

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

185,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Risk Assessment and Functional Safety Analysis to Design Safety Function of a Human-Cooperative Robot

Suwoong Lee<sup>1</sup> and Yoji Yamada<sup>2</sup>

<sup>1</sup>*Yamagata University*

<sup>2</sup>*Nagoya University  
Japan*

## 1. Introduction

Human-cooperative robots (HCRs) are expected to benefit various industries, and many studies related to physical human-robot interactions have been conducted (Moore et al., 2003; Kim et al., 2005; Tsuji et al. & Tanaka, 2005); some HCRs have been gradually introduced in manufacturing and welfare fields. For instance, power-assist systems in manufacturing assist workers in carrying heavy modular parts to the target site (Konosu & Yamada, 2003; Santos et al., 2010). In the welfare field, power-assisted meal-carrying carts enable caregivers to move numerous dishes at once (Fujiwara et al., 2002), and electro-hybrid wheelchairs make it easier for caregivers to move a person with weakened leg muscles (Seki et al., 2006).

Safety is regarded as a critical issue for HCRs. In particular, safety functions that can bring HCRs to a safe state in an emergency are essential because their hazardous movement may cause serious injuries to operators. The reliability of the safety functions must be sufficiently high in response to the estimated risk. Therefore, it is important to predetermine the required safety level for a HCR, to design a suitable safety function that ensures this safety level, and to analyze the validity of safety-function design.

Several attempts have been made to develop safety-design methodologies for HCRs in the related research fields. Ogorodnikova integrated several approaches related to risk estimation and safety design for a human-centered robotic work cell (Ogorodnikova, 2008). Kazanzides reported a tutorial overview of safety design for medical robots with a discussion of high-level safety requirements and methods for risk assessment (Kazanzides, 2009). Guiochet et al. studied a model-based, user-centered risk assessment that estimates the associated risks of an HCR (Guiochet et al., 2010). However, these studies mainly introduce methodologies for the overall safety design for HCRs, especially focusing on the inherent safety design, and do not present details on safety-function design involving validity analysis. On the other hand, Laible et al. studied safety-function design with a multichannel voting architecture that is based on the top-down risk assessment of an HCR (Laible et al., 2004). Okada et al. reported an example of the application of international safety-standard concepts to a robot cell-production system and showed that safety devices can be effectively used within a safety architecture (Okada et al., 2007). Nakabo et al. developed an integrated

safety-function module for an HCR, which is designed to be compliant with international safety standards (Nakabo et al., 2009). However, these studies neither predetermine the safety level required by the system nor assess whether the designed safety functions match the requirement. An established safety-function design for HCRs has become a very important issue, but a methodology involving the validity analysis of safety-function design has not yet been examined.

IEC 61508, an international standard of safety-critical systems, has been gradually introduced in various industrial fields that adopt programmable controllers (IEC 61508 Technical Committee, 1998; 2002). This standard is concerned with functional safety, which is a part of the overall safety that depends on a system or equipment operating correctly in response to its inputs, and provides guidelines for not only determining the required safety-integrity level (SIL) but also analyzing the validity of safety-related system (SRS) design.

Therefore, we consider a methodology for safety-function design involving risk assessments and a functional safety analysis based on IEC 61508; this chapter introduces a case study that focuses on the system failures of an HCR in order to propose this methodology. The details of the methodology for Skill-Assist, an HCR we adopted as a platform system, are described in this chapter. Section 2 describes the outline of the Skill-Assist, and Section 3 explains the SIL determination for the Skill-Assist and risk assessments of the system failures. Section 4 describes an SRS designed on the basis of the risk-assessment results and the functional safety analysis of the SRS. The proposed methodology for safety-function design is discussed in Section 5, and the conclusion is presented in Section 6.

## 2. Skill-Assist

Figure 1 shows performing a task with Skill-Assist. Skill-Assist is a power assist system which is able to allow the operator to perform his/her task without disturbing the human skill by varying the virtual mechanical impedance (Konosu & Yamada, 2003). The Skill-Assist has been introduced in automobile assembly lines of a motor company, and is also expected to be applied to welfare field. Figures 2 presents the schematic overview of Skill-Assist. Skill-Assist has three degrees of freedom (DOF) and can move in transverse, traveling, and elevated directions using electric-powered actuators installed on lanes. The displacement and velocity of Skill-Assist are recorded using pulse linear encoders (Numerik JENA, RIA-22) attached to the lanes. An operator grips the lever of analog-type force sensor (Nitta, IFS-100M40A50-I63) and can maneuver the end effector of Skill-Assist to pick up and move the workload. The control computer (Advantech, IPC-610) of Skill-Assist processes sensor signals for impedance control, generates analog command signals with a D/A converter (Interface, PCI-3310), and drives the actuators using AC servo controllers (Mitsubishi, MR-J2S-40AS).

As fundamental safety measures, an enable switch is attached to the lever of the force sensor and an emergency stop switch is within close reach of the operator. Signal logic around the control system and power supply to actuators is managed by a programmable logic controller (PLC, Keyence, KV series). When the enable switch is not pushed or the emergency stop switch is pushed, the PLC disables the contactor (Mitsubishi, SD-Q19) to shut down the power supply and activates the regenerative brake (Mitsubishi, MR-RB12) simultaneously to bring Skill-Assist to a halt. Overcurrent, overheat, and openload protective functions are incorporated in the AC servo controllers.



