FUNCTIONAL SAFETY ANALYSIS OF SAFETY-RELATED SYSTEMS USING MAJORITY DECISION ACCORDING TO IEC 61508

K. Suyama

Tokyo University of Mercantile Marine, Japan suyama@ipc.tosho-u.ac.jp

Keywords: control system, majority decision, functional safety, IEC 61508.

Abstract

This paper analyzes functional safety of a safety-related system using majority decision to evaluate its safety integrity according to the international safety standard, IEC 61508. This analysis is one of the most valuable concrete examples indispensable for system safety design according to IEC 61508.

1 Introduction

Over the past decade the social environment surrounding system safety has changed rapidly[1]. One epoch was that TC65 WG9&10 in IEC, International Electrotechnical Commission, established an international standard, IEC 61508[3]. It is applied to almost all electrical / electronic / programmable electronic (E/E/PE) safety-related systems (SRSs). It has been already quoted into several national standards or guidelines of UK, USA and Japan, including those for process, aerospace and railway transportation sectors.

Sensors in a control system break down more frequently than actuators or controllers, and sensor failures are likely to bring about more serious situations than actuator failures or controller failures. From a practical viewpoint, it is important to realize safety function against sensor failures in a control system by considering simultaneously fault detection and emergency measures in a unified framework. The author has presented such a framework, i.e., a safety-related system against sensor failures consisting of the following aspects [5, 6, 7]:

(a) reliable stability against sensor failures using a decision rule which functions as majority decision among redundant sensors, and
(b) fault detection for redundant sensors.

The decision rule itself has been often used in various scenes until now. However it has not been clarified theoretically that the decision rule functions as majority decision in fault cases. Its functional safety, one of the most important concepts in IEC 61508, was firstly analyzed in [7], where especially detection was evaluated from a viewpoint of a stand-by safety-related system in low demand mode of operation, i.e., average probability of failure to perform its design function on demand.

For the last several years, the importance of safety function realized in a control system has been growing. One of the reasons is that ISO / IEC Guide 51 (E) [4] adopted newly risk for environment and risk for properties as its scope. It is widely known that there are many cases where safety-related systems are not enough to reduce the risk for environment/properties. This safety-related system is regarded highly as one of the key techniques for realizing safety function in a control system.

Under such social environment surrounding system safety, this paper analyzes the functional safety of the safety-related system according to the policy of the IEC 61508 to evaluate its safety integrity in continuous mode of operation, i.e., probability of a dangerous failure per hour. This analysis is one of the most valuable concrete examples indispensable for system safety design according to IEC 61508.

2 Safety-related system using majority decision

The primary control system is shown in Figure 1, where the controlled object is called an equipment under control (EUC) in IEC 61508. A basic control system (BCS) includes a control logic, sensors such as Sensor *i* and actuators.

Suppose that a sensor measuring the output $y_i(t)$ of a controlled object is susceptible to failures, and that the primary control system cannot be stable, i.e., it falls into a dangerous state, without the correct information on $y_i(t)$.

The hazard considered here is that the control system falls into an unstable and dangerous state by failures in sensors measuring $y_i(t)$. Its probabilistic occurrence leads to a risk.

The primary control system has only one sensor measuring $y_i(t)$, Sensor $i(j)$, which has a great risk of the hazard.

We install Safety-Related System (SRS) *i* as shown in Figure 2 to reduce the (initial) risk of the primary control system so that the residual risk of the overall system is less than the predetermined tolerable risk level. That is, SRS *i* reduces the probability that the hazard occurs. SRS *i* consists of four parts, Sensor set *i*, Decision part *i*, Detection part *i*, and Override *i*.

2.1 Sensor set

Sensor set *i* consists of three sensors, Sensor $i(1)$, Sensor $i(2)$ and Sensor $i(3)$, which are in operation for measuring $y_i(t)$ with a sampling period T_s simultaneously and independently. Each Sensor $i(j)$ $(j = 1,2,3)$ presents its measured value $y_{i(j)}[k]$ for $y_i(kT_s)$ at the *k*-th sampling-time, $t = kT_s$.

