International Journal of Engineering & Technology, 7 (2.12) (2018) 62-67

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Quantitative risk evaluation based on IEC 61508 for SW functional safety of marine bigdata analysis system

Hee Yeong Kim *

Department of Computer Information, Hanyang Women's University, Seoul, Korea
**Corresponding author E-mail: heeykim0@naver.com*

Abstract

Background/Objectives: SW functional safety is beyond the SW quality and IEC 61508 is needed instead of ISO/IEC 9126.Embedded SW for Sensor or actuation is needed to be tested as perspectives of functional safety.
Methods/Statistical analysis: Risk analysis and quantitative risk evaluation procedure is used for estimating the risk of SW related to safety of equipment and embedded system. FMEDA (Failure Mode, Effects and Diagnostic Analysis) is one of the method for certifying SIL(Safety Integrity Level) but it is not easy to use when the sensors or actuations are too many. FMEA (Failure Mode and Effects Analysis) is simple method to use with another bigdata analysis technique. MBAS (Marine Bigdata Analysis System) is the SW to be analyzed the risk quantitatively in this study to assure the target safety.
Findings: Test methods based on IEC 61508-3 are defined as SIL to assure SW quality effectively but SIL of FMEDA uses complex equations to be defined and sensing equipment parts could be classified as failure rates for input data for equations. I recommend simple method to decide test methods as Severity Level that is very similar to SIL but very easy based on FMEA in this study. MBAS is bigdata solution and sensing data can be validated and verified by the analyzed results of the relation of process functions as dependent value from sensor data as independent value.
Improvements/Applications: No needed to be classified and be calculated the detected or undetected failure rate of sensor to assign the parts of equipment to define risks.

Keywords: *Functional Safety; Fmea; Fmeda; IEC 61508; SIL (Safety Integrity Level)*

1. Introduction

The accidents caused of SW defects are increasing every year.Arian 5 Rocket explosion in 1996, Russia Mars weather explore ship crash-down in 1999 and recall state of Toyoda Prius in 2014 had all SW problems. The future of accidents of SW problemis unavoidable in all area of industry because the dependency of SW is bigger with 4th industry revolution. The methods to avoid the accident are validation and verification of SW based on strict quality standards but it is not enough to minimize the risk of systems included sensors and actuations.
The quality of SW is evaluated by ISO/IEC 9126 or ISO/IEC 25023. ISO/IEC 9126 has 6 quality characteristics (functionality, reliability, usability, efficiency, maintainability, portability). ISO/IEC 25023 is called "Systems and Software Quality Requirement and Evaluation" and 2 more quality characteristics (functional suitability, reliability, performance efficiency, operability, security, compatibility, maintainability, transferability). SW safety belongs to one of characteristics of SW quality but there is no characteristic of safety to evaluate the risk of accident in ISO/IEC 9126 and 25023 though the reliability is similar to the concept of safety.
The concept of functional safety is differentwith SW reliability precisely. The defects of systemremained in machines or equipment would be cause of big disasters. Especially sensorrelated to safety or actuation SW to control the system is riskier and it is needed rigid regulations to protect property and human life. The scope of SW functional safety is wider than the scope of SW quality. It is based on the SW quality to verify and valid the defects of SW but needed risk analysis quantitatively and cross check method to warn the risk situation as alarm to overcome the disater and control the equipment before breaking out of accidents.

2. Background

Korea is peninsula and many fish ships and passenger ships are operating in the maritime area. But the current ships have to be examined more deeply because the ships are very old and exposed to danger without safety equipments. From the report of Korean Statistics as shown in table 1, it states that the number of marine accidents is not decreasing[1], but the scale of accident is bigger as the size of ship is bigger than the old one and the number of boarding people is increasing. To avoid the accidents, the navigation system is adopted in new big ship but the functional safety of the system is another issue to be examin

