Case Study on the Assessment of SIL Using FMEDA

Byung Chul Kim¹ · Young Jin Kim^{2*}

¹Department of Automotive Engineering, Hanyang University

²Department of Systems Management and Engineering, Pukyong National University

FMEDA 기법을 적용한 SIL 등급 판정에 관한 사례연구

김병철¹ · 김영진²

¹한양대학교 미래자동차공학과 / ²부경대학교 시스템경영공학과

As the number, complexity and interaction of electrical, electronic and programmable electronic (E/E/PE) systems increase, a growing emphasis has been placed on the concept of functional safety during product development. IEC 61508 provides guidelines and standardized procedures in the development of reliable and dependable E/E/PE systems to assure functional safety. Determining risk classes (i.e., safety integrity levels, SILs) associated to a specific E/E/PE item may be recognized as one of the most crucial activities in the product development per IEC 61508 since SILs are used to specify necessary safety requirements for achieving an acceptable residual risk. This article presents a case study on the assessment of SILs applying failure modes, effects and diagnostic analysis (FMEDA) from which failure rates may be derived for each important failure category by combining a standard FMEA with online diagnostic techniques.

Keyword: functional safety, IEC 61508, safety integrity level (SIL), FMEDA, reliability prediction

1. Introduction

Compliance with the standard IEC 61508 becomes imperative in developing electrical, electronic and programmable electronic (E/E/PE) systems related to functional safety to cope with various safety related regulations with the increase of number, complexity and interaction of those systems. The standard covers all the relevant phases of development cycle (from initial concept, through design, implementation, operation and maintenance, to decommissioning) by providing guidelines for the design, verification and validation of safety related systems (SRSs) which imple-

ment the required safety functions necessary to achieve and maintain a state of Equipment Under Control (EUC). For each SRS, safety functions and their corresponding safety integrity levels (SILs) need to be specified. Representing a safety performance requirement for a system, the SIL is arranged in four distinct levels from SIL 1 to SIL 4, where SIL 4 is the highest with most stringent requirements. As a central concept of IEC 61508, safety integrity is defined as the probability of an SRS satisfactorily performing the required safety functions under all stated conditions within a specific period of time. (IEC 61508, 2010) A safety function is defined by two requirements : (1) the functional requirement describing what the

This work was partially supported by the MKE (Ministry of Knowledge and Economy of Korean Government) under the Quality Innovation Infra Development Program (No. B0012262) and by the MKE under the CITRC (Convergence Information Technology Research Center) support program (NIPA-2012-H0401-12-2003) supervised by the NIPA (National IT Industry Promotion Agency).

*Corresponding author : Young Jin Kim, Department of Systems Management and Eng., Pukyong National University, Busan 608-737 Korea,

Fax : +82-51-629-6478, E-mail : youngk@pknu.ac.kr

Received 16 July 2012, Revised(1st : 2 September 2012, 2nd : 7 September 2012), Accepted 7 September 2012.

safety function does and is derived from a hazard analysis and (2) the safety integrity requirement specifying the likelihood of the safety function being performed correctly (Glotzner, 2008).

If the risk inherent to a system exceeds an acceptable level, it is required to implement one or more safety functions to lower the actual risk to an acceptable level. Depending on the SIL to be achieved, appropriate measures and methods to be used are also described in the standard when implementing safety functions. Thus, a proper assessment of the SIL for SRSs is very important in applying IEC 61508. In this regard, the main objective of this study is to investigate a case example of the assessment of SILs applying failure modes, effects and diagnostic analysis (FMEDA) from which failure rates may be derived for each important failure category. FMEDA described in this article adopts the standard FMEA format from MIL-STD 1629A. Furthermore, MIL-HDBK 217F has been adopted for the purpose of reliability prediction since proof test data (i.e., field failure data) are not available for the product under study. It has been demonstrated that safe failure fraction (SFF) and other parameters necessary for the calculation of probability of failure on demand (PFD) may be obtained from FMEDA. The case study discussed here is based on the electrode type level gauge system which consists of two parts, micro process unit (MPU) and remote indicator unit (RIU). Depending on the proof-test intervals and operating conditions, the assessment of SILs has been conducted on the basis of PFDs obtained from FMEDA.