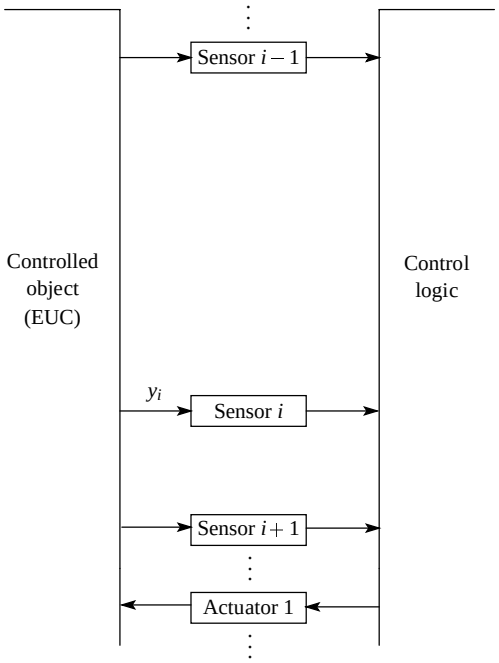

Figure 1. Primary control system.

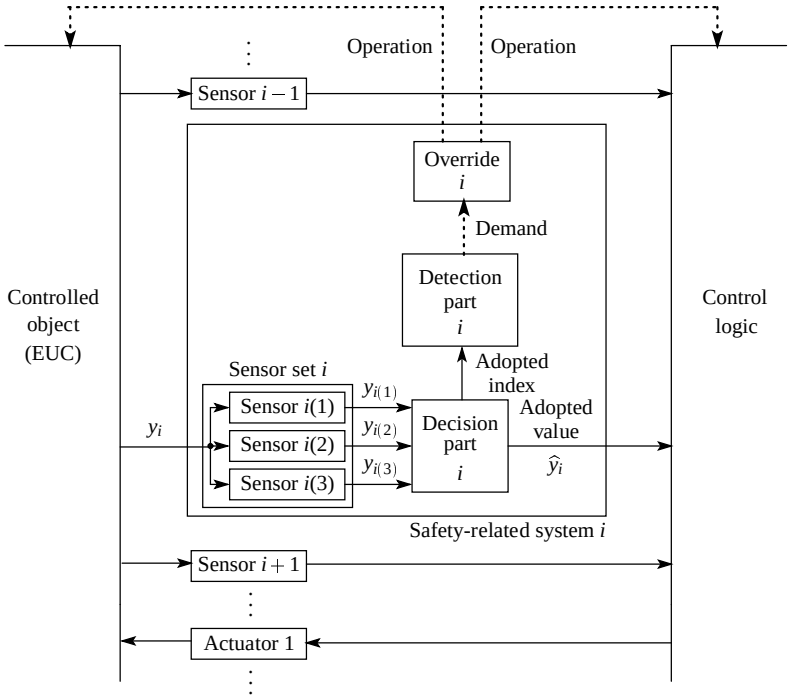

Figure 2. Control system with SRS i using majority decision.

A measured value from a normal sensor is represented by

$$y_{i(j)}[k] = y_i(kT_s) + \rho_{i(j)}[k] + \omega_{i(j)}[k].$$

A bounded systematic error $\rho_{i(j)}[k]$ can be corrected in general. On the other hand, an accidental error $\omega_{i(j)}[k]$ causes probabilistic dispersion, which cannot be corrected. It is usually assumed that $\omega_{i(j)}[k]$ follows a normal probability distribution $N(\mu_{i(j)}, \sigma^2_{i(j)})$ where $|\mu_{i(j)}|, \sigma^2_{i(j)} < \infty$.

Assumption 1: $\rho_{i(j)}[k] = 0, \quad \mu_{i(j)} = 0, \quad \sigma_{i(j)} = \sigma_i$.

Suppose that when a sensor is in a fault, its measured value is only white noise as follows:

$$y_{i(j)}[k] = \omega'_{i(j)}[k]$$

where $\omega'_{i(j)}[k]$ follows $N(\mu'_{i(j)}, \sigma'^2_{i(j)})$ $(|\mu'_{i(j)}|, \sigma'^2_{i(j)} < \infty)$.