Table 1. Marine Accidents of Korea

Year	Collision	Contact	Stranding	Capsizing	Fire	Sinking	Distress	Casualty	sum

2004	210	12	75	35	57	69	45	80	583
2005	172	10	46	22	71	45	16	34	416
2006	167	17	66	16	41	25	11	20	363
2007	148	9	39	21	37	19	8	11	292
2008	125	15	32	8	25	18	11	17	251
2009	160	10	43	18	34	22	16	21	324
2010	174	22	64	17	25	22	9	33	366
2011	208	23	64	38	57	27	41	82	540
2012	157	21	53	25	55	26	44	57	438
2013	149	21	58	20	43	13	19	42	365
sum	1,670	160	540	220	445	286	220	397	3,938
frequency	42.4%	4.1%	13.7%	5.6%	11.3%	7.3%	5.6%	10.1%	100.0%

2.1. Functional safety

Functional safety is the part of the overall safety of programmable equipment or system that depends on operating correctly. Equipment failures, operator error and rapid environmental changes are causes of emergency of whole machinery embedded SW as important alarming or monitoring. Embedded system has main role to control and check data from the sensors. The mission of safety control embedded system is to check operation of the systems that are constituted sensor, logical operator, actuator. Programmed SW on embedded system monitors the data from the sensor and operator but sometimes is extended the role to the external signal of environment and weather. IEC 61508 is intrinsicinter national standard for functional safety and related to risk mitigation. Functional safety is different to SW quality characteristics and is needed to enlarge the scope of SW to sensors and machine for safety of equipment like [Figure 1].

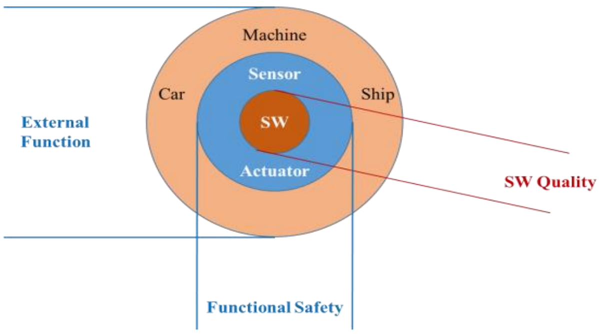

Fig. 1: The Scope of Functional Safety

2.2. IEC 61508

IEC 61508 is basic international standard for functional safety to adopt all kinds of industry and proposes the safety lifecycle for electrical/electronic/programmable electronic safety-related systems [2]. IEC 61508 does not only cover the classical technique aspects of a product, but also meet the demands of an entire safety lifecycle[3]. ISO 26262(automotive functional safety related) and IEC 60601(medical functional safety related) are derived from IEC 61508, but there is no specific international standard method or manual for marine or ship industry. Though new approaches like marine safety information systems are adopted to reduce the accidents but there is needed specific method to assure the safety and the regulations.

IEC 61508 defines the basic risk analysis process and [Figure 2] shows the process from concept to allocation of risk. The phase 3, "Hazard and risk analysis" in the process minimizes the risks and recommends checklist for risk factor excavation. There is calculation of probability and severity to analyze the risk factors quantitatively in the phase 3.

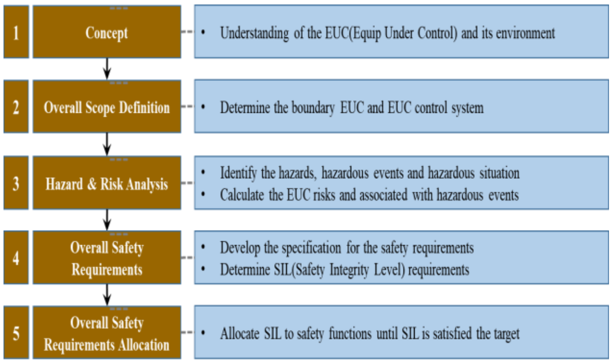

Fig. 1: Risk Analysis Process Based on IEC 61508.