Fig. 1. Performing a task with Skill-Assist

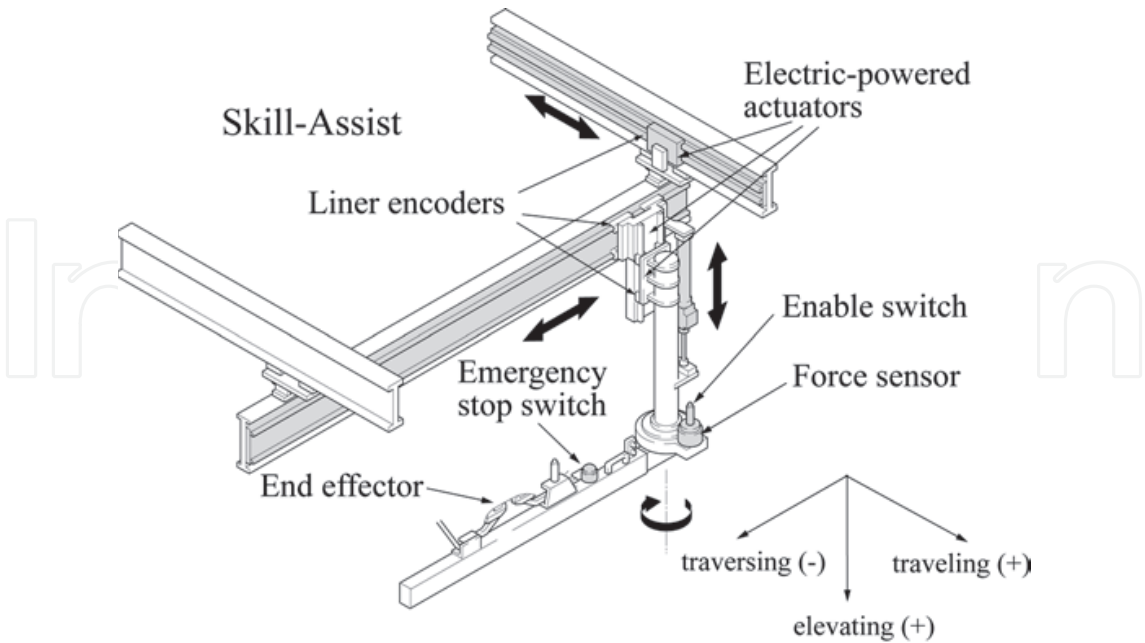


Fig. 2. Schematic overview of Skill-Assist

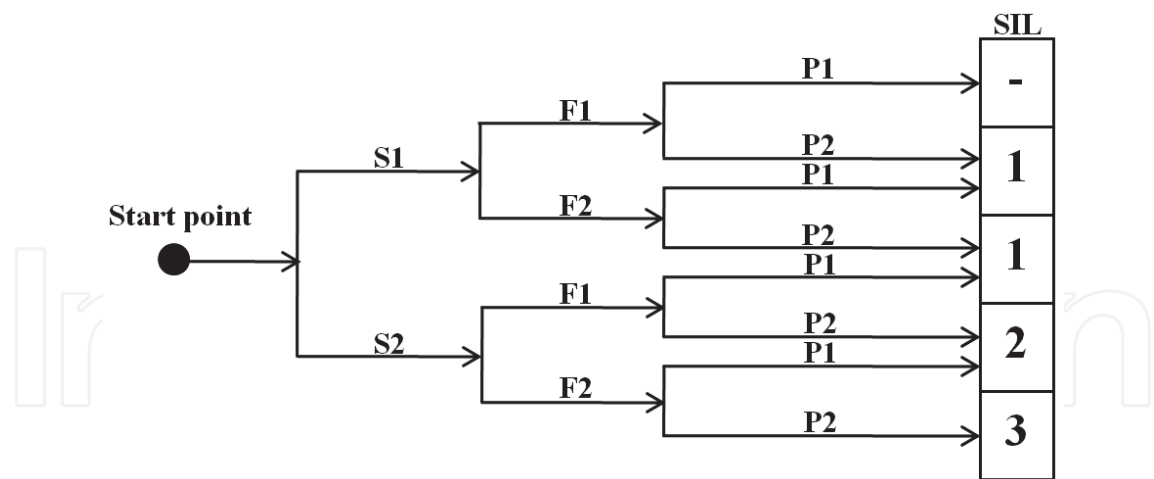


Fig. 3. Risk graph for determining required SIL

3. SIL determination and risk assessment

3.1 SIL determination for Skill-Assist

As the first step in the proposed safety-function design process, we determine the SIL for the Skill-Assist. SIL is defined in (IEC 61508 Technical Committee, 1998) as a relative level of risk reduction provided by a safety function, which is represented by SIL-1, SIL-2, SIL-3, and SIL-4. The most dependable level is SIL-4, which is required for an aircraft or a train, where catastrophic accidents can occur if the SRS fails. In general, the target SIL required for a system is determined by a qualitative or quantitative method; we use a risk graph, which is a qualitative method, for determining the target SIL from the information on risk factors (IEC 61508 Technical Committee, 1998). Fig. 3 shows the risk graph adopted in the proposed methodology and also used in the risk evaluation of a human-robot collaborative system (Behnisch, 2008; ISO Technical Committee 114, 2006). The risk graph is initiated at the start point on the left side and is implemented on the basis of risk parameters such as the severity of injury (S1, S2); the frequency of exposure to hazards (F1, F2); and the possibility of avoiding a hazard (P1, P2). The selection of the risk parameters leads to one of the five outputs on the right side, and the number at each output indicates the required SIL that must be achieved by the SRS.

3.1.1 Severity of injury (S1, S2)

S1 and S2 indicate "normally reversible injury" and "normally irreversible injury", respectively. Considering horizontal inertia (202 kg) and maximum velocity (1.43 m/s) of Skill-Assist, based on the results mentioned in (Haddadin et al., 2009), crushing or collision caused by its hazardous movement may result in a fracture-level or a serious permanent injury at worst. Hence, we select parameter S2 at the start point.

3.1.2 Frequency of exposure to hazards (F1, F2)

F1 and F2 indicate "seldom-to-less-often" and "frequent-to-continuous", respectively. A work-space that includes the Skill-Assist can be regarded as a hazardous zone because the operator usually makes contact with the Skill-Assist while conducting tasks. Therefore, it

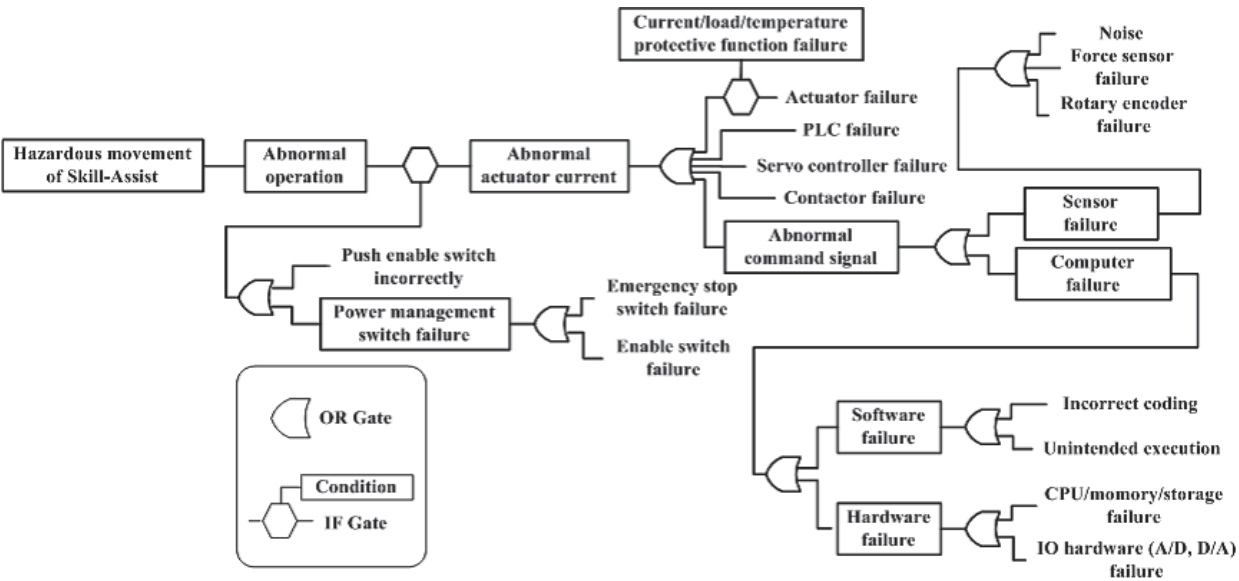


Fig. 4. Simplistic version of FTA that focuses on potential system failures

seems reasonable to assume that the operator is always exposed to the hazardous zone, and thus, we select parameter *F2* at the second branch point.