Assumption 2: $\mu'_{i(j)} = 0, \quad \sigma'_{i(j)} = \sigma_i$.

Assumption 3: Failure occurrences in the three sensors in Sensor set i are probabilistically independent of each other.

2.2 Decision part

In Decision part i, the intermediate value of the three measured values in Sensor set i, $y_{i(1)}[k], y_{i(2)}[k]$ and $y_{i(3)}[k]$, is adopted as $\widehat{y}_i[k]$. That is, at the k-th sampling time $t = kT_s$, if

$$y_{i(j_1)}[k] \le y_{i(j_2)}[k] \le y_{i(j_3)}[k],$$

the adopted value is

$$\widehat{y}_i[k] = y_{i(j_2)}[k].$$

Only $\widehat{y}_i[k]$ is used in a control part. The rest two measured values at $t = kT_s$ are not used.

Decision part i also notifies Detection part i, whose measured value is adopted as follows at each sampling time:

$$s_i[k] = j_2.$$

When one sensor in Sensor set i is in a fault, Decision part i does not always adopt a correct measured value from one of two normal sensors in the set because of the stochastic variables $\omega_{i(j)}[k], \omega'_{i(j)}[k]$. However the incorrect information from the failed sensor is unlikely to be used as majority decision, the stability and the performance in the normal case can suppress the instability caused by the sensor failure as shown in [6]. That is, the stability and the performance can be maintained against single sensor faults without their explicit and urgent detection.

2.3 Detection part

Detection of sensor faults is needed for avoiding more than one faults in Sensor set i. When two sensors in Sensor set i are in faults, the probability that Decision part i adopts the incorrect information from one of the two failed sensors tends to one, and hence we assume the following.

Assumption 4: Failures in two sensors will result in the control system falling into an unstable and dangerous state.

Detection part i judges whether or not all of the sensors in Sensor set i are in normal operation every sampling-time, which is derived from making the best use of the characteristics of the decision rule. Paying attention to the change of decision result, Detection part i judges whether or not one or more sensors in

Sensor set i are in faults by using the χ^2-goodness-of-fit test.

Let $\chi^2(\alpha)$ denote α-point of the χ^2-distribution with two degrees of freedom, where α means the significant level. For example, $\chi^2(5\%) = 5.99$ and $\chi^2(1\%) = 9.21$.

Detection algorithm:
Step 1: Out of N data of s_i, i.e., the latest $N-1$ data, $s_i[k-N+1],\ldots,s_i[k-1]$, in the memory and the current data $s_i[k]$, let $n_{i(j)}[k]$ denote the number of k' such that $s_i[k'] = j$.
Step 2:

$$\gamma_i[k] = \frac{3}{N}\sum_{j=1}^{3}\left(n_{i(j)}[k] - \frac{N}{3}\right)^2. \tag{1}$$

Step 3: If $\gamma_i[k] \le \chi^2(\alpha)$, the judgment is "all the sensors in Sensor set i are in normal operation at $t = kT_s$." Delete $s_i[k-N+1]$ from the memory, and save $s_i[k]$. If $\gamma_i[k] > \chi^2(\alpha)$, the judgment is "one or more sensors in Sensor set i are in faults at $t = kT_s$." Detection part i notifies Override i immediately.

Under Assumption 1, if all of the sensors in Sensor set i are in normal operation at the sampling time $t = kT_s$,

$$\text{Probability}\{s_i[k] = j\} = \frac{1}{3}, \quad j = 1,2,3.$$

Then $(n_{i(1)}[k], n_{i(2)}[k], n_{i(3)}[k])$ follows a multinomial distribution with $p_1 = p_2 = p_3 = \frac{1}{3}$. On the other hand, if Sensor $i(j)$ is in a fault at $t = kT_s$,

$$\begin{aligned}&\text{Probability}\{s_i[k] = j\}\\ &< \frac{1}{2}\left[1 - \sqrt{1 - e^{-\frac{[y_i(kT_S)]^2}{4\sigma_i^2}}}\right]\left[1 + \sqrt{1 - e^{-\frac{[y_i(kT_S)]^2}{2\sigma_i^2}}}\right]\end{aligned} \tag{2}$$

(see [6]). Then $(n_{i(1)}[k], n_{i(2)}[k], n_{i(3)}[k])$ follows another multinomial distribution. It can be judged by the χ^2-goodness-of-fit test as in Detection algorithm.

