http://dx.doi.org/10.7471/ikeee.2012.16.2.145

A Study of Software Hazard Analysis for Safety Critical Function in Military Aircraft

Hung-jae Oh*, Jin-pyo Hong*★

Abstract

This paper is the Software Hazard Analysis (SWHA) which will study the managerial process and the technical methode and techniques inherent in the performance of software safety task within the Military Aircraft System Safety program. This SWHA identifies potential hazardous effects on the software intensive systems and provides a comprehensive and qualitative assessment of the software safety. The purpose of this paper is to identify safety critical functions of software in Military A/C. The identified software hazards associated with the design or function will be evaluated for risks and operational constraint to further improve the software design requirement, analysis and testing efforts for safety critical software. This common SWHA, the first time analysis in KOREA, was review all avionics OFP(Operational Flight Program), and focus only on software segments which are safety critical. This paper provides a important understanding between the customer and developer as to how the software safety for the Military A/C will be accomplished. It will also provide the current best solution which may as one consider the necessary step in establishing a credible and cost-effective software safety program.

Key words: software hazard analysis, SW intensive system, safety critical function, risk assessment, avionics OFP

I. Introduction

Software safety, an element of the system safety and software development process, can not be allowed to function independently of the total effort. Both simple and highly integrated multiple systems are experiencing an extraordinary growth in the use of computer and software to monitor and/or control safety critical subsystems of functions. A SW specification error, design flow, or the lack of generic safety critical requirements can contribute to or cause a system failure or erroneous human decision. To achieve an acceptable level of safety for SW used in critical applications, Software Safety engineering must be given primary emphasis early in the requirements definition and system conceptual design process. Safety critical SW must receive continuos management and engineering analysis throughout the development and operational life cycle of the system. SW safety should optimize system safety in the design, development, use, and maintenance of SW system and their integration with safety critical hardware system in an operational environment. SW does not fail in the same manner as hardware. It does not wear out, or have increasing tolerance that result in failures. SW errors are generally errors in the requirements (failure to anticipate a set of conditions that lead to a hazard, or influences of an external component failure on the SW) or implementation errors (coding errors, incorrect interpretation of design requirements). If the conditions occur, the SW does not perform as expected and a failure occurs.[1]

* Department of Information & Communication Eng.. Anyang University

★ Corresponding Author

※ This research was studied on a sabbatical year.
Manuscript received May.25.2012,; revised Jun.15.2012

SW is generally application specific and reliability parameters associated with it cannot be estimated in the same manner as HW is. Development of SW to a SW level does not imply the assignment of a failure rate for that SW. Thus, the probability of SW failure based on reliability cannot be used by the general HW and system risk assessment process as can HW failure rate. Appling probability of this nature of SW, except in purely qualitative items are impractical. Therefore, reliability predictions become a prediction of when the specific condition will occur that cause it to fail. Without the ability to accurately predict a SW error occurrence, alternate methods of hazard categorization must be available when the hazard possesses SW causal factors. During the early phases of the system safety program and SW safety program as part of the SW development process, the prioritization and categorization of hazards is essential for the allocation of resources to the functional area possessing the highest risk potential.[2]

This SWHA present a method of categorizing hazards having SW causal factors strictly for purpose of allocation of resources to the SW development process. This methodology does not provide an assessment of residual risk associated with the SW at the completion of development. However, the execution of the SW safety program, the development and analysis of SW safety requirements and the verification of their implementation in the final SW provide the basis for a qualitative assessment of the residual in traditional terms.

II. SW Hazard Analysis Methodology

1. Analysis Guidelines

The SWHA is an iterative qualitative process of determining safety requirements for SW intensive systems and can be used to help identify safety critical functions, safety critical SW, and general safety requirements or mitigation guidelines. The Fault Hazard Analysis(FHA) is an inductive and qualitative hazard-identifying, analytical tool that can be is used to determine SW hazard conditions, causes of these hazards, and resultant effects to the aircraft system and its operation.[3] FHA will be prepared in a columnar format for the SWHA.