SW functional safety uses SIL (Safety Integrity Level) to evaluate risks of a system or an equipment quantitatively. There are some methods to decide the SIL like FTA (Fault Tree Analysis), HAZOP (HAZard and OPerability), LOPA (Layer of Protection Analysis), FMEA (Failure Modes and Effects Analysis) and FMEDA(Failure Modes, Effects andDiagnostic Analysis). FTA is a method to analyze the safety-related risks and is analysis technique supported by software tools[4]. OpenFTA and EMFTA are FTA analysis tools. HAZOP is a technique for studying the hazards of a system and its operability problems by exploring the effects of any difference in design intent [5]. HAZOP is also supported by software tools like PHAWorks or HAZOP+. LOPA is a tool to carry out an assessment of barriers and the protection using a simplified form of semi-quantitative assessment[6]. Furthermore, LOPA is used to determine the acceptable risk and the target factor[7]. FMEA is a systematic procedure to identify the potential failures and their causes in engineering management[8] and uses a structured qualitative analysis technique. FMEDA is similar to FMEAbut FMEDA is enforced by adding quantitative failure information to components being analyzed. FMEDA was developed by Exida that is a specialized company in functional safety area.

2.3. FMEA

FMEA is typical inductive analysis method and systematic What-If analysis. It was development in the USA by NASA (National Aeronautics Space Agency) to improve the reliability of equipment[9]. FMEA could be described as a bottom-up approach from the specific module or part of equipment to functional structure to identify and prioritize potential failure modes. From the process of FMEA, the criticality and possibility of failure is estimated to eliminate or reduce the incidence. The results of FMEA method are documented to provide a reference to act corrective measures.In the [Table 2], risk priority is the parameters used to determine the criticality of a process function and calculated by multiple of 3 parameters(severity, occurrence, detectability) of each potential failure mode.

Table 2: The Sample of FMEA Work Sheet

Process Function	Potential Failure Mode	Potential Effect of Failure	Severity	Occurrence	Detectability	Risk Priority	Recommended Action	Remarks

2.4. Fmeda

FMEDA technique has diagnostic analysis process to measure diagnostic coverage[10]. Diagnostic coverage is considered configuration, function, failure mode, the effect of failure and the detectability [11]. FMEDA guides the step for quantitative evaluation process as items of system failure. The structure of the ripple effects of failure is analyzed for product safety. FMEDA process guides the step to decide the SIL (Safety Integrity Level) and to mitigate the risk to meet the target safety along the process like [Table 3]. SIL is used to specify necessary safety requirements to achieve an acceptable risk.

Table 3. Fmeda Process

Step	activities
	• Interview for risk analysis • define the block diagrams and list up the failure modes • review the causes of failures • review the severity, occurrence rate, detection rate • decide the failure level and risk priority • estimate the failure rate • assign the failure rate to parts • decide the safety or the risk failure • classify the detectable failure and undetectable failure • estimate the PFD(Probability of Failure on Demand), PFH(Probability of Failure per Hour), etc. • decide SIL(Safety Integrity Level) • seek to mitigate the risk • decide to meet SIL target or not

The results of FMEDA method are also documented and [Table 4] shows the sample of worksheet. λSD, λSU, λDD, λDU are decided from quantitative evaluation of SIL.

Table 4. The Sample Offmeda Work Sheet

Process Function	Item	Failure Mode	Failure Detection Method	Likelihood of Failure Mode	Failure Rate of Failure Mode	Failure Rate(λ)				Remarks
						λSD	λSU	λDD	λDU	

- Detected safe failure rate : λSD
- Undetected safe failure rate : λSU
- Detected dangerous failure rate : λDD
- Undetected dangerous failure rate : λDU

2.5. SIL (Safety integrity level)

SIL is the probability of failure and has 1 to 4 levels as functional safety definition of IEC61508. Level 4 of SIL is the highest with the most stringent requirements. Quantitative evaluation is needed for deciding SIL. FMEDA is a good method for the evaluation of safety control system operation and a good process to decide SIL of the system.

Table 5. SIL Target Failure Measures

SIL	Demand mode of operation	
	PFD	PFH
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

* Source: IEC 61508-1, 2010.