The number of data N should be taken sufficiently large so that $N \ge 30$ for the sufficient approximation of the distribution of $\gamma_i[k]$ by the χ^2-distribution.

2.4 Override

When Detection part i judges that one or more sensors in Sensor set i are in faults, the information operates Override i immediately. Then Override i achieves or maintains a safe state for the control system.

In this paper Override i is not specified because it depends highly on the individual factor of the controlled object.

Note that Override i is a stand-by system operating only in case of need. If there is a hidden failure in Override i, sufficient emergency measures are not taken. Hence it is assumed without loss of generality that its functional safety is analyzed by itself in low-demand mode of operation.

Assumption 5: The average probability of failure to perform its design function on demand of Override i, P_{O_i}, is known.

In addition, it is assumed that any hazardous event does not occur even if Override i operates in the normal case.

3 Functional safety analysis

The functional safety of SRS i is its ability to perform the safety function against the hazard, i.e., failures in the sensors measuring the output $y_i(t)$. Because Sensor set i and Decision part i are indispensable for control, it is reasonable to consider that SRS i operates continuously in the BCS. The functional safety should be analyzed in continuous mode of operation according to IEC 61508. We should evaluate the safety integrity of the overall system including SRS i shown in Figure 2, i.e., the probability that the hazard occurs per hour in the overall system.

Assume the following.

(a) Preventive maintenance can restore sensors to their original state.

(b) Preventive maintenance is carried out at $t = 0$ and at $t = T_{pm}$.

(c) Sensor set i consists of identical sensors. That is, Sensors $i(1)$, $i(2)$, $i(3)$ in Figure 2 (and Sensor $i(j)$ in Figure 1) are identical.

The last is not only for simplicity but also for impartiality.

Assumption 6: Failure time of the sensors in Sensor set i follows an exponential distribution with density function

$$f_i(\tau) = \lambda_i e^{-\lambda_i \tau}$$

where λ_i denotes the (constant) failure rate.

In the primary control system shown in Figure 1, if Sensor $i(j)$ fails, then the hazard occurs. Its probability per one preventive maintenance interval is

$$\int_0^{T_{pm}} f_i(\tau)d\tau = \int_0^{T_{pm}} \lambda_i e^{-\lambda_i\tau}d\tau = 1 - e^{-\lambda_i T_{pm}}.$$

Then, in the primary control system, the mean probability per hour that the hazard occurs, i.e., hazard rate, is

$$HR_{pri} = \frac{1 - e^{-\lambda_i T_{pm}}}{T_{pm}}.$$

For example, if $\lambda_i = 10^{-4}[1/\text{hour}]$ and $T_{pm} = 10^4[\text{hour}]$, then

$$HR_{pri} = 6.3 \times 10^{-5}[1/\text{hour}].$$

This cannot be accepted from a practical viewpoint. In fact, according to the SILs in continuous mode of operation in IEC 61508 where a hazard rate is equal to a dangerous failure rate, IEC 61508 does not provide the primary control system any Safety Integrity Levels (SILs).

3.1 Fault tree analysis

In the system with SRS i shown in Figure 2, when two sensors in Sensor set i are in faults, the probability that Decision part i adopts the incorrect information from one of the two failed

sensors tends to one, and hence it is assumed that failures in two sensors will result in the control system falling into an unstable and dangerous state.

The fault tree shown in Figure 3 illustrates the following two scenarios where the hazard and the hazardous situation occur. Note that priority AND gates are used, where output event occurs if all input events occur in the order from left to right [2].

Scenario 1:

1. The primary failure occurs in Sensor set *i*.
2. The secondary failure occurs in Sensor set *i* before Detection part *i* detects the fault caused by the primary failure and before the next preventive maintenance.

