2008 American Control Conference
Westin Seattle Hotel, Seattle, Washington, USA
June 11-13, 2008

Safety function in a control law and its assessment and management

Koichi Suyama
Tokyo University of Marine Science and Technology
Etchujima, Koto-ku, Tokyo 135-8533, Japan

Abstract— **This paper clarifies a safety function in a control law from a viewpoint of the international safety standard, IEC 61508, and presents a probabilistic safety assessment and management framework using an idea of representative safety functions, which is newly introduced from a practical viewpoint.**

I. INTRODUCTION

The social environment surrounding system safety has changed rapidly. One of the epochs was that TC65 WGs 9 and 10 in IEC, International Electrotechnical Commission, established an international standard, IEC 61508[4]. It is applied to almost all electrical/electronic/programmable electronic (E/E/PE) safety-related systems (SRSs) irrespective of their applications. It has been quoted into several national standards or guidelines of UK, USA and Japan.

Since the late 1970s many studies have been made on control system design under possible device failures as reliable control theory[6], e.g., integrity, reliable H_∞ control. Recently the importance of such safety function in a control law has been growing. One of the reasons is that ISO/IEC Guide 51[5] adopted newly risk to the environment and to property as its scope. It is widely known that there are many cases where safety measures outside a control system are not enough to reduce risk to property or to the environment.

This paper presents a safety assessment and management framework based on IEC 61508 for a control law. From a practical viewpoint, it uses a set of representative safety functions, which is a key idea of this paper. It also uses Markov techniques summarized in IEC 61165[3] to take repair of failed control devices into consideration. It is more practical than the one in [7], [8], [9].

The presented framework clarifies quantitatively a concrete contribution of safety function in a control law to risk reduction and an established meaning in system safety design according to IEC 61508.

In the ongoing maintenance of IEC 61508 a more detailed safety assessment framework for software used in E/E/PE SRSs is newly prepared for publication. However it will not go much beyond qualitative assessment, i.e., it will only set requirements on selecting methods for coding, testing, and so on. Quantitative and probabilistic safety assessment and management of software is one of the most important problems to be solved in future. The content of a control law is software designed by control theory or firsthand knowledge. Hence the presented framework for a control law is ahead of the times.

II. SAFETY FUNCTION IN A CONTROL LAW

A. IEC 61508

Figure 1 illustrates the overall system configuration considered in IEC 61508. A control system consists of an equipment under control (EUC), i.e., a controlled object, and a basic control system (BCS) which responds to input signals from the process and/or an operator and generates output signals causing the EUC to operate in the desired manner. IEC 61508 requests to reduce the initial risk, i.e., EUC+BCS risk, by E/E/PE SRSs and/or other technology SRSs and external risk reduction facilities (ERRFs) so that the residual risk of the overall system is less than the predetermined tolerable risk level as shown in Fig. 2. To be precise, IEC 61508 is the standard for E/E/PE SRSs.

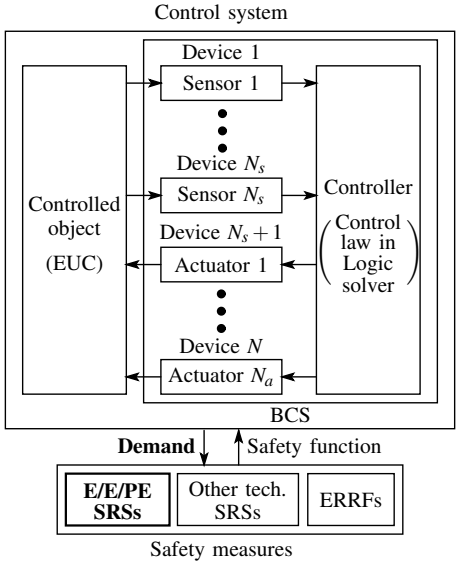

Fig. 1. Overall system.

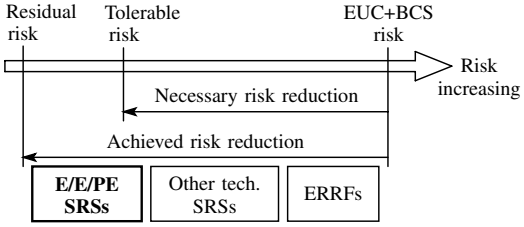

Fig. 2. Risk reduction.

TABLE I

SAFETY INTEGRITY LEVELS IN LOW DEMAND MODE OF OPERATION.

SIL	Average probability of failure to perform its design function on demand (PFD_{avg})
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 $< 10^{-1}$

A SRS has safety function to achieve or to maintain a safe state of the EUC. Functional safety is its ability to perform the safety function. Note that a hardware failure occurs at a random time in a SRS. Then there is the possibility that the SRS cannot perform its safety function. IEC 61508 assesses functional safety of an E/E/PE SRS, i.e., the probability of failure to perform its safety function, using four safety integrity levels (SILs) for two kinds of operation modes, low demand mode of operation as shown in TABLE I and high demand / continuous mode. If a SRS shoulders a heavy burden for risk reduction, it is required to fit a higher SIL.