PFD (Probability of Failure on Demand) and PFH (Probability of Failure per Hour) are calculated the failures like [Table 5] for SIL decision. PFD is low-demand operation and is calculated for an equipment that is used 1 time per year of or not. PFH is high-demand/continuous operation and is calculated for an equipment that is used 2 times more a year or continuous operating mode. PFH and PFD would be calculated from very complex equations (1), (2) and (3) for single-channel system based on IEC 615081[1].

$$\text{PFH single-channel system} = \sum \lambda \text{DU} \quad \ldots\ldots \quad \ldots\ldots\ldots.. \ (1)$$

$$\text{PFD single-channel system} = \left(\sum \lambda \text{DD} + \sum\sum \lambda \text{DU}\right) tce \quad (2)$$

$$tce \ = \ \frac{\sum \lambda \text{DU}}{\sum \lambda \text{D}}\left(\frac{T1}{2} + MRT\right) + \frac{\sum \lambda \text{DD}}{\sum \lambda \text{D}} \ \text{MTTR} \quad \ldots\ldots\ldots \quad .. \ (3)$$

- Failure rate: λ.
- Detected safe failure rate : λSD
- Undetected safe failure rate : λSU
- Detected dangerous failure rate : λDD
- Undetected dangerous failure rate : λDU

λ_D is the dangerous failure rate as the sum of λ_{DD} and λ_{DU}. t_{ce} is the channel equivalent mean downtime(hour) and T1 is the proof test interval. MRT is the mean repair time and MTTR is the mean time to restoration [12].

To decide the SIL, it is required to decide the scope of safety system to be analyzed. The purpose of the scope decision is to define the boundary of control system and to identify the risk. Definition of related equipment, external factors, the feature of accidents and sub-systems of the safety system is considered to make the scope decision. The risks would be decided to be PFH or PFD in the scope and it is very complex like upper function (1), (2), but there is qualitative method to decide like below question.

- Is it possible to demand rate based on data?
- Is it the frequency of the required actuation for safety system below one time a year?
- Is it the frequency of the required actuation for safety system more than twice of test frequency?

If only one more answer is agreeable, the function is belong to PFH. A automobile brake system using programmable electronic equipment and a train velocity control equipment are categorized to PFH[13]. SIL based on FMEDA is not easy to define because the failure rates of parts of sensor are collected from objective field data (i.e., proof-test data). When the parts of sensor or equipment are too many, it is impossible to estimated even based on the Part Stress Method of reliability prediction described in MIL-HDBK217F [14]. MBAS (Marine Bigdata Analysis System) of this study is operating by 24 X 7 on the ship and belong to PFH.

3. Case study: MBAS (marine bigdata analysis system)

3.1. MBAS

MBASis a SW to collect the sailing data from the related systems and analyze the sensor data to make the status report of the cruising ship. The main purpose of MBAS is to predict the failure of the parts or equipment related navigation from the analyzed data mathematically and to alarm the risky situation. The calculated output of MBAS is the image of efficiency fuel usage and correct route of the ship. The results of analysis show the safety of cruising status and validity of the safe environment of the ship. [Figure 3] shows the scope of MBAS and the boundary of related systems to collect the sensing data. MBAS checks the speed of ship by sea and land, and is monitoring the engine operation by RPM and fuel usage. From the sensor monitoring sub-system (GPS, compass, oscilloscope, Loran C, etc), 370 basic sensing data are collected to send MBAS. MBAS makes categorized 9 dependent values(velocity based on land, velocity based on sea, Max output of engine, RPM, fuel oriented control, etc) as process functionsfrom the sensing dependent values to make the information of the efficient and safe voyage.

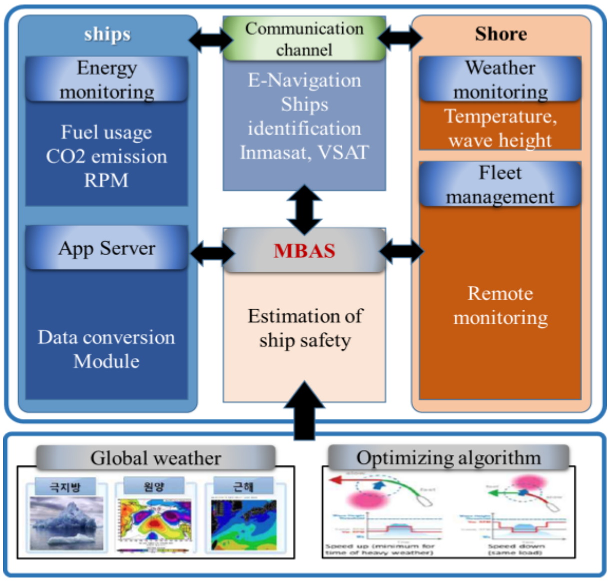

Fig. 3:.Mbas and Related Systems.