Scenario 2:

1. The primary failure occurs in Sensor set *i*.
2. Detection part *i* detects the fault caused by the primary failure and demands operation of Override *i*.
3. Because there are hidden failures in Override *i*, no urgent measures are taken against the fault caused by the primary failure.
4. The secondary failure occurs in Sensor set *i* before the next preventive maintenance.

Then, in the system with SRS *i*, the mean probability per hour that the hazard occurs, i.e., hazard rate, is

$$HR = \frac{P_{S1} + P_{S2}}{T_{pm}}. \tag{3}$$

3.2 Evaluation of detection

The possible errors of Detection part *i* are the following two:

Type I error: although all of the sensors in Sensor set *i* are in normal operation, the judgment is "one or more sensors are in faults."

Type II error: although one or more sensors are in faults, the judgment is "all the sensors are in normal operation," i.e., Detection part *i* misses the fault.

It follows from the property of the χ^2-goodness-of-fit test that the probability of a type I error is less than the significant level α used in Detection algorithm. As shown in the fault tree in Figure 3, a type I error has no relation with the hazard considered in this paper. On the other hand a type II error is related with Scenario 1. Hence its probability should be evaluated.

Suppose that only one sensor, Sensor $i(j)$, is in a fault at the sampling time $t = kT_s$, and that it failed before $t = (k-N)T_s$, i.e., the memory for $s_i[k]$ stores only data in the fault case. Taking (2) into consideration, suppose that

$$\text{Probability}\{s_i[k] = j\} = \varepsilon_i \left(\ll \frac{1}{3} \right)$$

$$\text{Probability}\{s_i[k] = j'(\neq j)\} = \frac{1-\varepsilon_i}{2}.$$

In general ε_i depends on $|y_i(kT_s)|$, and it should be written as $\varepsilon_i[k]$. However, we regard $\varepsilon_i[k]$ as a sufficiently constant ε_i because Probability$\{s_i[k] = j\}$ is sufficiently small if $|y_i(kT_s)| \gg \sigma_i$. Then $\gamma_i[k]$ in (1) follows the non-central χ^2-distribution with two degrees of freedom and its non-centrality:

$$\phi_i = 3N \left[2 \left(\frac{1-\varepsilon_i}{2} - \frac{1}{3} \right)^2 + \left(\varepsilon_i - \frac{1}{3} \right)^2 \right].$$

Let $\chi^2_{\phi_i}$ denote such a statistic. Then the power is given by

$$\beta_i = \text{Probability}\{\chi^2_{\phi_i} > \chi^2(\alpha)\}, \tag{4}$$

which is the probability that when a sensor is in a fault, Detection part *i* can detect it. Then the probability of a Type II error is less than $1 - \beta_i$.

For example, suppose that $N = 30$, $\alpha = 1\%$. In the region $|y_i(kT_s)| > 5\sigma_i$, we can have Probability$\{s_i[k] = j\} < 0.001 (= \varepsilon_i)$. Then, by numerical calculation of (4), we can have $\beta_i \geq 0.999$ in this region. The probability of a type II error that Detection part *i* misses the fault is less than 0.1% if more than *N* steps have passed since its occurrence.

Note that this evaluation presents the probability of an error at each sampling time, and that Detection part *i* operates every sampling time. Even if the probability of a type II error is more than 1%, the probability that it repeats the errors and misses the fault for several steps is extremely small.

3.3 Scenario 1

The probability that Scenario 1 occurs in one preventive maintenance interval is given by

$$P_{S1} = \int_0^{T_{pm}} P_{S1,1}(\xi) P_{S1,2}(\xi) d\xi \tag{5}$$

where $P_{S1,1}(\xi)$ and $P_{S1,2}(\xi)$ are the following probability density and probability:

$$\begin{aligned} P_{S1,1}(\xi) &= \text{Probability density}\{\text{Primary failure occurs} \\ &\qquad \text{at } t = \xi (\in [0, T_{pm}])\} \\ P_{S1,2}(\xi) &= \text{Probability}\{\text{Secondary failure occurs} \\ &\qquad \text{before Detection part } i \text{ detects} \\ &\qquad \text{fault caused by primary failure} \mid \\ &\qquad \text{Primary failure occurs at } t = \xi\}. \end{aligned}$$

Here we can easily have

$$P_{S1,1}(\xi) = 3 f_i(\xi) [\Gamma(\xi)]^2 \tag{6}$$

where

$$\Gamma(\xi) = \int_\xi^\infty f_i(\tau) d\tau.$$

From now, we evaluate the probability $P_{S1,2}(\xi)$.