The SWHA is essentially a safety requirements analysis and not associated with the system and the probable causes to the critical hazards. In general, SW that is identified to be a catastrophic hazard cause is safety critical SW. SW bugs that reside in safety critical SW could potentially lead to a hazardous outcome. Unlike HW, the performance of SW is independent on the operating environment and the operating duration. Hence it is important to ensure that safety critical SW is as robust as possible. SW causes or contributions to hazards will be identified at the SW functional level (a SW functions out-of-time or out-of sequence, malfunctions, degrades in function, or does not respond appropriately to system stimuli). In SW intensive systems hazard occurrence will likely be caused by a combination of HW, SW and human errors. These complex initiation pathway will be analyzed for the purpose of identifying hazard mitigation requirements and/or constraints to the HW and SW design and test teams. SW safety is integral to The Total System Safety and The System Safety Engineering and SW Engineering should be responsible for the coordination with System Engineering to perform and document the analysis in accordance with the contractual requirements, if applicable.

2. Software Risk Assessment

Safety critical SW is identified through SW hazard analysis based on the SW risk assessment process. The Software Risk Index(SRI) serves as a guide for the SW safety engineering, SW development and integrity process, and program management to accord the right amount of effort to ensure SW robustness of safety critical SW.

Risk assessment of identified SW hazards will be conducted on the basis of the assigned SW failure condition (SW severity classification) and the SW's control capability or level within the context of the SW causal factors. This risk assessment will focus on the basic principles of system safety and hazard resolution. Specific safety assessment regarding how SW safety influences or is related to hazards will be described in detail in follows.[4][5]

3. Software Failure Condition

The first step in assessment of risk requirement the establishment of SW failure condition (mishap severity) within the context of the system and user environments. SW failure conditions are defined to provide a qualitative measure of the worst credible hazard resulting from SW-intensive-safety-critical systems hazard occurrence caused by a SW error. The general definition of SW failure categories are rationalized and supplementary definitions are typically as Table 1.[7]

Table 1. Software Failure Condition
(Mishap Severity Categories)

Desc'	CAT	Definition
Catas-trophic	I	Could result in death or permanent total disability, or system loss or irreversible severe environmental damage.
Critical	II	Could result in severe injury, permanent partial disability or major system damage, or reversible environmental damage.
Margi-nal	III	Could result in minor injury or system damage, or mitigatible environmental damage.
Negli-gible	IV	Could result in less than minor injury or system damage or minimal environmental damage.

Note) The mishap severity categories are derived and interpreted from MIL-STD-882C and MIL-STD-882D(Appendix A, Table A-1)

4. Software Control Category (SCC)

Software Risk assessment will not be assigned probability of SW failure occurrences. Due to the inherent of SW, the probability of occurrence for HW is an unsatisfactory methode of assessing SW risk. It is recognized that SW failure probability and their contribution to critical functional failures cannot be quantified. There are no techniques to verify SW against quantitative safety requirements. The verification of SW is carried out using a qualitative indicator, the SW development level, defined by most severe failure conditions.[1]

Table 2. Software Control Category (SCC)

SCC	Description	Control Descriptor
I	Failure of the SW or a failure to prevent an event leads directly to a hazard's occurrence.	Time critical of hazard without intervention
II	A. Allowing time for intervention by independent safety system to mitigate the hazard. B. SW item displays information requiring immediate operator action to mitigate a hazard.	Time critical with intervention Display requiring operator control
III	A. Requiring human action to complete the control funct'. There are several, redundant, independent safety measures for each hazardous event. B. SW generates information of a safety critical nature used to make safety critical decisions.	Not time critical requiring operator action Generates information for operator decision
IV	Software does not control safety critical HW systems, and does not provide safety critical information.	Minimal involvement

Note)

1. To determine the level of control of the SW over safety-related functionality, the general definition and suggested Software Control Categoty(SCC) levels are derived and interpreted from MIL-STD-882C(Appendix A, 30.7. a)
2. A: SW control of hazard
   B: SW display safety information for operator

There have been numerous methode of determining the SW's influence on system-level hazards. These do not specifically determine SW-caused hazard probabilities, but instead assess the SW's control capability or level within the context of the SW causal factors. One of the most popular is presented in MIL-STD-882C. In doing so, each SW causal factor can be labeled with a SW Control Category (SCC), given in Table 2, for the purpose of helping to determine the degree of autonomy that the SW has on the hazardous event. Once identified, each safety-critical function should be assessed and categorized against the SCC to determine the level of control of the SW over safety-related functionality.