3.2. SW Functional safety analysis project for mbas

The MBAS development project is belong to 4S project that are carried forward by a big consortium to make whole scope of [Figure 3]. The data from the energy monitoring would be sent to MBAS through app server and MBAS can analyze the data. The functional safety analysis of MBAS is another pilot project to verify and validate the software safety function of MBAS modules. MBAS Functional Safety Test (MFST) project has procedure like [Figure 4].

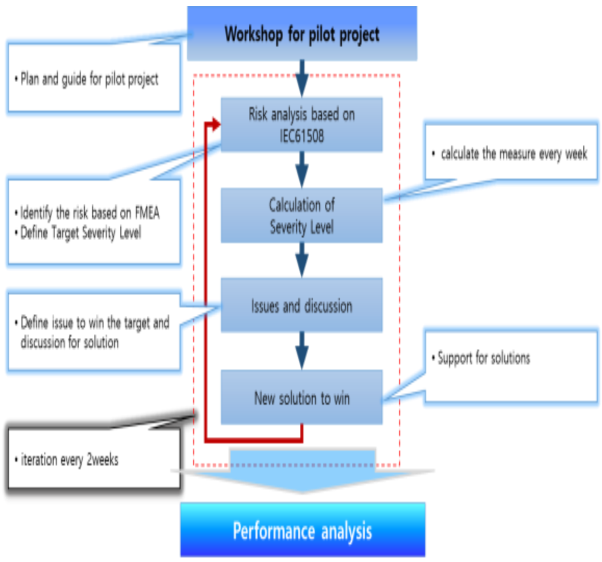

Fig. 4:.Mbasfunctional Safety Analysis Project.

The mfst project started from the identification of the risk based on fmea and the document of risk analysis is resulted like [Table6]. RPN is risk priority number and RPN RE is minimized the risk after recommended actions to protect the risk.

Table 6: The Risk of MBAS (Sample).

Process Function	Potential Failure Mode	Possible disaster	S	O	D	RPN	Recommended Action(s)	S RE	O RE	D RE	RPN RE
Velocity based on the land	calculation defect	collision	8	5	3	120	confirm the calculation of sensor regullary	8	3	2	48
	signal ommision	stranding	10	4	5	200	verify the cable and channel	10	3	3	90
	communication defect	collision	8	5	3	120	verify the cable and channel	8	3	2	48
	malfunction	fire	7	4	4	112	algorithm of malfunction detection	3	3	3	27
	alarm defect	collision	8	5	3	120	mathmatic modelling for anticipation of alarm failure	5	4	2	40
	access failure	shipwreck	9	3	3	81	authorization and re-set the access	9	2	2	36
Engine rotation	calculation defect	fire	7	4	3	84	confirm the calculation of sensor regullary	7	3	2	42
	malfunction	fire	7	4	4	112	algorithm of malfunction detection	3	3	3	27
	access failure	shipwreck	9	3	3	81	authorization and re-set the access	9	2	2	36
	alarm defect	collision	8	5	3	120	mathmatic modelling for anticipation of alarm failure	5	4	2	40
RPM (Revolutions Per minute)	calculation defect	fire	7	4	3	84	confirm the calculation of sensor regullary	7	3	2	42
	malfunction	minor collision	6	3	4	72	algorithm of malfunction detection	3	2	3	18
	alarm defect	fire	7	4	3	84	mathmatic modelling for anticipation of alarm failure	5	3	2	30

FMEA is easier than FMEDA that has very complex mathematical equations to make out. It is not easy to find out the failure rate of the sensors also when the number of sensors are too many. Target SIL can be defined by FMEDA with whole failure rate but SL (Safety Level) is estimated on this study based on the mean of RPN RE instead of SIL like [Table 7]. SIL is needed to decide the test method but SL can be used to decide test methods with RPN mean values. The test methods are recommended by IEC61508-3. There is not needed to assign the failure rate to parts and classify the detectable or undetectable failure in this simple SL method to decide test methods but the sensor data were classified based on EASI(Effective Algorithm for Computing Global Sensitive Indices) that is one of regression analysis method to verify the SW functional safety. The sensor data are independent values and had effects on process functions as dependent value that were calculated EASI results.