3.1.3 Possibility of avoiding hazard (*P1*, *P2*)

*P1* and *P2* indicate "possible under specific conditions" and "scarcely possible", respectively. Considering the implementation of the enable and emergency stop switches, crushing or colliding caused by the hazardous movement of the Skill-Assist can be avoided by using the safety switches. Therefore, we select parameter *P1* at the third branch point.

As a result of these risk parameters, the target SIL required for the Skill-Assist is SIL-2.

3.2 Fault Tree Analysis (FTA)

To examine the potential system failures and the appropriate safety measures against failures with unacceptable risk levels, we implement fault-tree analysis (FTA) (IEC 61025 Technical Committee, 2006).

Fig. 4 presents a simplistic version of the FTA, which focuses on the potential system failures that may cause the hazardous movement of the Skill-Assist. Note that we have omitted minor details, which are summarized in representative terms in Fig. 4, to focus on the sequence of safety-function design, because the actual FTA we conducted is more complex and too large to be represented in this chapter. The top event of the FTA is the hazardous movement of the Skill-Assist, which links to the lower-level events through IF and OR gates. The cumulative failure and simultaneous failure of multiple components are not considered in the FTA. An abnormal actuator current can be prevented if a human operator correctly pushes the power management switches or the switches normally work; otherwise, the abnormal current directly affects the movement of the Skill-Assist, resulting in crushing or colliding. The abnormal actuator current that occurs because of the failure of actuator, PLC, servo controller or contactor affects the hazardous movement of the Skill-Assist. We assume the actuator failure can be neglected if overcurrent, overheat, and openload protective functions incorporated in the AC servo controller normally work. The abnormal command signal can be

Parts	Failure mode	Effect	S	O	U	RPN	Safety measures
Force sensor	Continuous signal output	Runaway	3	2	1	6	Dual-channel voting, diverse programming
	Drift	Unstable operation	2	3	1	6	Drift compensation
	Noise (surge)	Unstable operation	2	3	1	6	Noise filter
Computer software	No output command	No operation	1	3	2	6	Dual-channel voting, diverse programming
	Continuous signal output	Runaway	3	3	2	18	Dual-channel voting, diverse programming
Computer hardware (D/A)	Continuous signal output	Runaway	3	2	1	6	Dual-channel voting, diverse programming
	Surge (short)	Unstable operation	2	3	1	6	Noise filter
PLC	Continuous signal output	Runaway	3	1	3	9	Safety PLC

Fig. 5. Simplistic version of FMEA that focuses on high RPN values

traced to sensor failures, such as noise or the malfunction of each sensor, or computer failures, such as software and hardware failures.

The FTA result enables us to easily trace the failures. Hence, we can develop safety measures for failures that may cause the hazardous movement of the Skill-Assist. For effectiveness, it is important to prioritize safety measures according to the effects and risks of the failures.

3.3 Failure Mode and Effects Analysis (FMEA)

To examine the potential failures and the appropriate safety measures against unacceptable risk levels estimated for the Skill-Assist, we next conduct a risk assessment based on a failure mode and effects analysis (FMEA) (IEC 60812 Technical Committee, 2006) on the basis of the FTA results.

In the FMEA, the consequences of a part failure are evaluated using three criteria: severity (S), likelihood of occurrence (O), and undetectability (U). The overall risk of each type of failure is called the risk priority number (RPN), which is the product of severity, occurrence, and undetectability ratings. S, O, and U have simplified ratings of low (1), medium (2), and high (3) in the proposed methodology. The ratings are each determined to suit the FMEA on the basis of the method mentioned in (IEC 60812 Technical Committee, 2006) and the experience of the control-system designers. The incidents of failure in the control system are graded on an RPN scale of 1–27, where a failure with a rating of 27 is regarded as the most hazardous.

Fig. 5 shows a simplistic version of the FMEA that especially focuses on failure modes with high risk-priority number (RPN) values. In Fig. 5, we have omitted the minor details and summarized in representative terms. The basic function of FMEA is to describe the parts of a system and to list the consequences of a part failure. The RPN threshold was determined to be four by several control-system designers. They consider it as the most suitable threshold value in the FMEA from a safety perspective, i.e., the failure modes with RPN more than the threshold are considered to be sufficiently serious to require safety measures. In Fig. 5, we categorize the severity of failure effects that may cause runaway, unstable operations, and no operation as high, medium, and low, respectively. The likelihood of the occurrence of noise and incorrect coding failure modes is rated as high. The undetectability of actuator failures are rated as low, while that of PLC is rated as high.

We then define a safety measure for each failure mode with a high RPN. For instance, a combination of dual-channel voting and diverse programming (Mitra et al., 1999; Littlewood, 2000; IEC 61508 Technical Committee, 1998) is adopted as an effective safety measure for sensor and computer failures, because it can address some common mode failures and is also recommended by a safety standard (BSR/T15.1 Technical Committee, 2002). A

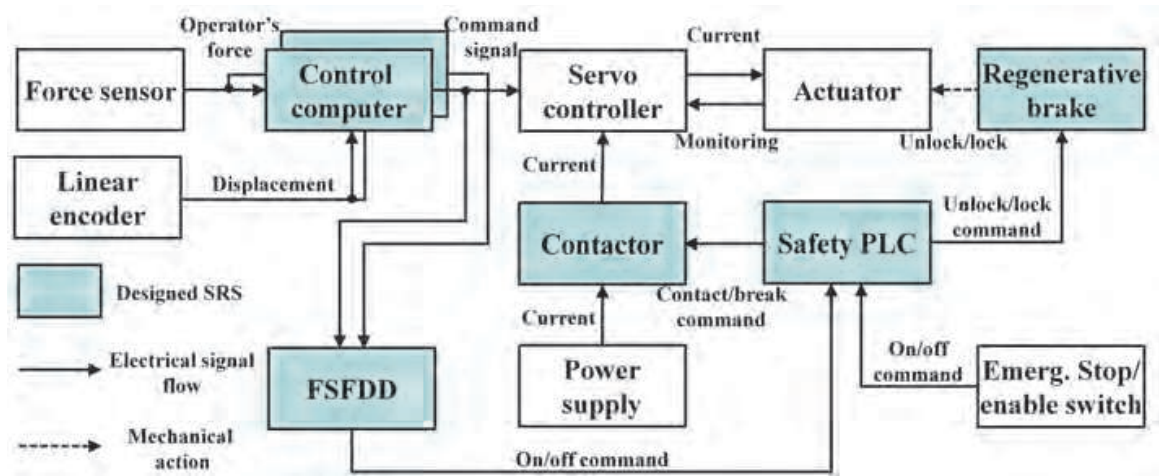


Fig. 6. Improved control system with the designed SRS

signal-monitoring function that utilizes dual-channel voting architecture is required for detecting abnormal command signal the control computer generates through the D/A converter. Safety PLC is adopted as an alternative of the PLC incorporated in the conventional control system of Skill-Assist.