B. Condition setting

Consider a control system shown in Fig. 1. Let Device 1,..., Device N denote Sensor 1,..., Sensor N_s and Actuator 1,..., Actuator N_a, where $N = N_s + N_a$.

A failure, a functional stoppage, probabilistically occurs in Device k in accordance with the exponential distribution with the failure rate λ_k, $k = 1,\ldots,N$. Repair of failed Device k probabilistically ends in accordance with the exponential distribution with the mean time to repair, MTTR_k, $k = 1,\ldots,N$[1]. The repair rate of Device k is given by $\mu_k = 1/\mathrm{MTTR}_k$. This is an ordinary formulation in the field of safety/reliability engineering.

We assume the followings.

Assumption 1: The failure rate of the logic solver is sufficiently smaller than λ_k and its effect is negligible.

Assumption 2: A demand on an E/E/PE SRS occurs when the control system falls into an unstable state.

Remark 1: The presented framework can be extended to a more general one by considering stability degree or permissible deterioration in control performance.

Assumption 3: The frequency that the control system falls into an unstable state by control device failures is sufficiently higher than the frequency by other causes.

Remark 2: In general several causes can make a control system fall into an unstable state, e.g., external hazards. Such causes depend on each case, and the dependence should be avoided to obtain a general safety assessment framework for a control law. Hence this paper considers only control device faults as most basic internal causes.

[1]In IEC 61508 repair process is quantitatively treated by MTTR.

C. Device context

Device k $(k = 1,2,\ldots,N)$ is in either of normal operation or fault as described in the following:

$$\delta_k = \begin{cases} 0, & \text{Device } k : \text{normal} \\ 1, & \text{Device } k : \text{fault} \end{cases} \qquad (k = 1,2,\ldots,N). \quad (1)$$

Describe a device situation of the control system by $(\delta_1,\delta_2,\ldots,\delta_N)$, which is referred to hereafter as the *device context*. For example, $(0,\ldots,0)$ denotes the normal operation, *Normal*, $(1,0,0,0,\ldots,0)$ represents a device situation where only Device 1 is in a fault, and $(0,1,1,0,\ldots,0)$ represents a device situation where only Devices 2 and 3 are in a fault. Device contexts considered are 2^N in all.

D. Safety function in a control law

The safety function in a control law is the ability to maintain the stability of the control system in a device context except Normal. Hence, in substance, it can be identified with a set of device contexts except Normal, S, where the control system with the control law is stable.

For example, the safety function in a control law corresponding to a set of device contexts: $\mathrm{S} = \{(1,0,0,0,\ldots,0),(0,0,1,0,\ldots,0),(1,0,1,0,\ldots,0)\}$ is the ability to maintain the stability of the control system with the control law in either Normal or a situation where Device 1 and/or Device 2 is in a fault.

III. REPRESENTATIVE SAFETY FUNCTIONS IN A CONTROL LAW

A general safety function in a control law defined in the previous section is approximated by a representative one to assess it. In this section a representative safety function in a control law is defined and expressed. It plays an essential role in the presented assessment and management framework for a control law due to the followings.

- All device contexts in a representative safety function is reachable from Normal.
- All representative safety functions can be expressed in the simple and fixed-length structure.
- They can be enumerated systematically.
- They can easily be assessed.

A. Definition and expression

In order to consider a representative safety function in a control law, define m-th n-DG (device group), $\mathrm{G}_{(n,m)} = \{\text{Device } k_{n,m,1},\ \text{Device } k_{n,m,2},\ \ldots,\ \text{Device } k_{n,m,n}\}$, where n denotes the number of devices in the DG, and m denotes the order in n-DGs (in the expression of a representative safety function). Let $\mathrm{S}_{(n,m)}$ denote the set of $2^n - 1$ device contexts, all possible normal/fault combinations of the devices in $\mathrm{G}_{(n,m)}$ except Normal. For example, for a DG $\mathrm{G}_{(2,1)} = \{\text{Device 1},\ \text{Device 2}\}$, we have the corresponding sets of device contexts $\mathrm{S}_{(2,1)} = \{(1,0,0,\ldots),(0,1,0,\ldots),(1,1,0,\ldots)\}$.

Consider a representative safety function in a control law by

$$\Big\{\mathrm{G}_{(n,m)}\ (n,m=1,2,3,\ldots)\,\Big|\ \mathrm{G}_{(n_1,m_1)}\cap\mathrm{G}_{(n_2,m_2)}=\phi\ ((n_1,m_1)\neq(n_2,m_2))\Big\}\quad(2)$$

i.e., the set of device contexts $\bigcup_{n,m}\mathrm{S}_{(n,m)}$. Define $\mathrm{G}_{\mathrm{rest}}=\big\{\text{Device 1},\ldots,\text{Device } N\big\}\setminus\big(\bigcup_{n,m}\mathrm{G}_{(n,m)}\big)$.