Table 7. The Severity Level of Process Function

Process Fuction	The mean of RPN RE	Severity Level	Test Method			
			performance	interface	dynamic	blackbox
Velocity based on the Sea	44.66					
Velocity based on the land	48.16	3	0	0	0	0
DFOC(Daily Fuel Oil Consumption)	42.5					
Engine rotation	36.25					
RPM(Revoltions Per minute)	30					
SFOC(Stator-Flux Oriented Control)	30.2	2			0	0
Efficiency of engine	35.5					
Fuel usage per 1 knot	38.5					
FOC(Field Oriented Control)	29.5	1				0

4. Results and Discussion

Sensing data from the equipment parts were 4,000 at every sensor and the number of sensor is 370. Sensors related to every process function were classified by EASI. For example, “fuel usage per 1 knot” has relationship with 115 sensing data like [Table 8].

Table 8. The Sensing Data Related Fuel Usage per 1 Knot.

GPGGA_EX11	M/E NO.6 CYL EXH. GAS OUT TEMP._30	NO.1 HFO PURIFIER & SUPPLY PUMP(P-1M-8)_103	NO.1 440V FEEDER PANEL(LR-1)_335
GPZDA_EX2	M/E NO.7 CYL EXH. GAS OUT TEMP._31	NO.2 HFO PURIFIER & SUPPLY PUMP(P-2M-8)_104	NO.2 440V FEEDER PANEL(LR-2)_336
GPZDA_EX4	M/E NO.8 CYL EXH. GAS OUT TEMP._32	NO.3 HFO PURIFIER & SUPPLY PUMP(P-1M-9)_105	EM"CY 440V FEEDER PANEL_337
GPZDA_EX5	M/E NO.9 CYL EXH. GAS OUT TEMP._33	NO.4 HFO PURIFIER & SUPPLY PUMP(P-2M-9)_106	E/R 220V FEEDER PANEL_338
IIRSA_EX1	M/E NO.10 CYL EXH. GAS OUT TEMP._34	NO.1 MAIN LO PURIFIER & SUPPLY PUMP(P-1M-10)_107	BOW THRUST CURRENT(A)_339
IROT_EX1	M/E NO.11 CYL EXH. GAS OUT TEMP._35	NO.2 MAIN LO PURIFIER & SUPPLY PUMP(P-2M-10)_108	NO.1 G/E F.O SUPPLY PUMP_340
VDVBW_EX4	M/E NO.12 CYL EXH. GAS OUT TEMP._36	NO.1 G/E LO PURIFIER(P-1M-11)_109	NO.1 G/E F.O BOOSTER PUMP_342
VDVBW_EX5	M/E EXH.GAS MANIFOLD TEMP._54	NO.2 G/E LO PURIFIER(P-2M-11)_110	M/E LO INLET PRESS_354
VDVBW_EX9	M/E NO.1 T/C EXH. GAS IN TEMP._55	M/E JACKET C.F.W IN PRESS._162	M/E NO.1 T/C LO PRESS_359
WIMWV_EX1	M/E NO.1 T/C EXH. GAS OUT TEMP._56	M/E JACKET C.F.W IN TEMP._163	M/E NO.3 T/C LO PRESS_361
WIMWV_EX3	M/E NO.2 T/C EXH. GAS IN TEMP._57	M/E J.C.F.W COMMON OUT TEMP._164	M/E LO IN TEMP_377
MAIN STEAM PRESS_9	M/E NO.2 T/C EXH. GAS OUT TEMP._58	M/E NO.1 J.C.F.W OUT TEMP._165	M/E NO.1 T/C LO OUT TEMP_402
BOILER F.O IN TEMP._10	M/E NO.3 T/C EXH. GAS IN TEMP._59	M/E NO.2 J.C.F.W OUT TEMP._166	M/E NO.2 T/C LO OUT TEMP_403
BOILER F.O IN PRESS._11	M/E NO.3 T/C EXH. GAS OUT TEMP._60	M/E NO.3 J.C.F.W OUT TEMP._167	M/E NO.3 T/C LO OUT TEMP_404