4. Design of SRS and functional safety analysis based on IEC 61508

4.1 Control system for securing functional safety with the designed SRS

We design a SRS based on the risk assessment results and Fig. 6 shows an improved control system with the SRS. The designed SRS (shaded blocks in Fig. 6) consists of primary and secondary control computers, FSFDD (see also the Appendix), a safety PLC (JTEKT, TOYOPUC-PCS series), a contactor, and a regenerative brake.

The two control computers function as a dual-channel voter, diversely process sensor signals, and transfer two equivalent analog commands to the FSFDD. A force-sensor-based control algorithm is built into the primary computer and operates the Skill-Assist. Therefore, the command signal of the primary computer is also transferred to the servo controller. A diversely-programmed control algorithm is built into the secondary computer and calculates the redundant command signal to be compared with the command signal of the the primary computer. Unlike the command signal of the primary computer, that of the secondary computer is not transferred to the servo controller. Power is supplied to the DC servo motor through a contactor. The motor current is monitored by the servo controller by using the Hall-effect device.

When a fault is detected because of a difference in the command signals on the basis of the preset threshold, the FSFDD automatically shuts the power supply down and locks the drive wheels by using the contactor and regenerative brake through the safety PLC.

4.2 Configuration of the designed SRS

Fig. 7 depicts the architecture of the designed SRS. For the convenience of the functional safety analysis to be hereinafter described, the SRS is divided into the following sub-systems:

- Input sub-system: primary and secondary control computers

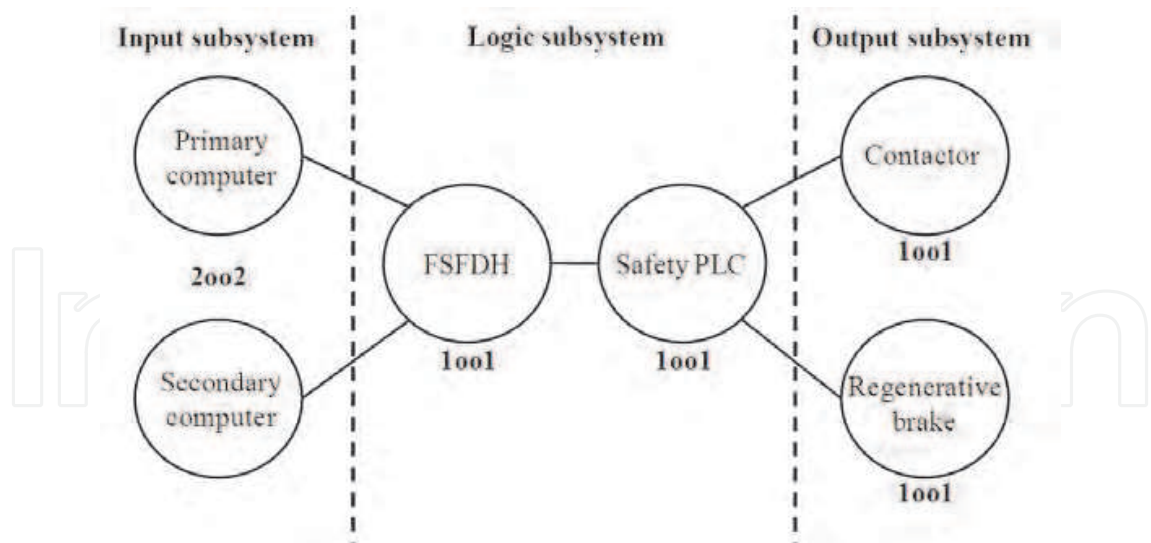


Fig. 7. Architecture of the proposed SRS

- Logic subsystem: FSFDD and safety PLC
- Output subsystem: contactor and regenerative brake

The input sub-system, which is expressed by 1 out of 2 (1002), enables the FSFDD to detect a fault in the command signals generated from the primary or secondary control computers. 1002 consists of dual channels connected in parallel, such that either channel can process the safety function. The logic sub-system comprises 1 out of 1 (1001) devices, where any dangerous failure leads to the failure of the safety function when a demand arises (IEC 61508 Technical Committee, 1998); therefore, in particular, the FSFDD and safety PLC involved in the logic sub-system should be highly reliable from the viewpoint of functional safety. The output sub-system comprises 1001 devices that can be actuated in a complementary manner in order to enhance the reliability of an emergency stop.

4.3 Process of functional safety analysis

To analyze the validity of the SRS design, we conduct functional safety analysis according to the approach mentioned in (IEC 61508 Technical Committee, 1998). We adopt the SIL, previously determined in subsection 3.1, as the quantitative criterion. Fig. 8 provides an overview of the functional safety-analysis process. First, the component failure rates, failure modes and failure mode distributions of the SRS are obtained. Second, failure modes, effects, and diagnostic analysis (FMEDA)<sup>1</sup> is implemented to examine the effects of the failure modes on the SRS (Goble et al., 1999). Next, the safety-failure fraction (SFF) and the probability of failures per hour (PFH) are calculated on the basis of the result of FMEDA in order to examine whether the target SIL has been achieved (IEC 61508 Technical Committee, 1998). Note that the evaluation process for the SRS software is not considered in Fig. 8, and we only consider the hardware of the designed SRS.

<sup>1</sup> FMEDA is a different process from FMEA.