Take a new time axis by $\tau = t - \xi$. The primary failure occurs at $\tau = 0$. The last preventive maintenance was carried out at $\tau = -\xi$, and the next preventive maintenance will be carried out at $\tau = T_{pm} - \xi$. Suppose that the earliest sampling time

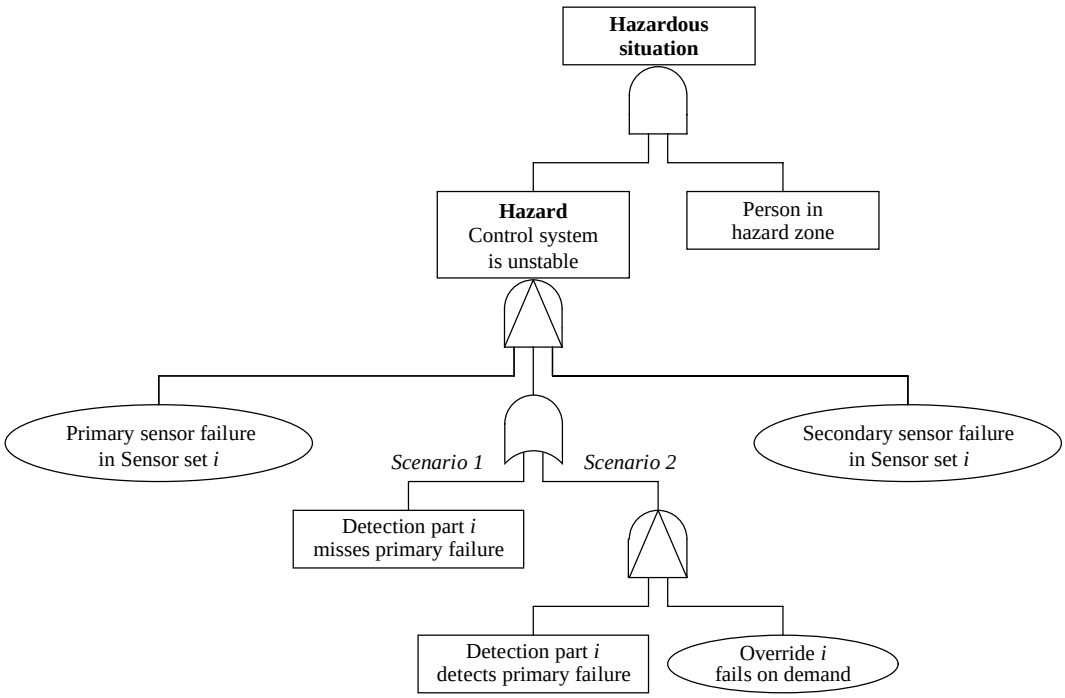

Figure 3. Fault tree to the hazardous situation.

after $\tau = 0$ is $\tau = mT_s,\ 0 \le m < 1$. For simplicity, let $\tau = (k' + m)T_s,\ k' = 0,1,\ldots$, denote the sampling time after $\tau = 0$.

We assume that Detection part i can not detect the fault caused by the primary failure within N steps after its occurrence, i.e., if data used in Fault detection algorithm include data in the normal case. (This is a conservative assumption because Detection part i can do within N steps if the multinomial distribution after the primary failure drastically changes from the normal-case one [6].) That is, it cannot do until $\tau = (N-1+m)T_s$.