2. Key Concepts : SIL, SFF and PFD

The most important aspect of SRSs is to enhance the safety of the system itself by reducing potential inherent risk factors which can be done by reducing the PFDs. According to the standard IEC 61508, the SILs are defined as shown in <Table 1> depending on the PFD. A higher SIL means that a safer system can be achieved.

In terms of safety, system failures can be roughly divided into two categories: Safe and Dangerous Failures. Safe Failures mean those at the level of modules or subsystems inside the system. For these failures, the system can be migrated to the safe side through automatic diagnoses by the diagnostic function of

Table 1. Safety Integrity Level (Low Demand Mode)

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD), Average
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

the system. Failures in MPUs and RIUs correspond to this type of failure mode. On the other hand, Dangerous Failures mean, for example, that an error in operational processes inside an MPU cannot be found unless deviations in the relation between input and output signals is determined. In other words, even if an abnormality occurs inside the device, it appears to be working normally when viewed from outside. In such a case, the device continues to be used without stopping because the abnormality cannot be detected, which may lead to hazardous situation (Karou, 2005). For this reason, the above two failure modes are again divided into detectable and undetectable elements, and safe failure fraction (SFF) can be determined on the failure rate of Dangerous Failure Undetected, the most dangerous element for safety. The calculation of SFF is given as follows :

$$SFF = \frac{(\lambda_{SD} + \lambda_{SU} + \lambda_{DD})}{(\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU})} \quad (1)$$

where λ_{SD} : Safe Failure Detected
 λ_{SU} : Safe Failure Undetected
 λ_{DD} : Dangerous Failure Detected
 λ_{DU} : Dangerous Failure Undetected.

If SFF exceeds 60%, 90% or 99%, SIL 1, SIL 2, or SIL 3 is obtained respectively. For each component of the SRS, the average PFD is calculated from the failure rate of Dangerous Failure Undetected and the proof-test interval as follows:

$$PFD_{avg} = \frac{1}{T_p} \int_0^{T_p} [1 - \exp(-\lambda_{DU} \cdot t)] dt \quad (2)$$

where T_p represents the proof-test interval. The average PFD for the system is simply the sum of the average PFD of each component. Based on the PFD calculations, one may now determine whether the SRS satisfies the requested levels of SIL.

3. Reliability Prediction and FMEDA

The electrode type level gauge system consists of two parts: Micro Process Unit (MPU) and Remote Indicator Unit (RIU). An MPU receives 16 digital inputs from the sensor. Water level is divided into 16 levels from the bottom (0%) to the top (100%). If the water hits the pre-defined level, an RIU indicates the height in color out of 16-stepwise vertical bar. The device is turned on only if the water level changes, and the mode of operation is designated as 'low demand mode' from the past experience. A schematic drawing of the system is shown in <Figures 1>. The MPU has own display monitor and the RIU is usually placed in a remote site.

Figure 1. Schematic Drawing of Electrode Type Level Gauge

The device is newly developed by the company, and thus the field failure data (i.e., proof-test data) are not available. The failure rates of individual components are estimated based on the Part Stress Method of reliability prediction described in MIL-HDBK 217F. As shown in <Appendix 1>, an important information for each part is provided in reliability prediction results such as category, brief description, quantity used, individual and overall failure rates along with reference number. For example, the part BEAD (2012) is a kind of bead coil with the resistance of 10 ohm and referred as L1 (i.e., reference number L1). It is used only once in an MPU and its failure rate is 0.4 FIT (Failure In Time, the number of fai-

lure that can be expected in 10^9 hours of operation).

Proof-test has been conducted under two different temperature conditions, 30°C and 80°C. The outputs are transmitted to the RIU either by hardwire (4~20mA) or by RS-485 communication. If the transmission through hardwire fails, the alarm is annunciated and the RS-485 communication is turned on. Individual failure rates are calculated for the proof-test intervals of 1 month, 3 months, 6 months and 12 months. The MPU and RIU are consisted of 142 and 44 part components, respectively, and the failure rates for each component are obtained. These failure rate data may be used to estimate the failure rate of module or hardware block by each failure category in FMEDA. In addition to causes and effects for each failure mode, constituent parts of a component are listed in the table shown in Appendix 2. The overall failure rate of a component can be calculated as the sum of individual failure rates of constituent parts. Further the failure rate of a hardware block is simply the sum of individual failure rates of corresponding components. Considering safety assessment and detection method for each component, the failure category is determined.

For example, the hardware block 'Power' has two components, SMPS and Battery Charger. An SMPS is composed of 27 individual parts, including one ACDC motor (ACDC1), three diodes (U39, U40, D21), five coils (L3, L4, L5, LF1, LF2), four connector (CN1, SW6-2, SW6-3, SW6-4), one bead coil (LB1), and 13 capacitors (C132~C144). Adding up 27 individual failure rates from reliability prediction results, the failure rate of the component SMPS is found to be 3,524 FIT. Similarly, the component Battery Charger has 24 constituent parts, including four diodes (U41, D22, D23, D24), one relay (RY1), one transistor (Q6), one photo coupler (PC17), two capacitors (J10, C145), nine resistors (R210~R209), five connectors (SW100, SW101, SW102, SW105, SW6-1), and one battery (BT2). The failure rate of the component Battery Charger is simply the sum of failures rates of 24 individual parts which yields the failure rate of 508 FIT. Consequently, the failure rate of hardware block 'Power' is 4,032 FIT (= 3,524 + 508). Failures in 'Power' are classified as Dangerous Failure Detected through safety assessment resulting in $\lambda_{DD} = 4,032$ FIT for this hardware block. For each hardware block, the failure rates and their failure category are obtained in a similar way to construct the FMEDA table.

4. Results

Obtained from the FMEDA, failure rates by category are summarized in <Table 2> and <Table 3> for temperatures of 30°C and 80°C, respectively. It should be noted that failure rates remains the same without regard to proof-test interval and the SFF is calculated using equation (1). Based on the data of failure rate given in <Table 2> and <Table 3>, we may now calculate the PFDs at each temperature condition depending on proof-test intervals. The PFDs and corresponding SILs of the system is summarized in <Table 4> and <Table 5>. It should also be noted that the PFD for each part is calculated using equation (2) and the overall PFD is simply the sum of individual PFDs of MPU and RIU.

Table 2. Failure Rates at the Temperature 30°C

Rate and SFF	MPU	RIU
Total Failure Rate (FIT)	25,850	7,772
SFF (%)	97.5	99.0
λ_{SD} (FIT)	14,651	4,451
λ_{SU} (FIT)	79	0
λ_{DD} (FIT)	10,470	3,244
λ_{DU} (FIT)	650	76

Table 3. Failure Rates at the Temperature 80°C

Rate and SFF	MPU	RIU
Total Failure Rate (FIT)	55,331	12,542
SFF (%)	94.4	98.5
λ_{SD} (FIT)	34,220	7,839
λ_{SU} (FIT)	213	0
λ_{DD} (FIT)	17,783	4,516
λ_{DU} (FIT)	3,115	188

Table 4. PFD and SIL with Respect to Proof-Test Interval at the Temperature 30°C

T_P (month)	PFD of MPU (FIT)	PFD of RIU (FIT)	System PFD	SIL
1	239,596	29,128	2.69E-04	SIL 3
3	707,668	84,064	7.92E-04	SIL 3
6	1,429,279	168,757	1.60E-03	SIL 2
12	2,852,998	335,854	3.19E-03	SIL 2

Table 5. PFD and SIL with Respect to Proof-Test Interval at the Temperature 80°C

T_P (month)	PFD of MPU (FIT)	PFD of RIU (FIT)	System PFD	SIL
1	1,131,669	69,924	1.20E-03	SIL 2
3	3,374,109	205,068	3.58E-03	SIL 2
6	6,831,204	413,415	7.24E-03	SIL 2
12	13,651,959	824,478	1.45E-02	SIL 1

For the case of temperature 30°C, the system has SIL 2 or SIL 3 depending on the proof-test intervals. For the case of temperature 80°C, on the other hand, the system has SIL 1 or SIL 2 depending on the proof-test intervals. It is intuitive that a higher SIL is assigned for a shorter proof-test interval with a given fixed failure rate since the calculated PFDs for a shorter intervals are lower.

Another important issue for SRSs is the operation records in the field. While the PFD is an important index used for actual SRS designs, MTBF (Mean Time Between Failures) determined by taking the actual field failure records into account is also an important factor. The requirement for operational reliability reinforces the need for simplicity in SRS design and development. It should be carefully implemented for introducing design changes to improve the SIL since the operational reliability of the system may be affected by these changes. The above example, although relatively simple, demonstrates how IEC 61508 may be applied to a real application. Individual failure rates are first obtained, from which the required average PFD and hence the SIL of SRSs are derived. This case example discussed only the design of the SRS. It must be appreciated that the scope of IEC 61508 is much wider than this, and other requirements must be met in order to claim compliance.

5. Conclusion

The concept of functional safety has recently drawn a great deal of attention from practitioners in reliability and safety community. More specifically, the standard IEC 61508 provides guidelines and procedures in the development of reliable E/E/PE systems for functional safety. For a successful implementation of IEC 61508, a proper assessment of SIL is recognized as one of the most critical steps. This article presents a case study of SIL assessment based on FMEDA for

an electrode type level gauge system. Failure rate prediction has first been carried based on MIL-HDBK 217F since the system is newly developed and thus field failure data are not available. The SFF and other parameters are derived to calculate PFDs.

It should be clear that the design of SRSs involves more than simply specifying subsystem components that are approved for use at the required SIL. The designer must demonstrate that the average PFD of the design as a whole meets the required SIL. For periodic proof tests, appropriate intervals must be selected since these intervals have a bearing on the average PFDs. This only applies to SRSs operating on low demand mode. For SRSs operating in continuous or high demand mode, the probability of dangerous failure per hour, PFH, is considered in place of the average PFD.

References

- Bukowski, J. V. and Goble, W. M. (2012), Properly Assessing Mechanical Component Failure Rates, In *Proceedings of Reliability and Maintainability Symposium (RAMS)*, Reno, NV, USA.
- Bukowski, J. V. and Goble, W. M. (2009), Validation of a Mechanical Component Constant Failure Rate Database, In *Proceedings of Reliability and Maintainability Symposium (RAMS)*, Fort Worth, NV, USA.
- Catelani, M., Ciani, L., Luongo, V., and Singuaroli, R. (2010), Evaluation of the Safe Failure Fraction for an Electromechanical Complex System : Remarks about the Standard IEC 61508, In *Proceedings of Instrumentation and Measurement Technology Conference*, Austin, TX, USA.
- Glötzner, T. (2008), IEC 61508 Certification of a Code Generator, In *Proceedings of IET International Conference on System Safety*, Birmingham, UK.
- Goble, W. M. and Bukowski, J.V. (2007), Development of a Mechanical Component Failure Database, In *Proceedings of Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, USA.
- IEC 61508, *Functional Safety-Electric/Electronic/Programmable Electronic Safety-Related Systems*, 2010.
- Karou, S. (2005), EJX Series of IEC 61508 Safety Standard-Compliant Differential Pressure Transmitter, *Yokogawa Technical Report*, 40, 51-54.
- Xie, Y., Li, J., and Zhang, A. (2011), Extended FMEA Method Applied in the Field of Functional Safety, In *Proceedings of International Conference on Reliability, Maintainability and Safety (ICRMS)*, Guiyang, China.