AUX BOILER STEAM DRUM PRESS_12	M/E NO.1 T/C EXH. GAS IN PRESS._87	M/E NO.4 J.C.F.W OUT TEMP._168	M/E T/C LO IN TEMP_406
BOILER EXH. GAS OUT TEMP._13	M/E NO.2 T/C EXH. GAS IN PRESS._88	M/E NO.5 J.C.F.W OUT TEMP._169	NO.2 MAIN LO COOLER IN PRESS._409
M/E EXH. GAS ECONO OUT TEMP_14	M/E NO.3 T/C EXH. GAS IN PRESS._89	M/E NO.6 J.C.F.W OUT TEMP._170	NO.1 MAIN LO COOLER OUT PRESS._410
NO.1 BOILER FEED W. PUMP_16	M/E NO.1 T/C EXH. GAS OUT PRESS._90	M/E NO.7 J.C.F.W OUT TEMP._171	NO.2 MAIN LO COOLER OUT PRESS._411
NO.1 BOILER W. CIRC. PUMP_18	M/E NO.2 T/C EXH. GAS OUT PRESS._91	M/E NO.8 J.C.F.W OUT TEMP._172	NO.1 MAIN LO COOLER IN TEMP._412
NO.2 BOILER W. CIRC. PUMP_19	M/E NO.3 T/C EXH. GAS OUT PRESS._92	M/E NO.9 J.C.F.W OUT TEMP._173	NO.2 MAIN LO COOLER IN TEMP._413
AUX. BOILER(P-1M-21)_20	M/E EXH. GAS MANIFOLD PRESS._93	M/E NO.10 J.C.F.W OUT TEMP._174	NO.1 MAIN LO COOLER OUT TEMP._414
NO.1 MAIN AIR COMP._21	M/E EXH. GAS ECONO IN PRESS._94	M/E NO.12 J.C.F.W OUT TEMP._176	NO.2 MAIN LO COOLER OUT TEMP._415
NO.2 MAIN AIR COMP._22	M/E EXH. GAS ECONO IN TEMP._95	M/E AIR COOLER F.W IN PRESS._181	NO.1 MAIN LO PUMP_416
NO.3 MAIN AIR COMP._23	M/E EXH. GAS ECONO OUT PRESS._96	NO.2 M/E J.C.F.W PUMP_185	NO.2 MAIN LO PUMP_417
NO.4 MAIN AIR COMP._24	M/E F.O IN PRESS._97	NO.1 CENTRAL C.F.W PUMP_186	NO.3 AUX. BLOWER_426
M/E NO.1 CYL EXH. GAS OUT TEMP._25	M/E F.O IN TEMP._98	NO.2 CENTRAL C.F.W PUMP_187	
M/E NO.2 CYL EXH. GAS OUT TEMP._26	NO.1 M/E F.O CIRC. PUMP_99	M/E NO.3 A/C C.W OUT PRESS._195	
M/E NO.3 CYL EXH. GAS OUT TEMP._27	NO.2 M/E F.O CIRC. PUMP_100	NO.6 REEFER TR LOAD_328	
M/E NO.4 CYL EXH. GAS OUT TEMP._28	NO.1 M/E F.O SUPPLY PUMP_101	NO.1 STEP DOWN TR LOAD_333	
M/E NO.5 CYL EXH. GAS OUT TEMP._29	NO.2 M/E F.O SUPPLY PUMP_102	NO.2 STEP DOWN TR LOAD_334	

SW could be tested for validation and verification and SIL would be the important value to decide the test method on IEC 61508-3. SIL can be defined through FMEDA but it is not easy when the sensing equipment parts are too many. FMEA and Severity Level based on the mean value of RPN is another simple method to decide the test methods for effectiveness and efficiency. MBAS was tested prioritized process functions. “fuel usage per 1 knot” has very high priority (SL is 3) and 4 test methods (performance, interface, dynamic, function and black box) were used to validation and verification for high quality. “FOC (Field Oriented Control)” has low priority (SL is 1) and function and black box test are used.