5. Software Risk Index (SRI) Matrix

The key to developing most SW risk assessment is the characterization of SW risks. The Software Risk Index (SRI) Matrix is based solely upon the SW failure condition of the SW against the level of command or control the SW has safety-critical HW or system function. The matrix is established using the SW failure conditions for the rows and the SW control categories for the columns, see Table 3.

Table 3. Software Risk Index (SRI) Matrix

Condition	Catas-trophic I	Critical II	Marginal III	Negli-gible IV
I	1	1	3	5
II A/B	1	2	4	5
III A/B	2	3	4	5
IV	3	4	5	5

Assigning SRI numbers to each element completes the matrix. A SRI of '1' from the matrix implies that the safety risk is "very high" and requires more design and test rigor than SW with less safety risk. A SRI of '2' to '4' possesses lesser degree of safety risk and requires less design and test rigor than high-risk SW and/or requires acceptance from the managing activity.[8] The SRI ranges between '1' and '5'. A lower SRI implies a more safety critical SW.

III. Software Hazard Analysis Result

1. Identified Subsystems and individual Software

A common SWHA was perform to evaluate and to identify common safety critical function of SW in essential avionics system from KF-16/F-15K/FA-50. The findings will be used to obtain an initial risk assessment of a system, and to identify requisite hazard control and follow on mitigation actions. The identified SW hazards associated with the design or function will be evaluated for risks and operational constraint to further improve the SW design requirement, SW analysis and testing effort for critical SW.

This analysis examines SW components at a gross level to obtain an initial SW safety evaluation of the SW system. In SW intensive, safety critical systems hazard occurrence will likely be caused by a combination of HW, SW, and human errors. These complex initiation pathways will be analyzed for the purpose of identifying hazard mitigation requirements and/or constraints to the HW and SW design and test teams. In case where the safety features are not adequate to eliminate or control a potential hazard, corrective action will be initiated and recommended for incorporation into the design.

The analysis data presented in this study is based on the current configuration of KF-16/F-15K/FA-50. Table 5 illustrates the status of identified individual SW, we call it OFP (Operational Flight Program)[6]

2. Detailed Functional Hazard Analysis

The common SWHA present a detailed functional hazard analysis for each SW failure condition(Total 178). Refer to Table 4 'Sample SWHA Worksheet' illustrates detailed investigation of the SW function to identify the critical failure conditions, their inherent and aircraft operational effects within the design.

Table 4. Sample SWHA Worksheet

Avionic (# of Fun)	OFP Function Description	Effect of Failure Condition (Hazard Description & Rational for Classification)	Risk Assessment		
			CAT	SCC	SRI
FLCC (91)	ability to correctly manage air data sensors	If the FLCS has no redundancy, subsequent failure could result in loss of the aircraft.	I	IIA	1 High
EGI (8)	Prvide attitude information (pitch, roll and horizon)	EGI provides incorrect attitude data to the avionics system. Its may increase significantly increase pilot workload or distress in condition impairing pilot efficiency.	II	IIIB	3 Med
VOR/ILS (10)	provides glideslope and localizer validity information	Ability to landing approach and descent to desired runaway spot will be impaired.	III	IIIB	4 Med
RALT (2)	Provides the aircraft operational range above ground data	Loss of function can result in a slight decrease in safety margin and slight increased workload during a low level flight.	III	IIIB	4 Med
U/VHF (3)	Provide a voice communication	Loss of radio communication redundancy and degraded communication capability.	III	IIIA	4 Med
ICS (6)	Controls volume for the intercom	Loss of audio input volume level control to the intercom has no safety effect.	IV	IIIA	4 Med
Mission Computer (6)	To implement computations for weapon delivery and release	In the event of a MC failure, most primary functions of A-A and AG weapons delivery and release capabilities are lost or degraded.	III	IIA	4 Med
HUD (19)	Information Display of Attitude Indication	A misleading data in the HUD may adversely affect the pilot's ability to recognize and recover from an unusual attitude.	II	IIB	2 Med
UFC (2)	Provides a data entry and control of the HUD	When the MFD DISP switch is in the decouple position, the aft seat IUFC function transitions from a repeater mode to an independent cockpit to support full mission functionality.	IV	IIIA	4 Med
MFD (6)	Provides head-down displays during the mission	It is displayed data with other instrumentation, therefore it increases in pilot work load in VFR and IFR conditions.	III	IIIB	4 Med
SMS (6)	Provides weapons release function	Potential personnel injury or damage of equipment on ground in vicinity of dropped store caused by inadvertent store release signal	II	IIIA	3 Med
FCR (1)	Controls all the units and processes in the radar,	Loss of function has no effect on aircraft operational safety. It affects mission capability only.	IV	IV	5 Low
IFF (4)	provide selective aircraft identification	Loss of function would create a increased workload on the pilot. But no effect on aircraft operational safety.	IV	IV	5 Low
Recording System (4)	A self-contained, crash hardened, solid state recording system	Loss of function has no effect on aircraft operational safety. It affects review/analysis and accident investigation only.	IV	IV	5 Low
CMDS (4)	Dispenses payloads	Failure conditions would not reduce aircraft safety.	IV	IV	5 Low
MIDS (6)	TACAN bearing provides radio navigation functions	Loss of TACAN bearing function and navigation would not increase the pilot's workload, it would slightly reduce the safety margins.	IV	IV	5 Low

Table 5. Identified OFP for essential avionics

Avionics	Software	Remark
Flight Control	FLCC OFP	Redundant Flight control computing
Navigation	EGI OFP	Primary source of Nav.
	VOR/ILS OFP	Secondary source of Nav.
	RALT OFP	Secondary source of navigation
Communi -cation	U/VHF OFP	Redundant radio communication
	ICS OFP	Redundant inter communication
Mission Computer	FC OFP	Primary mission computing
	HUD OFP	Head up display
	MFD OFP	Head down multifunction display
	SMS OFP	Store management
	IUFC OFP	Data entry avionics & control HUD display
RADAR	FCR OFP	Radar control
Identi-fication	IFF OFP	Provide selective A/C identification
Electronic Warfare	RWR OFP	Report the presence of emitter
	CMDS OFP	Capable of dispensing chaff/flare
Recording System	VADR OFP	Records specified parameters from the various A/C systems
	DTRS OFP	Recording specified video & audio
Data-Link	MIDS OFP	Data communication with TACAN capability

3. Risk Assessment Result

A risk for individual SW has been assessed. Decisions regarding resolution of identified hazards are based on assessment of the risk involved. To aid the achievement of the objectives of system safety, SW risks are characterized as to SW failure condition and control categories.

Decision regarding resolution of identified higher risk indexes of SW hazard will be based on assessment of the risk involved. SW risk index values are used in grouping individual hazards into SW risk categories. Refer to Table 6, total potential SW failure conditions are identified and their risk assessment values are assessed in SWHA for each OFP function.[9]

Table 6. Result of SRI Matrix

Cond'	Cata' I	Criti' II	Marg' III	Negl' IV	Total
I	-	-	-	-	-
IIA/B	28	27	64	-	119
IIIA/B	-	6	19	10	35
IV	-	1	4	19	24
Total	28	34	87	29	178

Unlike the HW related Mishap Risk Index, a low Software Risk Index(SRI) number does not mean that a design is unacceptable. It just reflects the degree of SW control over the system and indicates that greater resources need to be applied to the analysis and testing of the SW and its interaction with the system. Simply, this SRI will determine the scope of development and verification plan for the safety related SW. The SRI matrix does not consider the likelihood of a SW caused hazard occurring in its assessment. However, through the successful implementation of a SW safety integrity process, the likelihood of SW contributing to a hazard occurrence will be greatly reduced.

A SW risk assessment, as shown in Table 7 will be used to recommended or determine the scope of development and verification for the each subsystems SW. Assigning SRI numbers to each SW element completes the matrix.[10]

● A SRI of '1' from the matrix implies that the SW exercises control over potentially catastrophic or critical HW system without intervention and safety risk is very high. This high risk category requires more significant safety design and test rigor than SW with less safety risk.

● A SRI of '2' to '4' from the matrix implies that the SW control of catastrophic to marginal hazard is reduced or SW controls less significant hazards. These subsystems SW possesses lesser degrees of safety risk and requires less design and test rigor than high risk SW. However, safety design and in depth testing is required and it requires acceptance from the managing activity.

● A SRI of '5' from the matrix implies that the SW control non critical HW system or does not provide safety critical information. Low level safety analysis and/or testing are required.

Table 7. Suggested Criteria for avionics OFP

OFP	SRI (Risk)	Suggested Criteria
FLCS	1 (High)	SW controls catastrophic or critical hazard. Significant analysis and testing is required.
EGI VOR RALT U/VHF FC HUD MFD SMS	2~4 (Medium)	SW control of catastrophic or critical is reduces, but still significant. Requirements and design analysis and in-depth testing is required.
ICS UFC FCR IFF DTRS CMDS MIDS	5 (Low)	SW control of less significant hazards. Low level analysis and testing is acceptable.

IV Conclusion

System Safety performing the SW requirement hazard analysis will accomplished the SW safety analysis task. This task ensures that SW is considered in its contribution to hazard occurrence. This task should be defined and common to overall system safety program. Software Hazard Analysis (SWHA) for the SW subsystems has been accomplished to investigate the critical failure conditions, their inherent and aircraft operational effect within the design

This comon SWHA can be used to help identify in Military A/C :

● Safety Critical Software Function

● Safety Criticality of each OFP

● General Safety Requirement or Mitigation

Also, through this risk assessment will be used to recommended or determine the scope of development and verification for the each avionics OFP.

This study will be good reference to make SW development plan for next generation Korea Fighter Development Program.

References

[1] Debra S. Herrmann, *"Software Safety and Reliability"* IEEE Computer Society, Los Alamitos, pp.18-27, pp.160-190, 2010.

[2] U.S Airforce *"Weapon Systems Software Management Guidebook"* Secretary of the Air Force for Aquisition, ver.1 pp73-82, Aug. 2008.

[3] DO-178B *"Software Consideration in Airborne system and Equipment Certification"* RTCA Inc. Washington D.C, pp. 5-8, 1992

[4] Lawrwnce Livermore National Lab *"Software safety Hazard Analysis"* U.S. Nuclear Regulatory Commission, NASA-GB-8719 pp.22-32, 2004.

[5] Joint Services Software Safety Committee *"Software System Safety Handbook"* Joint Services Computer Resources Management Group, pp.63-73, Dec. 1999.

[6] Jinpyo Hong, Hungjae Oh *"A study of Design Concept for Mission computer in KFX program",* The 7th Conference on National Defence Technology, Vol 1 pp.249-256, July 2011.

[7] MIL-STD-882C/D *"Standard Practice for System Safety"*, USA Department of Defence, Appendix A, Feb. 2000.

[8] Mats P.E.Heimdahl *"Formal Verification of Flight Critical SW"* AIAA Guidance, Navigation and Control Conference, Aug. 15-18 2005.

[9] Andrew Kornecki *"SW Certification for Safety Critical System : A Status Report"*, Processing of the International Multiconference on Computer Science Technology, pp.665-672, 2008.

[10] Chang Jin Kim *"Formalism-Based Defence Safety/Security Critical SW Development & Certification Criteria"* Korea Institute of Military Science and Technology, Vol 10. Mar. 2007.

BIOGRAPHY

Hung-jae Oh(Member)

1985 : B.S degree in Electronic Engineering, ROK Air Force Academy.

1991 : M.S degree in Electronic Engineering, Hanyang Univ.

2009 ~ Present : ROK Military Aircraft Airworthiness Certification Center,

2010 ~ Present : Ph.D Course in Information and Communication Engineering, Anyang University.

<Interests Area> Software Safety, Avionics OFP, Airworthiness, Computer Network.

Jin-pyo Hong(Member)

1980 : B.S degree in Electronic Engineering, Hanyang Univ.

1982 : M.S degree in Electronic Engineering, Hanyang Univ.

1990 : Ph.D degree in Electronic Engineering, Hanyang Univ.

1983 ~ 1991 : A Research Institute of LG Electronics

1991 ~ Present : Professor Department of Information and Communication Engineering, Anyang University.

<Interests Area> Fiber Optic Communication, Computer Network.