Note that all device contexts in a representative safety function is reachable from Normal. That is, they do not include an isolated device context to which there is no state transition paths from Normal.

In this paper such a representative safety function is expressed by $[i_1,i_2,\ldots,i_N]$ where

$$i_k=\begin{cases}1 & \text{Device } k\in\text{1-DG}\\ n+1-(1/2)^{m-1} & \text{Device } k\in m\text{-th } n(\geq 2)\text{-DG}\\ 0 & \text{Device } k\in\mathrm{G}_{\mathrm{rest}}\end{cases}$$

If $i_{k_1}=i_{k_2}$, Devices k_1 and k_2 belong to the same device group. $n(\geq 2)$-DGs including n devices are expressed by $n, n\,1/2, n\,3/4, n\,7/8, \ldots$, in the order of appearance in order of device numbers. This simple and fixed-length expression can make it possible to enumerate all representative safety functions easily and systematically.

For example, in the case where $N=6$, a representative safety function $[0,2,2\,1/2,2\,1/2,1,2]$ maintains the stability of the control system in the following device contexts except Normal:

- device contexts $\mathrm{S}_{(1,1)}=\big\{(0,0,0,0,1,0)\big\}$ corresponding to (1st) 1-DG $\mathrm{G}_{(1,1)}=\big\{\text{Device 5}\big\}$
- device contexts $\mathrm{S}_{(2,1)}=\big\{(0,1,0,0,0,0),(0,0,0,0,0,1),(0,1,0,0,0,1)\big\}$ corresponding to 1st 2-DG $\mathrm{G}_{(2,1)}=\big\{\text{Device 2, Device 6}\big\}$
- device contexts $\mathrm{S}_{(2,2)}=\big\{(0,0,1,0,0,0),(0,0,0,1,0,0),(0,0,1,1,0,0)\big\}$ corresponding to 2nd 2-DG $\mathrm{G}_{(2,2)}=\big\{\text{Device 3, Device 4}\big\}$.

B. Class

In order to enumerate all representative safety functions in a control law, introduce a class of them, $<j_1,j_2,\ldots,j_N>$. j_n $(n=2,3,\ldots)$ denotes the number of n-DGs, and

$$j_1=\begin{cases}1, & \text{a 1-DG and/or a device}\in\mathrm{G}_{\mathrm{rest}}\text{ exists}\\ 0, & \text{otherwise}\end{cases}.$$

For example, in the case where $N=6$, a representative safety function $[0,2,2\,1/2,2\,1/2,1,2]$ includes two 2-DGs and an 1-DG, and belongs to the class $<1,2,0,0,0,0>$.

A class of representative safety functions corresponds to a partition of N, which is the number of devices. Hence the number of classes is equivalent to the number of partitions of N shown in TABLE II.

TABLE II
NUMBER OF PARTITIONS

N	Number of partitions
2	2
3	3
4	5
5	7
6	11
7	15
8	22
9	30
10	41
11	56
12	77

The class $<1,0,\ldots,0>$ includes 2^N-1 representative safety functions. Another class $<j_1,j_2,\ldots,j_N>$ includes

$$M=\prod_{l=0}^{N-1}T_{N-l}\qquad(3)$$

representative safety functions, where

$$R_n=\begin{cases}N-\sum_{l=n+1}^{N}l\cdot j_l & (n=1,2,\ldots,N-1)\\ N & (n=N)\end{cases}$$

$$T_n=\begin{cases}2^{R_1} & (n=1)\\ \frac{1}{j_n!}\prod_{l=1}^{j_n}{}_{R_n-(l-1)n}\mathrm{C}_n & (n\geq 2,\ j_n\geq 1)\\ 1 & (n\geq 2,\ j_n=0)\end{cases}$$

For example, in the case where $N=6$, classes, corresponding partitions, and the numbers of included representative safety functions are shown in TABLE III.

TABLE III
CLASSES OF REPRESENTATIVE SAFETY FUNCTIONS

Class	Corresponding partition	Number of representative safety functions
$<1,0,0,0,0,0>$	$1+1+1+1+1+1$	63
$<1,1,0,0,0,0>$	$2+1+1+1+1$	240
$<1,2,0,0,0,0>$	$2+2+1+1$	180
$<0,3,0,0,0,0>$	$2+2+2$	15
$<1,0,1,0,0,0>$	$3+1+1+1$	160
$<1,1,1,0,0,0>$	$3+2+1$	120
$<0,0,2,0,0,0>$	$3+3$	10
$<1,0,0,1,0,0>$	$4+1+1$	60
$<0,1,0,1,0,0>$	$4+2$	15
$<1,0,0,0,1,0>$	$5+1$	12
$<0,0,0,0,0,1>$	6	1
Total number		876

The key is that all representative safety functions can be enumerated systematically for each class.

C. Safety assessment

A representative safety function $[i_1, i_2, \ldots, i_N]$ includes m-th n-DG $\mathrm{G}_{(n,m)}$ $(n,m = 1,2,3\ldots)$ determined by the following rules:

- If $i_{k_1} = i_{k_2} = \cdots = i_{k_l} = \cdots = 1$ $(k_1 < k_2 < \cdots < k_l < \cdots)$, $\mathrm{G}_{(1,l)} = \{\text{Device } k_l\}$.
- If $i_{k_1} = i_{k_2} = \cdots = i_{k_n} = n' = n+1-(1/2)^{m-1}$, $\mathrm{G}_{(n,m)} = \{\text{Device } k_1,\ \text{Device } k_2,\ \ldots,\ \text{Device } k_n\}$, where n is the integer such that $n \le n'$.

Define

$$\lambda_{\text{total}} = \sum_{k=1}^{N} \lambda_k \tag{4}$$

and for each $\mathrm{G}_{(n,m)} = \{\text{Device } k_{n,m,1}, \text{Device } k_{n,m,2},\ \ldots,\ \text{Device } k_{n,m,n}\}$ $(n,m = 1,2,3,\ldots)$ calculate

$$\lambda_{(n,m)} = \sum_{l=1}^{n} \lambda_{k_{n,m,l}}, \quad \lambda'_{(n,m)} = \lambda_{\text{total}} - \lambda_{(n,m)} \tag{5}$$

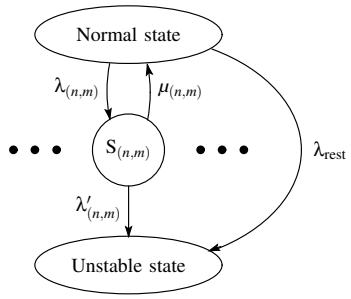

Fig. 3. State transition diagram.

Approximation condition: Simultaneous repair in each group $\mathrm{G}_{(n,m)}$, $n,m = 1,2,\ldots$, probabilistically ends in accordance with the exponential distribution with the repair rate

$$\mu_{(n,m)} = \min_{l=1,\ldots,n} \mu_{k_{n,m,l}} \tag{6}$$

regardless of the number of failed devices.

Note that this approximation condition on simultaneous repair with the smallest rate in a device group gives a conservative assessment result.

Under this condition, a Markov diagram in Fig. 3 describes the state transition from the normal state, Normal, to demand occurrence, i.e., an unstable state of the control system. The arrows with $\lambda_{(n,m)}$ and with $\mu_{(n,m)}$ denote a failure and a repair in $\mathrm{G}_{(n,m)}$, respectively. The arrow with $\lambda'_{(n,m)}$ denotes a failure in another device than $\mathrm{G}_{(n,m)}$ on the state $\mathrm{S}_{(n,m)}$. The arrow with $\lambda_{\text{rest}} (= \lambda_{\text{total}} - \sum_{n,m} \lambda_{(n,m)})$ denotes a failure in G_{rest}. The important point of the presented probabilistic safety assessment framework for a control law is that the Markov diagram has its simple structure with only one absorbing state.

Remark 3: Approximation condition makes it possible to get all the situations belonging to $\mathrm{S}_{(n,m)}$ together into one state in the Markov diagram as shown in Fig. 3. As a result, the Markov diagram has its simple structure. Hence, even if there are numerous control devices, we can easily assess a control law used in it. While Approximation condition certainly gives a conservative assessment result, this kind of assumption is inevitable from a practical viewpoint especially in Markov analysis[3].

Assumption 4:

$$\text{MTTD} \gg (\text{SRS operation time}) + \text{MTTR}_{\text{sys}} \tag{7}$$

where MTTD denotes the mean time to demand, and MTTR_{sys} denotes the mean time to repair of the control system.

Under this reasonable assumption, we can obtain the following formula of the demand frequency in the same manner as [9]:

$$\text{DF}([i_1, i_2, \ldots, i_N]) = \left[q_0 + \sum_{n,m} q_{(n,m)} \right]^{-1} \tag{8}$$

where

$$q_0 = \left[\lambda_{\text{total}} - \sum_{n,m} \frac{\lambda_{(n,m)} \mu_{(n,m)}}{\mu_{(n,m)} + \lambda'_{(n,m)}} \right]^{-1}$$

$$q_{(n,m)} = \frac{\lambda_{(n,m)}}{\mu_{(n,m)} + \lambda'_{(n,m)}} q_0 \quad (n,m = 1,2,3,\ldots).$$

The important point is that all representative safety functions can easily be assessed, i.e., the demand frequency can be obtained by simple calculation (8).

IV. Safety assessment framework for a control law

The presented safety assessment framework for a control law is based on demand frequency of the resulting control system. The demand frequency itself is used for E/E/PE SRS design achieving a given target safety integrity level, i.e., target hazardous event frequency. The framework consists of the following steps:

Step 1: for the control system with the assessed control law, obtaining a set of all stable device contexts, SDC

Step 2: obtaining the demand frequency, DF, of the control system using representative safety functions

Step 3: SIL assignment to SRS, if necessary.

A. Step 1: a set of stable device contexts

By stability analysis in all device contexts (and in Normal) one by one, we can obtain a set of all stable device contexts except Normal, SDC. It can be identified with the safety function in the assessed control law. If the control system is in either the normal operation or one device contexts of SDC, it maintains its stability. However if it transfers to another device context, it falls into an unstable state and a demand on safety measures such as an E/E/PE SRS occurs.

TABLE IV

STABLE DEVICE CONTEXTS OF THE SYSTEM WITH THE ASSESSED CONTROL LAW.

Device context	(0,0,0,0,0) (Normal)	(1,0,0,0,0)	(0,0,1,0,0)	(0,0,0,1,0)	(1,0,0,1,0)
Poles	-10.08	-6.48	-3.52	-5.45	-7.56
	-5.12	$-1.76+j2.66$	$-0.74+j5.41$	-4.00	-2.20
	-1.80	$-1.76-j2.66$	$-0.74-j5.41$	-0.55	-0.24

B. Step 2: assessment using representative safety functions

Define a set of representative safety functions such that

$$\mathrm{S}_0 = \Big\{[i_1, i_2, \ldots, i_N] \,\Big|\, \Big(\bigcup_{n,m} \mathrm{S}_{(n,m)}\Big) \subseteq \mathrm{SDC}\Big\}. \tag{9}$$

Then the demand frequency of the control system with the assessed control law can be obtained as follows:

$$\mathrm{DF} = \min_{[i_1,i_2,\ldots,i_N]\in \mathrm{S}_0} \mathrm{DF}([i_1, i_2, \ldots, i_N]). \tag{10}$$

C. Step 3: SIL assignment to SRS

Functional safety of an E/E/PE SRS in low demand mode of operation is evaluated by average probability of failure to perform its design function on demand ($\mathrm{PFD}_{\mathrm{avg}}$). Here, the hazardous event frequency, HEF, is given by

$$\mathrm{HEF} = \mathrm{DF} \times \mathrm{PFD}_{\mathrm{avg}}. \tag{11}$$

Hence, given a target hazardous event frequency, $\mathrm{HEF}_{\mathrm{tar}}$, it should be that

$$\mathrm{PFD}_{\mathrm{avg}} \leq \frac{\mathrm{HEF}_{\mathrm{tar}}}{\mathrm{DF}}. \tag{12}$$

We should install an E/E/PE SRS of the corresponding SIL shown in TABLE I.

The lower demand frequency, the better control law in the sense of system safety. An E/E/PE SRS shoulders a light burden for risk reduction, i.e., it is required to fit a lower SIL. This is the concrete contribution of safety function in a control law to risk reduction required in IEC 61508.

V. ASSESSMENT EXAMPLE

A control system consists of a controlled object, three sensors, Sensors 1, 2 and 3 (Devices 1, 2 and 3), two actuators, Actuators 1 and 2 (Devices 4 and 5), and a control law in a logic solver. Suppose that

$$\begin{array}{ll}
\lambda_1 = 5\times 10^{-5}[1/\mathrm{hr}], & \mathrm{MTTR}_1 = 10[\mathrm{hr}] \\
\lambda_2 = 1\times 10^{-5}[1/\mathrm{hr}], & \mathrm{MTTR}_2 = 20[\mathrm{hr}] \\
\lambda_3 = 2\times 10^{-5}[1/\mathrm{hr}], & \mathrm{MTTR}_3 = 10[\mathrm{hr}] \\
\lambda_4 = 5\times 10^{-5}[1/\mathrm{hr}], & \mathrm{MTTR}_4 = \ 5[\mathrm{hr}] \\
\lambda_5 = 1\times 10^{-5}[1/\mathrm{hr}], & \mathrm{MTTR}_5 = 20[\mathrm{hr}]
\end{array}$$

Consider a plant consisting of the controlled object, the three sensors measuring the state variables, and the two actuators given by

$$\frac{d}{dt}x(t) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} x(t) + \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} u(t)$$

TABLE V

REPRESENTATIVE SAFETY FUNCTIONS FOR ASSESSMENT EXAMPLE.

Class	$[i_1, i_2, \ldots, i_N] \in \mathrm{S}_0$	DF [/hr]
$<1,0,0,0,0>$	[1,0,0,0,0]	9.000×10^{-5}
	[0,0,1,0,0]	1.200×10^{-4}
	[0,0,0,1,0]	9.000×10^{-5}
	[1,0,1,0,0]	7.002×10^{-5}
	[1,0,0,1,0]	4.004×10^{-5}
	[0,0,1,1,0]	7.002×10^{-5}
	[1,0,1,1,0]	2.007×10^{-5}
$<1,1,0,0,0>$	[2,0,0,2,0]	4.000×10^{-5}
	[2,0,1,2,0]	2.004×10^{-5} (min)

and state feedback

$$u(t) = -\begin{bmatrix} 7 & 10 & 4 \\ 8 & 17 & 12 \end{bmatrix} x(t)$$

where this is the assessed control law.

A. Step 1: a set of stable device contexts

TABLE IV shows all stable device contexts including Normal. Then

$$\mathrm{SDC} = \big\{(1,0,0,0,0),\ (0,0,1,0,0),\ (0,0,0,1,0),\ (1,0,0,1,0)\big\}.$$

B. Step 2: assessment using representative safety functions

See TABLE V. Then we have

$$\mathrm{DF} = \mathrm{DF}([2,0,1,2,0]) = 2.004\times 10^{-5}[/\mathrm{hr}].$$

Remark 4: If Approximation condition is not applied to assessment, we should consider a more complicated Markov diagram shown in Fig. 4 than Fig. 3. Markov analysis based on this diagram results in $\mathrm{DF} = 2.0035\times 10^{-5}$[/hr]. That is, the above assessment result under Approximation condition, $\mathrm{DF} = 2.0040\times 10^{-5}$[/hr], includes only 0.025% error.

C. Step 3: SIL assignment to SRS

Suppose that the target hazardous event frequency is $\mathrm{HEF}_{\mathrm{tar}} = 10^{-3}[1/\mathrm{yr}]$, i.e., one time per 1000 years.

In the control system with the assessed control law, it should be that

$$\mathrm{PFD}_{\mathrm{avg}} \leq \frac{10^{-3}[1/\mathrm{yr}]}{2.004\times 10^{-5}[1/\mathrm{hr}]} = 5.70\times 10^{-3}.$$

Hence it is enough to install an E/E/PE SRS of SIL3 to achieve the target hazard frequency. Note that an E/E/PE

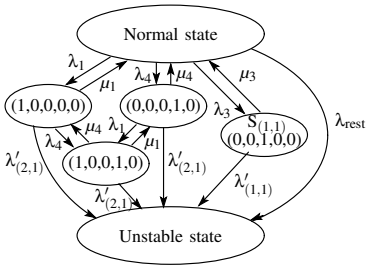

Fig. 4. State transition diagram without Approximation condition.

SRS of SIL2 with a high $\mathrm{PFD}_{\mathrm{avg}}$ value in the range $[10^{-3}, 10^{-2})$ can not achieve the target hazardous event frequency.

VI. Safety management framework for a control law

In this section we present a probabilistic safety management framework for a control law based on demand frequency as a safety performance index, where representative safety functions play an essential role.

It consists of the following steps:

Step 1: setting a target demand frequency, $\mathrm{DF}_{\mathrm{tar}}$

Step 2: obtaining a set of all representative safety functions, S_1

Step 3: obtaining a set of all representative safety functions satisfying safety requirement, S_2

Step 4: obtaining a control law achieving one safety function in S_2 and the optimal control performance by reliable/robust control theory.

A. Step 1: target demand frequency

For given a target hazardous event frequency, $\mathrm{HEF}_{\mathrm{tar}}$, $\mathrm{PFD}_{\mathrm{avg}}$ of an E/E/PE SRS should be

$$\mathrm{PFD}_{\mathrm{avg}} \leq \frac{\mathrm{HEF}_{\mathrm{tar}}}{\mathrm{DF}}. \tag{13}$$

Then, a target safety integrity level, SIL_{tar}, is determined by TABLE I. We should install an E/E/PE SRS of $\mathrm{SIL}_{\mathrm{tar}}$. Hence, taking $\mathrm{HEF}_{\mathrm{tar}}$ and $\mathrm{SIL}_{\mathrm{tar}}$ into consideration, we should set a target demand frequency, $\mathrm{DF}_{\mathrm{tar}}$.

B. Step 2: all representative safety functions

Using classes of representative safety functions and (3), enumerate all representative safety functions and gather them into a set, S_1. For example, in the case where $N = 6$, S_1 includes 876 representative safety functions as shown in TABLE III. In each class we can use selection of n figures '$n+1-(1/2)^{m-1}$' out of device numbers, $1,2,\ldots,N$, for m-th n-DG and binary digit to enumerate all representative safety functions. For example, in the case where $N = 6$, the class $< 1,0,0,0,0,0 >$ includes $2^6 - 1 = 63$ representative safety functions: [1,0,0,0,0,0], [0,1,0,0,0,0], [1,1,0,0,0,0], [0,0,1,0,0,0], ... , [1,1,1,1,1,1], and the class $< 1,0,0,1,0,0 >$ includes [4,4,4,4,0,0], [4,4,4,4,1,0], [4,4,4,4,0,1], [4,4,4,4,1,1], [4,4,4,0,4,0], [4,4,4,1,4,0], [4,4,4,0,4,1], [4,4,4,1,4,1], [4,4,4,0,0,4], [4,4,4,1,0,4], [4,4,4,0,1,4], [4,4,4,1,1,4], ...

C. Step 3: all representative safety functions satisfying safety requirement

For each representative safety function $[i_1, i_2, \ldots, i_N] \in \mathrm{S}_1$, obtain $\mathrm{DF}([i_1, i_2, \ldots, i_N])$ by (8). Then obtain the following set of all representative safety functions satisfying safety requirement:

$$\mathrm{S}_2 = \left\{ [i_1, i_2, \ldots, i_N] \in \mathrm{S}_1 \,\middle|\, \mathrm{DF}([i_1, i_2, \ldots, i_N]) < \mathrm{DF}_{\mathrm{tar}} \right\}. \tag{14}$$

The important point is that $\mathrm{DF}([i_1, i_2, \ldots, i_N])$ can easily be obtained by (8).

D. Step 4: control law design

For each representative safety function $[i_1, i_2, \ldots, i_N] \in \mathrm{S}_2$, design a control law such that

- it achieves the safety function $[i_1, i_2, \ldots, i_N]$, i.e., the resulting control system maintains its stability even in one device context of $\bigcup_{n,m} \mathrm{S}_{(n,m)}$, and
- it achieves the optimal value of a control performance index, $\mathrm{CP}([i_1, i_2, \ldots, i_N])$.

If we reduce such design to a robust performance problem, we need an additional method such as LFT scaling[1] for obtaining a less conservative design result.

The solution is the control law corresponding to

$$\min_{[i_1, i_2, \ldots, i_N] \in \mathrm{S}_2} \mathrm{CP}([i_1, i_2, \ldots, i_N]). \tag{15}$$

VII. Management example

Consider the following generalized plant:

$$\begin{bmatrix} z \\ y \end{bmatrix} = \left[\begin{array}{cccc|cccc} -2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ -1 & 0 & -2 & -3 & 1 & 0 & 0 & 1 \\ -2 & -1 & 2 & -1 & 0 & 0 & 1 & 0 \\ \hline 1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \end{array}\right] \begin{bmatrix} w \\ u \end{bmatrix}$$

where $\left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$ denotes $C(sI-A)^{-1}B+D$. The controlled object has three outputs measured by Sensors 1, 2 and 3 (Devices 1, 2 and 3) and three inputs through Actuators 1, 2 and 3 (Devices 4, 5 and 6). That is, $N_s = 3$, $N_a = 3$, $N = 6$. Suppose that

$$\begin{aligned} \lambda_1 &= 4 \times 10^{-5}[1/\mathrm{hr}], \quad \mathrm{MTTR}_1 = \ 200[\mathrm{hr}] \\ \lambda_2 &= 9 \times 10^{-6}[1/\mathrm{hr}], \quad \mathrm{MTTR}_2 = 1000[\mathrm{hr}] \\ \lambda_3 &= 2 \times 10^{-5}[1/\mathrm{hr}], \quad \mathrm{MTTR}_3 = \ 500[\mathrm{hr}] \\ \lambda_4 &= 3 \times 10^{-5}[1/\mathrm{hr}], \quad \mathrm{MTTR}_4 = \ 200[\mathrm{hr}] \\ \lambda_5 &= 6 \times 10^{-6}[1/\mathrm{hr}], \quad \mathrm{MTTR}_5 = 1000[\mathrm{hr}] \\ \lambda_6 &= 9 \times 10^{-6}[1/\mathrm{hr}], \quad \mathrm{MTTR}_6 = 1000[\mathrm{hr}]. \end{aligned}$$

Control performance is evaluated by the index $\mathrm{CP} = \|T_{zw}\|_\infty = \|F_l(G,K)\|_\infty$ where G is the generalized plant, K is a control law, and F_l denotes lower LFT.

TABLE VI

REPRESENTATIVE SAFETY FUNCTIONS FOR MANAGEMENT EXAMPLE.

Class	[Step 2] Number of S_1	[Step 3] Number of S_2	[Step 4] Representative safety function (CP$<$ 1.6)		
			$[i_1, i_2, \ldots, i_N]$	DF [/hr]	CP
$<1,0,0,0,0,0>$	63	2	[1,1,1,1,0,1]	9.318×10^{-6}	1.5558 (min)
$<1,1,0,0,0,0>$	240	25	[2,1,2,1,0,1]	9.305×10^{-6}	1.5599
			[2,1,1,1,0,2]	1.051×10^{-5}	1.5635
			[1,2,2,1,0,1]	9.733×10^{-6}	1.5648
			[1,1,2,2,0,2]	9.390×10^{-6}	1.5647
			[1,1,2,1,0,2]	9.733×10^{-6}	1.5619
$<1,2,0,0,0,0>$	180	58	[2,2 1/2,2 1/2,1,0,2]	1.090×10^{-5}	1.5736
			[2,1,2 1/2,2 1/2,0,2]	1.057×10^{-5}	1.5732
$<0,3,0,0,0,0>$	15	15	—		
$<1,0,1,0,0,0>$	160	32	[3,1,3,1,0,3]	9.557×10^{-6}	1.5738
$<1,1,1,0,0,0>$	120	72	—		
$<0,0,2,0,0,0>$	10	10	—		
$<1,0,0,1,0,0>$	60	26	—		
$<0,1,0,1,0,0>$	15	15	—		
$<1,0,0,0,1,0>$	12	9	—		
$<0,0,0,0,0,1>$	1	1	—		
Total number	876	265			

A. Step 1: target demand frequency

Set $\mathrm{DF_{tar}} = 1.1416\times10^{-5}[/\mathrm{hr}]$ so that $\mathrm{HEF_{tar}} = 10^{-3}[/\mathrm{yr}]$ can be achieved by only one E/E/PE SRS of SIL2 in low demand mode of operation.

B. Step 2: all representative safety functions

A total of 876 representative safety functions can be considered as shown in TABLE III and in TABLE VI.

C. Step 3: all representative safety functions satisfying safety requirement

A total of 265 representative safety functions satisfy the safety requirement $\mathrm{DF}([i_1, i_2, \ldots, i_N]) < \mathrm{DF_{tar}}$ as shown in TABLE VI.

D. Step 4: control law design

Show representative safety function with CP$<$ 1.6 in TABLE VI because there is no space for all representative safety function in S_2. The solution is the following control law achieving representative safety function [1,1,1,1,0,1] and the minimum CP value 1.5558:

$$K = \left[\begin{array}{cccc} -69.05 & -287.3 & -251.8 & 1.369\times10^{5} \\ 2.11 & -9.476 & -5.485 & 2730 \\ -6.041 & -36.74 & -33.57 & 1.641\times10^{4} \\ 436.8 & -1673 & 2490 & -3.656\times10^{6} \\ \hline 0.5733 & -1.437 & -0.3474 & -928.5 \\ 74.58 & 313 & 275 & -1.499\times10^{5} \\ 0.1285 & -0.7374 & -0.9788 & -502.9 \end{array}\right.$$

$$\left.\begin{array}{ccc} 34.04 & 30.11 & 2.647 \\ 1.708 & 1.635 & -0.1548 \\ 4.269 & 4.046 & 0.3535 \\ 3860 & 3435 & -169.9 \\ \hline 0.4981 & 0.5697 & 0.08769 \\ -36.88 & -33.02 & -2.942 \\ -0.6163 & 0.4417 & -0.07587 \end{array}\right] .$$

VIII. CONCLUSION

No studies have ever tried to analyze and design safety integrity of a control law probabilistically. We should draw attention not only to the importance of the presented assessment and management framework according to IEC 61508 but also to its contribution to further theoretical advance in reliable control theory.

REFERENCES

[1] T. Asai, S. Hara and T. Iwasaki, "Simultaneous parametric uncertainty modeling and robust control synthesis by LFT-scaling," *Automatica*, Vol.36, pp.1457–1467, 2000.

[2] E. J. Henley and H. Kumamoto, *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*, IEEE Press, 1992.

[3] *IEC 61165: Application of Markov techniques*, 2006.

[4] *IEC 61508: Functional safety of electrical/electronic/ programmable electronic safety related systems*, 1998–2000.

[5] *ISO/IEC Guide 51: Guidelines for the inclusion of safety aspects in standards*, 2nd edition, 1999.

[6] K. Suyama, "Systematization of reliable control," *Proc. 2002 ACC*, pp.5110–5118, 2002.

[7] K. Suyama, "Safety integrity analysis framework for a controller according to IEC 61508," *Proc. 42nd IEEE CDC*, pp.2477–2483, 2003.

[8] K. Suyama, "Controller design using safety performance index according to IEC 61508," *Proc. 2004 ACC*, pp.1811–1816, 2004.

[9] K. Suyama, "Probabilistic safety assessment and management of control laws," *Proc. 2005 ACC*, pp.2232–2238, 2005.