Every process function has sensing equipment parts related to and analyzed to define the safety of cruising ship based on MBAS results. MBAS is bigdata solution and uses HAD (High Dimension Approximation) model to estimate the result values of process functions. MBAS was verified the estimated value with real sensing data through ship cruising from the start point to the ending point of cruising. When some sensing data has trouble to make normal result because of unusual condition, MBAS shows the signal that process function values are different with the real cruising data from the ship and sailors can check the sensor or condition of the ship for safety of the navigation.

5. Conclusion

This paper proposed Severity Level instead of SIL for easy decision of test methods for functional safety of embedded systems. The objective of this work is to acquire effectiveness and efficiency to test SW for functional safety based on FMEA. FMEDA is very good method to estimate the probability of failure and define SIL but is very difficult when the sensing equipment parts are too many to assign the failure rate on every sensor or part. Defined severity level as the mean value of RPN of FMEA are decided easily the test method based on IEC 61508-3 and it is very simple method. The functional safety was validated and verified the result value based on real sensing data of cruising ship in this case. It is possible because the target SW, MBAS is bigdata solution and can be verified and validated with estimated data and real data for functional safety of the sensors.

References

[1] Kim D. Y., Kim K. Y., Park G. K., Jeong J. S., A Study on the Implementation of Intelligent Navigational Risk Assessment System with IoT Sensor. In Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems, 2016 Joint 8th International Conference on IEEE. pp. 328-333.

[2] International Electrotechnical Commission(IEC), IEC61508-1:2010 Functional safety of electrical/electronic/programmable ecteronic safety-related systems-Parts 1, 2010

[3] Van Heel, K. A. L., B. Knegtering, and A. C. Brombacher., Safety lifecycle management. A flowchart presentation of the IEC 61508 overall safety lifecycle model. Quality and Reliability Engineering International, 1999, 15(6), pp.493-500.

[4] Ruijters Enno, Stoelinga Mariëlle., Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review, 2015, 15, pp. 29-62.

[5] DUNJÓ, Jordi, et al., Hazard and operability (HAZOP) analysis. A literature review. Journal of hazardous materials, 2010, 173(1), pp. 19-32.

[6] Habibi, Ehsanollah, et al., The application of the Layer of Protection Analysis (LOPA) in sour water refinery process. International Journal of Environmental Health Engineering, 2013, 2, pp. 1-48.

[7] Baybutt P., Layers of protection analysis for human factors (LOPA-HF). Proc Saf Prog 2002, 21(2), pp. 119-129.

[8] Zeng, Sai X., Tam, Chun M., Tam, Vivian WY., Integrating safety, environmental and quality risks for project management using a FMEA method. Engineering Economics, 2015, 66(1), pp.44-52

[9] Ebrahemzadih, M., Halvani, G. H., Shahmoradi, B., & Giahi, O., Assessment and Risk Management of Potential Hazards by Failure Modes and Effect Analysis (FMEA) Method in Yazd Steel Complex. Open Journal of Safety Science and Technology, 2014, 4(03), pp.127-135.

[10] Goble William M., Brombacher A. C., Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. Reliability engineering & system safety, 1999, 66(2), pp. 145-148.

[11] Keum Jong-Yong, Seo Y. S., Lee J. K., Park J. Y., Measurement of a Diagnostic Coverage for a Digital Signal Processor Board Using an FMEDA. Journal of Applied Reliability, 2008, 8(2), pp. 101-111.

[12] Kim Sung Kyu, Kim Yong Soo, An evaluation approach using a HARA and FMEDA for the hardware SIL. Journal of Loss Prevention in the Process Industries, 2013, 26(6), pp. 1212-1220.

[13] Smith, D. J., & Simpson, K. G. Functional Safety: A straightforward guide to applying IEC 61508 and related standards. Routledge, 2004

[14] Kim, Byung Chul, and Young Jin Kim., Case Study on the Assessment of SIL Using FMEDA. IE interfaces, 2012, 25(4), pp. 376-381.