Bukowski, J. V. and Goble, W. M. (2012), Properly Assessing Mecha-

<Appendix 1> Reliability Prediction Based on MIL-HDBK 217F

• Failure Rates of MPU for the Case of Temperature 30°C (Example)

No.	Category	Part	Description	Q'ty	Individual Failure Rate (FIT)	Failure Rate (FIT)	Reference
1	Battery	Ni-MH 1.2V AAA 2700mAh×6	Ni-MH 1.2V AAA 2700mAh×6	1	17.4	17.4	BT2
2	SMPS	FS30-12	SMPS Module, 12V/2.5A/30W/DIP 6PIN	1	3,333.3	3,333.3	ACDC1
3	Bead Coil	Bead(2012)	10ohm	1	0.4	0.4	L1
4	Coil	SC4532D-100K	SMD2P, 10mH	1	0.4	0.4	L2
5	Coil	100uH Ring Coil 18pi	100uH, 5A, DIP 2PIN	1	0.4	0.4	L3
6	Relay	PE30X-12V	250Vac/8A	8	55.1	440.8	RL1 ~ RL8
7	IC	MCP6242 (SOIC)	SMD SP OP-AMP	1	45.5	45.5	UB1
8	IC	TD62083AFG (SOIC)	8CH Darlington Sink Driver	1	45.5	45.5	U43
9	Diode	SA7.5CA	TVS Diode 7.5V	2	15.6	31.2	ZD1A, ZD2A
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
142	Transistor	2N3906 (TO92)	PNP Silicon Transistor, DIP 3P	1	1.5	1.5	Q3

<Appendix 2> Derivation of Individual Failure Rates Using FMEDA

• FMEDA of MPU for the Case of Temperature 30°C : An Example of Hardware Block 'POWER'

Application Item		Function	Relation Component (Reference)	Failure Mode	Failure Cause	Failure Effects	Failure Rate (FIT)				RPN				
Hardware Block	Sub Component						Sub Component	Hardware Block	S	O	D	RPN			
Power	SMPS	Main Power Supply	ACDC1, U39, U40, L3, L4, L5, CN1, LF1, LF2, D21, SW6-2, SW6-3, SW6-4, LB1, C123 ~ C144	No or Improper Output No Operation	Failure to Supply Voltage Component Defective/ Damaged	Front Display LCD/Lamp Off, Battery Mode On	3,524		4,032		A	II	A	6	
	Battery Charger	Standby Power Supply	U41, D22, D23, D24, RY1, Q6, PC7, J10, C145, R201 ~ R209, SW100, SW101, SW102, SW105, SW6-1, BT2	No or Improper Output No Operation	Failure to Supply Voltage Component Defective/ Damaged	Front Display LCD/Lamp Off	508								
⇒			Safety Assessment			Detection Method				Failure Rate of Hardware Block (FIT)				Corrective Action	
			Safe	Danger	Detected	Diagnosis (External)	Diagnosis (Internal)	Manual Test	Inspection	λ_S	λ_{SD}	λ_D	λ_{DD}		
				1	1	○			○	0	0	4,032	4,032	Replacement	
				1	1	○			○			4,032	4,032	Replacement

김병철

동아대학교 산업공학과 학사
부산대학교 대학원 수료
현재 : 한양대학교 산학협력전담 교수
관심분야 : Functional Safety, 자동차 부품
RAMS

김영진

한국과학기술원 경영과학 학사
한국과학기술원 경영과학 석사
Clemson University 산업공학 박사
현재 : 부경대학교 시스템경영공학과 교수
관심분야 : 실험계획, 품질공학, Functional
Safety