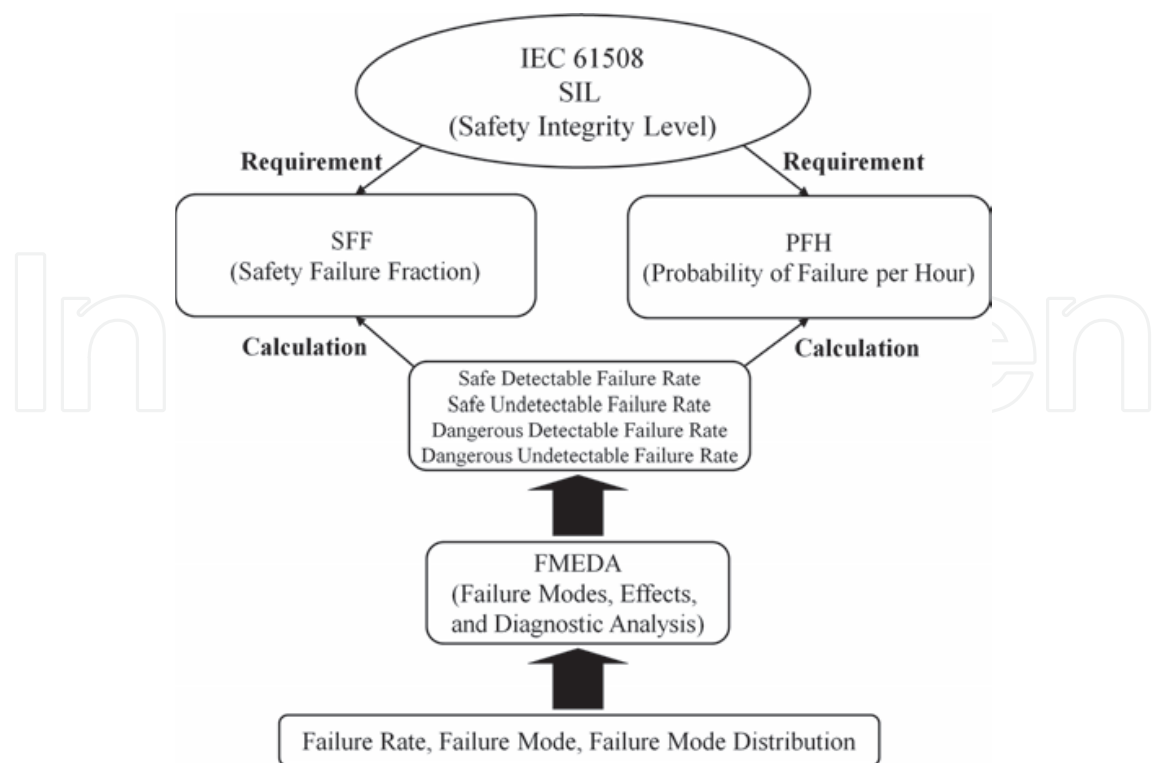


Fig. 8. Process of functional safety analysis

4.3.1 FMEDA

FMEDA is one of the steps required for analyzing the functional safety of a device. Fig. 9 shows a part of the FMEDA conducted for the FSFDD. Failure-in-time (FIT) denotes the unit of failure rate, and 1 FIT represents  $10^{-9}$  failures per hour. In the FMEDA, we refer to (MIL-HDBK-217F Technical Committee, 1991) and (IEC 62380 Technical Committee, 2004) as references for the failure rate, failure mode, and failure mode distribution. The safe detectable, safe undetectable, dangerous detectable, and dangerous undetectable failure rates are denoted by  $\lambda_{sd}$ ,  $\lambda_{su}$ ,  $\lambda_{dd}$  and  $\lambda_{du}$  respectively and calculated as the result of the FMEDA. Furthermore, the safe failure rate  $\lambda_s$ , dangerous failure rate  $\lambda_d$ , and total failure rate  $\lambda$  of a component have the following relationships:

$$\lambda_s = \lambda_{sd} + \lambda_{su} \tag{1}$$

$$\lambda_d = \lambda_{dd} + \lambda_{du} \tag{2}$$

$$\lambda = \lambda_s + \lambda_d \tag{3}$$

A failure that gives an FSFDD output of 0 V and shuts down the power source of the actuator is considered to be a detectable failure, irrespective of whether it is safe or dangerous. A failure that does not change the output signal is considered to be a safe undetectable failure, whereas a failure that causes oscillations, drift, or surge in the output signal is considered to be a dangerous undetectable failure. A circuit simulator Micro-Cap 9.0 (Spectrum Software) is utilized for examining the effects of the failure modes.

FMEDA for the simply configured electrical components such as power switch and EM brake is conducted in a manner similar to that for the FSFDD. However, for complex components such as the control computer, where a detailed analysis of each failure

Parts	ID	Function	Failure mode	Effects of failure	FIT	Failure probability	Safe/dangerous failure mode	Detectable/undetectable failure mode	$\lambda_{sd}$	$\lambda_{su}$	$\lambda_{dd}$	$\lambda_{du}$	Remarks
Capacitor: (Fixed ceramic dielectric capacitor)	C2	Stabilizing input signal to regulator 78M05F	Short	Continuous signal output	12.6	70%	Dangerous	Undetectable				8.82	
			Open	No output		10%	Safe	Detectable	1.26				
			Drift	No output		20%	Safe	Undetectable			2.52		
Variable resistor	VR1	Adjusting threshold of FS49B	Open	No output	138	80%	Safe	Detectable	110				
			Drift	No output		20%	Safe	Undetectable		27.6			
Transformer	T1	Rectifying output signal of FS57C	Short	Surge signal output	144	20%	Dangerous	Detectable			28.8		
			Open	No output		80%	Safe	Detectable	115				

Fig. 9. A part of FMEDA

SFF	Hardware fault tolerance		
	0	1	2
~60%	Not Acceptable	SIL1	SIL2
60%–90%	SIL1	SIL2	SIL3
90%–99%	SIL2	SIL3	SIL4
99%~	SIL3	SIL4	SIL4

Table 1. Architectural constraints determined by SFF and SIL

mode is impossible, a division of failures up to 50%  $\lambda_s$  and 50%  $\lambda_d$  is generally accepted (IEC 61508 Technical Committee, 1998). Furthermore,  $\lambda_{dd}$  and  $\lambda_{du}$  of the complex components are determined under the assumption that they have high diagnostic coverage (DC), which is expressed by following equation (IEC 61508 Technical Committee, 1998):

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d}$$

(4)

where  $\sum$  denotes the summation of the failure rates of the components involved in each sub-system.

4.3.2 SFF

SFF is a parameter that specifies the architectural constraints required for an SRS (IEC 61508 Technical Committee, 1998). SFF can be calculated as follows:

$$SFF = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda}$$

(5)

Table 1 shows the architectural constraints determined by SFF and SIL. A hardware fault tolerance of N indicates that N + 1 faults can cause a loss of the safety function. Because even a single fault cannot be allowed in the lool and loo2 architectures, in order to maintain the safety function, the architectures of all sub-systems in the designed SRS should meet an SFF in the range of 90%–99% to satisfy the target requirements of SIL-2.

SIL	PFH
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 $< 10^{-5}$

Table 2. SILs according to PFH in high demand or continuous operation modes

4.3.3 PFH

The SIL of an SRS in high demand or continuous operational modes is measured by the PFH of the safety function, which must be low enough to achieve the required SIL (IEC 61508 Technical Committee, 1998). According to Table 2, which shows the relationship between the SIL and the PFH, the designed SRS must satisfy a PFH in the range of  $10^{-7}$ – $10^{-6}$  to achieve the target requirements of SIL-2.

