,1) - P(S,D)} = \frac{\dfrac{\lambda DD \cdot \lambda M}{\mu M + \lambda DD} + \dfrac{\lambda M \cdot \lambda DD}{\lambda M + \mu SD}}{1 + \dfrac{\lambda M}{\mu M + \lambda DD} + \dfrac{\lambda DD}{\lambda M + \mu SD}}$$

- The real-average-dangerous-event rate can be evaluated without the restoration rate "m" from the harm nor the restoration rate "m'" after the safe shutdown.

7.Summary

- The relationship between the DD failures of SRS, the safe shutdowns of the overall system, the demands and dangerous events is modeled by a state transition diagram and formulated for reasonable determination of SIL.
- The formulation presents the calendar-time-averaged-dangerous-event rate and the real-average-dangerous-event rate, which are essential measures for the determination of SILs.
- In additions, it is found out that the latter probabilistic measure is calculated without the effect of restoration from the harm nor the safe shutdown state.

8.Future work

- There will be several types of shutdown functions;
  for which the more complicated treatment will be required.
- Thus, further study will be necessary to develop the state transition models for various types of safety functions.

Definitions of fault

- Dangerous fault: A state losing safety function of SRS
- DD fault：Dangerous fault which can be detected by the diagnostic function
- DD failure：Occurrence of DD fault
- DU fault：Dangerous fault which cannot be detected by the diagnostic function but proof test, checking activities after restoration and dangerous event by the DU fault after a demand
- DU failure： Occurrence of DU fault
- Safe shut down：Transition process to system shut down after a occurrence of DD fault

Descriptions of “Overall System”

- The overall system is composed of an EUC, BCS, E/E/PE SRS, other technology SRS and external risk reduction facilities
- The dangerous event occur when a demand occurs in the fault of subsystems.
- Diagnostic function can decrease a frequency of dangerous event to have a countermeasure as follows;
  - (1) To separate and repair the SRS as soon as possible after a detection of DD failure, but the EUC continues to run, or
  - (2) To transfer the EUC into a safe shutdown state as soon as possible after the detection of DD failure.
- The system like a production plant has an SRS designed based on the consideration of concept (1).
- On the other hand, chemical plants and nuclear power plants are typically designed based on the consideration of concept (2).

Notations of Transition model

- (0, 0): the initial state where SRS is normal and the overall system is not in any demand state.
- (1, 0): SRS is normal and the overall system is in a demand state where the implementation of the safety function is required.
- (0, 1): SRS is in a fault and the overall system is not in any demand state.
- (1, 1): SRS is in a fault and the overall system is in a on demand state, namely this state indicates a harm.
- S, D : The system is in a safe shutdown state after a fault of SRS.

P (*,*): Constant Probability of a state (*,*) in the state transition model.

Assumptions of Transition model

- EUC doesn't interrupt during either proof test of SRS or repair
- All DD faults of SRS can be detected
- Demands and failures of SRS occur statistically-independently
- The start of and the termination of the demand can be modeled by the exponential distribution with demand rate λM and restoration rate μM, respectively
- The DD fault can be modeled by the exponential distribution with failure rate, λDD
- The safety shutdown can be modeled by the exponential distribution with transition rate μSD

Assumptions of Transitions

- The system is put into a renewal after the dangerous event by the restoration rate "m".
- The system is put into a renewal after the DD fault and then a demand occurs before the safe shutdown by the restoration rate "m".
- The system is put into a renewal after the DD fault and then the safe shut down occurs before a demand by the restoration rate "m’".