Then we have

$$\begin{aligned}
&P_{S1,2}(\xi) \\
&\le \left[\frac{1}{\Gamma(\xi)}\int_0^{(N-1+m)T_s} f_i(\tau+\xi)d\tau\right] \\
&\qquad \times \left[\frac{1}{\Gamma(\xi)}\int_0^{(N-1+m)T_s} f_i(\tau+\xi)d\tau \right. \\
&\qquad\qquad \left. + \frac{2}{\Gamma(\xi)}\int_{(N-1+m)T_s}^{\infty} f_i(\tau+\xi)d\tau\right] \\
&\quad + \sum_{k'=N-1}^{[(T_{pm}-\xi)/T_s-m]} \left[\prod_{j=N-1}^{k'}(1-\beta_i[j])\right] \\
&\qquad \times \left[\frac{1}{\Gamma(\xi)}\int_{(k'+m)T_s}^{(k'+1+m)T_s} f_i(\tau+\xi)d\tau\right] \\
&\qquad \times \left[\frac{1}{\Gamma(\xi)}\int_{(k'+m)T_s}^{(k'+1+m)T_s} f_i(\tau+\xi)d\tau \right. \\
&\qquad\qquad \left. + \frac{2}{\Gamma(\xi)}\int_{(k'+1+m)T_s}^{\infty} f_i(\tau+\xi)d\tau\right] \qquad (7)
\end{aligned}$$

where the Gauss's symbol is used in $[(T_{pm}-\xi)/T_s - m]$. Note that $1-\beta_i[k']$ denotes the probability of a type II error at the k'-th sampling time, $\tau = (k'+m)T_s$. The first term in the right-hand side of (7) represents the probability that one or two failures occur within N steps after the primary failure. We should pay attention to conditional probabilities because under the condition that failures do not occur in the rest sensors at the primary failure, $t = \xi$. The second term in the right-hand side of (7) represents the probability that one or two failures occur while Detection part i misses the fault caused by the primary failure, i.e., it repeats type II errors after $k' = N-1$.

Assumption 7: $1-\beta_i[k'] \le \bar{\beta}_i, \quad k' = N-1, N, \ldots$

Under this assumption for technical simplicity,

$$P_{S1,2}(\xi) < \frac{2e^{-2\lambda_i\xi}}{[\Gamma(\xi)]^2}\left[1 - e^{-\lambda_i NT_s} + \frac{\bar{\beta}_i\lambda_i T_s}{1-\beta_i e^{-2\lambda_i T_s}}\right]. \qquad (8)$$

Note that $\bar{\beta}_i$ depends on N, α. The equation (8) does not depend on m because failure time of the sensors in Sensor set i follows the exponential distribution with the (constant) failure rate.

Hence, using (8) and (6) in (5),

$$P_{S1} < 2(1-e^{-3\lambda_i T_{pm}})\left[1 - e^{-\lambda_i NT_s} + \frac{\bar{\beta}_i\lambda_i T_s}{1-\beta_i e^{-2\lambda_i T_s}}\right]. \qquad (9)$$

For example, in the region $|y_i(kT_s)| > 5\sigma_i$, if $N = 30$ and $\alpha = 1\%$, we can take $\bar{\beta}_i = 0.001$ by the example in Section 3.2. Further, if $T_s = 1$[min], $\lambda_i = 10^{-4}$[1/hour] and $T_{pm} = 10^4$[hour], then $P_{S1} < 9.5 \times 10^{-5}$.

3.4 Scenario 2

The probability that Scenario 2 occurs in one preventive maintenance interval is given by

$$P_{S2} = \int_0^{T_{pm}} P_{S2,1}(\xi) \int_\xi^{T_{pm}} P_{S2,2}(\xi,\xi') P_{O_i} P_{S2,3}(\xi,\xi') d\xi' d\xi$$

where $P_{S2,1}(\xi)$, $P_{S2,2}(\xi,\xi')$ and $P_{S2,3}(\xi,\xi')$ are the following probability densities and probability:

$$\begin{aligned}
P_{S2,1}(\xi) &= \text{Probability density}\{\text{Primary failure occurs} \\
&\qquad \text{at } t = \xi (\in [0, T_{pm}])\} \\
P_{S2,2}(\xi,\xi') &= \text{Probability density}\{\text{Detection part } i \\
&\qquad \text{detects fault caused by primary} \\
&\qquad \text{failure at } t = \xi' (\in (\xi, T_{pm}]) \mid \\
&\qquad \text{Primary failure occurs at } t = \xi\} \\
P_{S2,3}(\xi,\xi') &= \text{Probability}\{\text{Secondary failure occurs} \\
&\qquad \text{after } t = \xi' \mid \\
&\qquad \text{Primary failure occurs at } t = \xi\}.
\end{aligned}$$

Taking the extremely small probability of missing the fault caused by the primary failure as shown before into consideration, we can evaluate as follows:

$$\int_0^{T_{pm}} P_{S2,1}(\xi) \int_\xi^{T_{pm}} P_{S2,2}(\xi,\xi') P_{S2,3}(\xi,\xi') d\xi' d\xi < P_{S2,4}$$

where

$$P_{S2,4} = \text{Probability}\{\text{More than one failures occur in } [0, T_{pm}]\}.$$

The probability that a sensor fails in $[0, T_{pm}]$ is given by

$$\int_0^{T_{pm}} f_i(x) dx = 1 - e^{-\lambda_i T_{pm}}.$$

Under Assumption 3, we easily have

$$P_{S2,4} = 3(1 - e^{-\lambda_i T_{pm}})^2 e^{-\lambda_i T_{pm}} + (1 - e^{-\lambda_i T_{pm}})^3.$$

Hence

$$P_{S2} < (1 - e^{-\lambda_i T_{pm}})^2 (1 + 2e^{-\lambda_i T_{pm}}) P_{O_i}. \qquad (10)$$

For example, if $\lambda_i = 10^{-4}[1/\text{hour}]$, $T_{pm} = 10^4[\text{hour}]$ and $P_{O_i} = 5.0 \times 10^{-5}$, then $P_{S2} < 3.5 \times 10^{-5}$.

3.5 Safety integrity

From (3),(9) and (10), the hazard rate in the system with SRS i is evaluated by

$$\begin{aligned}
HR < \frac{1}{T_{pm}} \Bigg[& 2(1 - e^{-3\lambda_i T_{pm}}) \left(1 - e^{-\lambda_i N T_s} + \frac{\bar{\beta}_i \lambda_i T_s}{1 - \beta_i e^{-2\lambda_i T_s}} \right) \\
& + (1 - e^{-\lambda_i T_{pm}})^2 (1 + 2e^{-\lambda_i T_{pm}}) P_{O_i} \Bigg]
\end{aligned}$$

For example, if $|y_i(kT_s)| > 5\sigma_i$, $N = 30$, $\alpha = 1\%$, $T_s = 1[\text{min}]$, $\lambda_i = 10^{-4}[1/\text{hour}]$, $T_{pm} = 10^4[\text{hour}]$ and $P_{O_i} = 5.0 \times 10^{-5}$, then

$$HR < 1.3 \times 10^{-8}[1/\text{hour}].$$

Hence, according to the SILs in continuous mode of operation in IEC 61508, where a hazard rate is equal to a dangerous failure rate, the system with SRS i has the SIL of 3 (see Table 1).

Table 1: SILs in high demand / continuous mode of operation.

SIL	Probability of a dangerous failure per hour
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 $< 10^{-5}$

4 Conclusions

The analysis in this paper is one of the most valuable concrete examples indispensable for system safety design according to IEC 61508 because few examples have been presented until now. A great deal of effort in the field of control theory will be made on safety analysis especially based on international standards such as IEC 61508.

References

[1] Health & Safety Executive (HSE). *Out of Control — Why control systems go wrong and how to prevent failure*, HSE Books, 1995.

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

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

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

[5] K. Suyama. "A New Type Reliable Control System Using Decision by Majority," *Proc. 1997 ACC*, pp. 52–56, 1997.

[6] K. Suyama. "Fault Detection of Redundant Sensors Used in Reliable Sampled-Data Control Systems," *Proc. 37th IEEE CDC*, pp. 1161–1164, 1998.

[7] K. Suyama. "Functional safety analysis of reliable control systems using decision by majority," *Proc. 1999 ACC*, pp. 618–621, 1999.

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