The PFHs of the lool and loo2 architectures,  $PFH_{1oo1}$  and  $PFH_{1oo2}$ , respectively, are obtained by the following equations (IEC 61508 Technical Committee, 1998):

$$PFH_{1oo1} = \sum \lambda_{du} \tag{6}$$

$$PFH_{1oo2} = 2 \left( (1 - \beta_d) \sum \lambda_{dd} + (1 - \beta) \sum \lambda_{du} \right)^2 t_{ce} + \beta_d \sum \lambda_{dd} + \beta \sum \lambda_{du} \tag{7}$$

$$t_{ce} = \frac{\sum \lambda_{du}}{\sum \lambda_d} \left( \frac{T_1}{2} + MTTR \right) + \frac{\sum \lambda_{dd}}{\sum \lambda_d} MTTR \tag{8}$$

where  $\beta$  and  $\beta_d$  represent the fraction of common-cause failures that are undetected and detected by the diagnostic tests, respectively. The channel-equivalent mean down time, the interval of the periodic diagnostic test, and the total elapsed time from the initial failure to the reinitialization of the system status (mean time to repair) are represented by  $t_{ce}$ ,  $T_1$ , and  $MTTR$ , respectively. Note that the unit of measurement for  $t_{ce}$ ,  $T_1$ , and  $MTTR$  is h.

4.4 Result of functional safety analysis

Table 3 summarizes the failure rates, SFF, and PFH that are acquired as a result of the functional safety analysis for the designed SRS. Each  $\lambda$  is provided by the manufacturers or determined by the failure-rate data obtained from (MIL-HDBK-217F Technical Committee, 1991; IEC 62380 Technical Committee, 2004). On the basis of the FMEDA results, we can determine  $\lambda_s$ ,  $\lambda_{dd}$ , and  $\lambda_{du}$  for the SRS components. The SFFs of all the sub-systems are calculated using Eqs. (1), (3), and (5). The PFH of the input sub-system, which is configured with the loo2 architecture, is calculated using Eqs. (7) and (8), where  $\beta = 20\%$  and  $\beta_d = 10\%$  as the worst case,  $T_1 = 8760$  h (one year), and  $MTTR = 8$  h, on the basis of the parameter range in a typical example of the functional safety analysis (IEC 61508 Technical Committee, 1998). The PFHs of the logic and output sub-systems, which are configured with the lool architecture, are calculated using Eq. (6). The result of the functional safety analysis in Table 3 suggests that all sub-systems of the SRS are able to satisfy the target requirements of SIL-2, i.e., they have the SFFs in the range of 90%–99% and the PFHs in the range of  $10^{-7}$ – $10^{-6}$ .

Subsystem	Item	Failure rates ( $\times 10^{-6}$ )				SFF	PFH
		$\lambda$	$\lambda_s$	$\lambda_{dd}$	$\lambda_{du}$		
Input subsystem (1oo2)	Control computer	11.60	5.80	5.37	0.43	96%	$3.3 \times 10^{-7}$
Logic subsystem (1oo1)	FSFDD	2.57	0.47	2.07	0.03	99%	$4.0 \times 10^{-8}$
	Safety PLC	0.26	0.13	0.12	0.01		
Output subsystem (1oo1×2)	Regenerative brake	0.58	0.29	0.23	0.06	90%	$1.6 \times 10^{-7}$
	Contactor	1.00	0.50	0.40	0.10		

Table 3. Result of functional safety analysis

5. Discussion

The sources of hazards in HCRs can be largely divided into human errors, the environment in which humans and robots interact, and the robot itself (Dhillon & Fashandi, 1997; Yamada et al., 1999; Alvarado, 2002). This research introduced a case study that focused on a robot, especially with regard to its system failures. The system failures of the robot could be identified by relatively simple risk assessments such as FTA, and the functional safety analysis was conducted by calculating the failure rates of different sub-systems the designed SRS comprises. Moreover, all equations in the functional safety analysis were deterministic and linear and all parameters in these equations took constant values; the parameters determined the SFF and PFH. However, if an operator and a robot are treated as a man-machine system, a human-robot cooperative system is stochastic and nonlinear, and in this case, human factors should be addressed by more sophisticated safety-analysis approaches. Therefore, the proposed methodology is limited to the design of the safety function for system failures and cannot be directly applied to other safety functions that can prevent hazardous events caused by human factors. To design the safety function for an HCR in consideration of human factors, human-behavior analysis must be considered, and the risk-analysis techniques proposed in related studies such as (Guiochet, 2003; Ogorodnikova, 2008; Ogure et al., 2009) may give us some hints for doing so.

From the viewpoint of safety-design issues of HCRs, conventional studies such as (Ogorodnikova, 2008; Kazanzides, 2009; Guiochet et al., 2010) mainly present methodologies that focus on the inherent safety design based on risk assessments. For instance, (Guiochet et al., 2010) proposes an approach based on a combination of well-known safety-analysis techniques and applies this approach to the safety design for an HCR. However, these studies do not present details of how to design the safety function for HCRs. On the other hand, (Laible et al., 2004), (Okada et al., 2007), and (Nakabo et al., 2009) propose design methodologies for the safety function for HCRs. However, they neither predetermine the safety level required by the system nor assess whether the designed safety functions match the requirement. The significance of our study compared to conventional studies is that the proposed methodology for safety-function design systematically evolves from a process of predetermining the safety level to that of analyzing it; the methodology enables the design of an adequate safety function for an HCR and provides an analysis process with the required safety level. We believe that the proposed methodology can be applied to safety-function design for system failures of HCRs such as power-assist systems or industrial robots with a hands-on control mode.

A dual-channel architecture can detect a fault that occurs in any one channel at a time. Therefore, if a component that is commonly connected to both channels causes a fault, a dual-channel voter such as FSFDD cannot detect the fault, because the same abnormal signals would be generated from the channels. Furthermore, the analog voting architecture proposed in this study limits the flexibility of the system configuration and has low performance in terms of noise tolerance. In the future, we will investigate the design of a dual-channel architecture that can address the simultaneous failure of both channels using digital processing.

A functional safety analysis of the software also needs to be implemented for an SRS involving programmable controllers. Unlike the case of hardware, which adopts a probabilistic approach as introduced in this paper, a software analysis is generally conducted by deterministic approaches and a specified software-development lifecycle (IEC 61508 Technical Committee, 1998). In particular, the method described in (IEC 61508 Technical Committee, 1998) concretely suggests software techniques, including safety specifications, architecture design, and programming languages, to be adopted in an SRS according to the required SIL. Such a functional safety analysis for software is also necessary for the proposed methodology, and the integration of safety-function design approaches for hardware and software should be discussed in the future.

System stability is an important issue related to the safety of HCRs. To stabilize a human-robot cooperative system constantly, it is primarily required to design a robust controller that can minimize the effects of uncertain factors in the system. As an additional safety measure, it is also required to establish a safety guideline for operators that prohibits aggressive maneuvering, which can cause the unstable movements of the system. The proposed methodology does not include the analysis for system stability because it focuses on the validity analysis of the safety-function design based on IEC 61508. To introduce the system-stability problem to the proposed methodology, it is necessary to analyze the maneuvering patterns of operators and the dynamics in the physical human-robot interaction, to quantify the analysis results to numerical parameters, and to apply these parameters to the process of safety-function design. Further discussion of how to implement system-stability analysis in the proposed methodology is an issue in the future.

## 6. Conclusion

In this chapter, we introduced a methodology for safety-function design involving functional safety analysis by using a case study on the system failures of the Skill-Assist. First, the target SIL required for the Skill-Assist was determined and the top-down and bottom-up risk assessments were then conducted. An SRS with two control computers, an FSFDD, and a safety PLC was designed on the basis of the risk-assessment results. We conducted a functional safety analysis for the designed SRS and found that it satisfied the target SIL.

## 7. Appendix – Fail-Safe Fault Detection Device (FSFDD): Signal-monitoring function for the analog voting architecture

Because an analog command signal is used in conventional control system of the Skill-Assist, we use an analog signal voting scheme to simplify the dual-channel architecture of the control computers. The analog voting scheme is also beneficial in simplifying the safety-related signal process once adequate measures are taken against noise. A fail-safe fault detection device (FSFDD) that we have developed can detect a fault by comparing the analog command

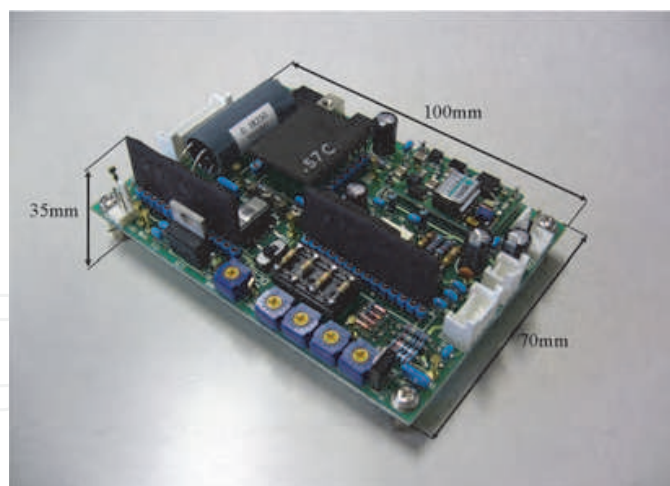


Fig. 10. Fail-safe fault detection device (FSFDD)

signals generated by the dual-channel control computer, and it reflects the result of the fault detection in the output signal (Lee & Yamada, 2007; 2009). By monitoring the command signals, the FSFDD is able to indirectly detect not only computer hardware/software failures, but also sensor failures that can cause hazardous movement of Skill-Assist. Fig. 10 shows the current version of the FSFDD. The fail-safe devices that dominate the FSFDD have the unique characteristic of generating an AC signal when the preset conditions for the input signals are met, and a constant DC signal otherwise (Kato, 1993; Sakai et al., 2000). The characteristics of fail-safe devices used in the FSFDD limit the effects of an internal failure on the output signal. Thus, the possibility of the FSFDD output signal reaching the inactive state of 0 V is high if a fault is detected in the command signals or its components fail. A noise filter circuit is incorporated into the input terminal of the FSFDD to smoothen the high-frequency noise in the command signals. More details on the FSFDD have been completely documented in studies (Lee & Yamada, 2007; 2009; Kato, 1993; Sakai et al., 2000).

## 8. References

- Moore, C., Peshkin, M., & Colgate, E. (2003). Cobot implementation of virtual paths and 3D virtual surfaces, *IEEE Transactions on Robotics and Automation*, 19 (2): 347–351, ISSN 1042-296X
- Kim, Y., Lee, J., Lee, S., & Kim, M. (2005). A force reflected exoskeleton-type masterarm for human-robot interaction, *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 35(2): 198–212, ISSN 1083-4427
- Tsuji, T., & Tanaka, Y. (2005). Tracking control properties of human-robotic systems based on impedance control, *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 35(4): 523–535, ISSN 1083-4427
- Konosu, H., & Yamada, Y., (2003). Skill-Assist: assisting device helping human workers in automobile modular component assembly, *Proc. of IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp.2514–2515, Las Vegas, USA.
- Santos, P. G., Garcia, E., Sarria, J., Ponticelli, R., & Reviejo, J. (2010). A new manipulator structure for power-assist devices, *Industrial Robot: An International Journal*, 37(5): 452–458, ISSN 0143-991X

- Fujiwara, S., Kitano, H., Yamashita, H., Maeda, H., & Fukunaga, H. (2002). Omni-directional cart with power assist system, *Journal of Robotics and Mechatronics*, 14(4): 931–937, ISSN 0143-991X
- Seki, H., Iijima, T., Minakata, H., & Tadakuma, S. (2006). Novel step climbing control for power assisted wheelchair based on driving mode switching, *Proc. of IEEE Int. Conf. on Industrial Electronics*, pp. 3827–3832, Paris, France
- Ogorodnikova, O. (2008). Methodology of safety for a human robot interaction designing stage", *Proc. of IEEE Int. Conf. on Human System Interactions*, pp. 452–457, Krakow, Poland
- Kazanzides, P. (2009). Safety design for medical robots, *Proc. of Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, pp. 7208–7211, Minneapolis, USA
- Guiochet, J., Martin-Guillerez, D., & Powell, D. (2010). Experience with model-based user-centered risk assessment for service robots, *Proc. of 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering*, pp. 104 -113, San Jose, USA
- Laible, U., Bürger, T., & Pritschow, G. (2004). A fail-safe dual-channel robot control for surgery applications, *Safety Science*, 42(5): 423–436, ISSN 0925-7535
- Okada, K., Maeda, I., Sugano, Y., Higuchi, & N., Fujita, T. (2007). Risk assessment of robot cell production system that achieved high productivity and safety in HMI environment, *Proc. of Int. Conf. on Safety of Industrial Automated Systems*, pp. 181–186, Tokyo, Japan
- Nakabo, Y., Saito, H., Ogure, T., Jeong, S., & Yamada, Y. (2009). Development of a safety module for robots sharing workspace with humans, *Proc. of 2009 IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, pp. 5345–5349, St. Louis, USA
- IEC 61508 Technical Committee (1998). *IEC 61508, Functional Safety of Electrical /Electronic/Programmable Electronic (E/E/PE) Safety Related Systems, Part 1: General Requirements*, IEC, Geneva, Swiss
- IEC 61508 Technical Committee (2002). *Functional safety and IEC 61508 – A basic guide*, IEC, Geneva, Swiss
- Homma, K., Yamada, Y., Matsumoto, O., Ono, E., Lee, S., Horimoto, M., Suzuki, T., Kanehira, N., Suzuki, T., & Shiozawa, S. (2009). A proposal of a method to reduce burden of excretion care using robot technology, *Proc. of IEEE 11th Int. Conf. on Rehabilitation Robotics*, pp.621–625, Kyoto, Japan
- IEC 61508 Technical Committee (1998). *IEC 61508, Functional Safety of Electrical/ Electronic/Programmable Electronic (E/E/PE) Safety Related Systems, Part 5: Examples of Methods for the Determination of Safety Integrity Levels*, IEC, Geneva, Swiss
- Behnisch, K. (2008). *White Paper Safe Collaboration with ABB Robots Electronic Position Switch and SafeMove*, ABB, Zurich, Switzerland.
- ISO Technical Committee 114 (2006). *ISO13849-1, Safety of Machinery – Safety-Related Parts of Control Systems – Part 1: General Principles for Design*, ISO, Zurich, Switzerland.
- Haddadin, S., Albu-Schäffer, A., & Hirzinger, G. (2009). Requirements for safe robots: measurements, analysis and new insights, *The International Journal of Robotics Research*, 28(11-12): 1507–1527, ISSN 1741-3176
- IEC 61025 Technical Committee (2006). *IEC 61025, Fault Tree Analysis (FTA)*, IEC, Geneva, Swiss
- IEC 60812 Technical Committee (2006). *IEC 60812, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)*, IEC, Geneva, Swiss
- Mitra, S., Saxena, N. R., & McCluskey, E. J. (1999). A design diversity metric and reliability analysis for redundant systems, *Proc. of International Test Conf.*, pp. 662–671, Atlantic City, USA

- Littlewood, B., Popov, P.T., Strigini, L., & Shryane, N. (2000). Modeling the effects of combining diverse software fault detection techniques, *IEEE Transactions on Software Engineering*, 26(12): 1157–1169, ISSN 0098-5589
- IEC 61508 Technical Committee (1998). *IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3*, IEC, Geneva Swiss
- BSR/T15.1 Technical Committee (2002). *Draft Standard for Trial Use for Intelligent Assist Devices – Personnel Safety Requirements*, RIA, Ann Arbor, USA
- Goble, W. M., & Brombacherb, A.C. (1999). Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems, *Reliability Engineering and System Safety*, 66(2): 145–148, ISSN 0951-8320
- MIL-HDBK-217F Technical Committee (1991). *Military Handbook 217F (MIL-HDBK-217F), Reliability Prediction of Electronic Equipment*, US Department of Defense, Arlington, USA
- IEC 62380 Technical Committee (2004). *IEC TR 62380, Reliability Data Handbook - Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment*, IEC, Geneva Swiss
- Dhillon, B., & Fashandi, A. (1997). Safety and reliability assessment techniques in robotics, *Robotica*, 15(6): 701-708, ISSN 0263-5747
- Yamada, Y., Yamamoto, T., Morizono, T., & Umetani, Y. (1999). FTA-based issues on securing human safety in a human/robot coexistence system, *Proc. of IEEE Int. Conf. on Systems, Man and Cybernetics*, pp. II1058–1063,, Tokyo, Japan
- Alvarado, M. (2002). *A Risk Assessment of Human-Robot Interface Operations to Control the Potential of Injuries/Losses at the XYZ Manufacturing Company (Master's thesis)*, University of Wisconsin-Stout, Menomonie, USA
- Guiochet, J., Motet, G., Baron, C. & Boy, G. (2003). Integration of UML in human factors analysis for safety of a medical robot for tele-echography, *Proc of IEEE Int. Conf. on Intelligent Robots and Systems*, pp. 3212–3217, Las Vegas, USA
- Ogorodnikova, O. (2008). Human weaknesses and strengths in collaboration with robots, *Periodica Polytechnica*, 25(33): 25–33,
- Ogure, T., Nakabo, Y., Jeong, S., Yamada, Y. (2009). Hazard analysis of an industrial upper-body humanoid, *Industrial Robot -An International Journal*, 36(5): 469-476, ISSN 0143-991X
- IEC 61508 Technical Committee, *IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems, Part 3: Software Requirements*, IEC, Geneva, Swiss
- Lee, S., & Yamada, Y. (2007). A highly-reliable force control system with a fail-safe fault detecting hardware for functional safety of Skill-Assist, *Proc. of Int. Conf. - Safety of Industrial Automated Systems*, pp. 403–408, Tokyo, Japan
- Lee, S., & Yamada, Y. (2009). Skill-Assist safety and intelligence technology, *International Journal of Automation Technology*, 3(6): 643–652, ISSN 1881-7629
- Kato, M. (1993). LSI implementation and safety verification of window comparator used in fail-safe multiple valued logic operations, *IEICE Transactions on Electronics*, E76-C(3): 356–366, ISSN : 1745–1353
- Sakai, M., Shirai, T., Mukaidono, M. (2000). A construction method of fail-safe interlocking module based on separation between safety-related parts and non-safety-related parts, *Proc. of 4th Int. Conf. on Engineering Design and Automation*, pp. 966-971, Orlando, USA



## **Human Machine Interaction - Getting Closer**

Edited by Mr Inaki Maurtua

ISBN 978-953-307-890-8

Hard cover, 260 pages

**Publisher** InTech

**Published online** 25, January, 2012

**Published in print edition** January, 2012

In this book, the reader will find a set of papers divided into two sections. The first section presents different proposals focused on the human-machine interaction development process. The second section is devoted to different aspects of interaction, with a special emphasis on the physical interaction.

### **How to reference**

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Suwoong Lee and Yoji Yamada (2012). Risk Assessment and Functional Safety Analysis to Design Safety Function of a Human-Cooperative Robot, Human Machine Interaction - Getting Closer, Mr Inaki Maurtua (Ed.), ISBN: 978-953-307-890-8, InTech, Available from: <http://www.intechopen.com/books/human-machine-interaction-getting-closer/risk-assessment-and-functional-safety-analysis-to-design-safety-function-of-a-human-cooperative-robo>

**INTech**  
open science | open minds

### **InTech Europe**

University Campus STeP Ri  
Slavka Krautzeka 83/A  
51000 Rijeka, Croatia  
Phone: +385 (51) 770 447  
Fax: +385 (51) 686 166  
[www.intechopen.com](http://www.intechopen.com)

### **InTech China**

Unit 405, Office Block, Hotel Equatorial Shanghai  
No.65, Yan An Road (West), Shanghai, 200040, China  
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元  
Phone: +86-21-62489820  
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the [Creative Commons Attribution 3.0 License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen