JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 20(1): 1-7, Feb. 2016

국제표준에 기반한 KASS 개발보증레벨 할당

Allocation of Design Assurance Level for KASS Based on International Standards

배 동 환
한국정보통신기술협회 소프트웨어시험인증연구소

Dong-hwan Bae
Software Testing & Certification Laboratory, Telecommunications Technology Association, Gyeonggi-do 13591, Korea

[요 약]

국토교통부는 2014년부터 한국형 위성보강항법시스템 (SBAS; satellite based augmentation system)인 KASS (Korea augmentation satellite system) 개발·구축 사업을 진행 중이다. KASS는 실제 운영 중 문제가 발생할 경우 인명 및 재산피해와 연결될 수 있어 시스템 개발을 위한 안전성 평가가 매우 중요하다. 안전성 평가의 핵심은 위해 식별과 심각도 판정에 따른 개발보증레벨 (DAL; design assurance level) 할당이다. 본 연구에서는 항공시스템의 안전성 평가 방법론을 제시하는 국제표준인 SAE (society of automotive engineers) ARP4761 (aerospace recommended practice)을 기반으로 KASS 및 그 하위시스템에 대해 개발보증레벨 할당을 수행한다. 이것은 전체 시스템 안전성 평가의 첫 단계이므로 향후 KASS 개발·구축 사업의 안전성 평가에 활용될 수 있다.

[Abstract]

Since 2014, MOLIT (Ministry of Land, Infrastructure, and Transport) is carrying out a KASS project to develop and construct Korean SBAS. KASS can cause damage of human & properties if it has some problem during operation. Therefore, system safety assessment for KASS development is very important. Principal point of system safety assessment is the allocation of DAL(design assurance level) based on the hazard identification and classification. In this parer, the author conducts the allocation of DAL for KASS & its sub-systems based on the international standard(SAE ARP4761), which suggests a best practice of aviation system safety assessment. The result of this paper are the first step of system safety assessment, and can be used for further system safety assessment of KASS project.

Key word : Korea augmentation satellite system, System safety assessment, Functional hazard assessment, Design assurance level.

http://dx.doi.org/10.12673/jant.2016.20.1.1

Received 31 January 2016; **Revised** 5 February 2016
Accepted (Publication) 17 February 2016 (28 February 2016)

***Corresponding Author; Dong-hwan Bae**

Tel: +82-31-704-0515
E-mail: dhwan@tta.or.kr

Ⅰ. 서 론

최근 항공기를 통한 여객 및 물류 수송의 양이 폭발적으로 증가하면서, 효율적이고 안전한 항행을 이룩할 수 있도록 하는 항행안전시설의 중요성이 부각되고 있다. 일반적으로 널리 알려진 GPS (global positioning system)는 단독으로 사용 시 항행 사용자의 안전을 보장하기 위해 요구되는 사항들을 만족시키지 못한다. 이를 보완하기 위해 개발된 SBAS는 기존 GPS에 더해 정지궤도위성 (GEO; geostationary earth orbit satellite)과 지상시스템을 활용하여 정확성, 무결성, 연속성, 가용성 등을 향상시킨 항법 서비스를 제공한다.

미국, 유럽, 일본, 인도 등 항공선진국들은 이미 SBAS를 구축하여 활용하고 있으며 한국의 국토교통부 역시 이러한 흐름에 발맞추어 국제민간항공기구 (ICAO; International Civil Aviation Organization)에서 제시하는 기술기준을 만족시키는 한국형 위성보강항법시스템 (SBAS; satellite based augmentation system)인 KASS (Korea augmentation satellite system) 개발·구축 사업을 진행 중이다.

SBAS가 항행 사용자의 안전성을 높이기 위한 시스템이란 것은, 역으로 시스템 개발이 잘못 이루어질 경우 사용자의 안전에 위협을 만들 수 있다는 뜻이다. 따라서 SBAS 개발·구축을 위해서는 개발 초기부터 시스템 안전성 평가 절차를 수행하여 시스템이 만족시켜야 하는 개발보증레벨을 설정하고, 시스템에서 유발될 수 있는 위해들을 식별하고 제거 및 경감시키는 과정이 필수적이다.

SAE (Society of Automotive Engineers)에서 제정되고 발표된 ARP4761 (aerospace recommended practice)은 항공분야에서 시스템 안전성 평가를 위해 널리 사용되는 국제 표준으로서 기능위해평가 (FHA; functional hazard analysis), 예비시스템안전성평가 (PSSA; preliminary system safety assessment), 시스템안전성평가 (SSA; system safety assessment) 등의 절차와 공통원인분석 (common cause analysis), FTA (fault tree analysis), FMEA (failure mode and effect analysis) 등의 방법론에 대해 가이드라인을 제시하고 있다[1].

KASS 역시 ARP4761을 활용하여 안전성 평가를 수행할 필요가 있으며, 본 논문에서는 그 첫 단계인 FHA 절차를 바탕으로 KASS 및 그 하위시스템에 대한 개발보증레벨 할당을 수행한다.

본 논문의 Ⅱ장에서는 KASS 개요를 살펴보고 기술기준에 따른 KASS 전체 시스템에 대한 개발보증레벨을 설정한다. Ⅲ장에서는 FHA 절차에 따라 KASS 최상위 기능을 식별하고, 식별된 기능에 몇 가지 분류의 고장 모드를 적용하여 위해를 식별한 후, 그 심각도에 따라 등급을 분류하여 각 하위시스템에 대한 개발보증레벨을 도출한다. Ⅳ장에서는 앞에서의 결과를 정리하고 KASS 개발·구축 사업에 활용 방안을 제시한다.

Ⅱ. KASS 구성 및 개발보증레벨

2-1 KASS 하위 시스템 구성

KASS는 표 1에서 볼 수 있듯이 크게 5가지의 지상시스템과 정지궤도위성으로 구분된다.

정지궤도위성은 약 36,000 km 상공에서 지구자전과 같은 주기로 지구 주위를 공전한다. 즉, 정지궤도위성은 항상 지구상의 같은 지역 위에 떠있게 되므로 특정 지역을 대상으로 하는 방송·통신용 위성으로 많이 사용된다. KASS 역시 한국지역을 대상으로 항상 운영되어야 하는 시스템이므로 정지궤도위성을 활용한다.

지상시스템은 통합운영국 (KCS; KASS control station), 중앙처리국 (KPS; KASS processing station), 위성통신국 (KUS; KASS uplink station), 기준국 (KRS; KASS reference station) 및 통신 네트워크로 구성되며 KASS의 가용성을 최대화하기 위해 국내 여러 곳에 분산되어 설치된다. 각 지상시스템이 담당하는 주요 역할은 표 1과 같다.

2-2 KASS 개발보증레벨 설정

개발보증레벨은 어떤 시스템 혹은 그 구성요소에 할당할 수 있는 속성으로서 해당 시스템/구성요소의 안전성을 보장하기 위해 개발이 얼마나 엄격한 과정을 거쳐 이루어져야 하는지에 대한 기준이다. 일반적으로 시스템의 개발보증레벨은 시스템의 최상위 기능을 바탕으로 관련된 위해를 식별하고 그 심각도에 따라 결정하게 된다.

표 1. KASS 하위시스템과 기능 요약
Table 1. Summary of sub-systems & functions of KASS.

sub-system	summary of function
KCS	Monitors and controls system functions and status. Also provides operation and maintenance.
KPS	Generates corrections and integrity bounds. Also formats messages compliant with the SBAS user interface.
KUS	Uplinks signal carrying SBAS message from KPS. Also provides monitoring for signal-in-space from GEOs.
KRS	Collects ranging and other data from GPS and GEOs.
Data Network	Transmission media for data between sub-systems.
GEO	Broadcast SBAS messages from KUS to users.

표 2. APV-I급 공간신호 성능 요구사항
Table 2. Siganl-in-space performance requirements for APV-I.

item	performance requirements
accuracy horizontal (95%)	16.0 m (52 ft)
accuracy vertical (95%)	20 m (66 ft)
integrity	$1-2\times10^{-7}$/approach
time-to-alert	10 sec
continuity	$1-8\times10^{-6}$/in any 15 sec
availability	0.99 ~ 0.99999

KASS의 경우 국내 항공법에서 명시하는 APV-I (approach with vertical guidance - I)급 성능을 목표로 개발 중이며, 성능적합증명을 받아야 하기 때문에 해당 성능에 대한 기술기준을 만족시켜야 한다. 이 기술기준은 표 2 와 같이 ICAO 표준에서 제시하는 공간신호 성능 요구사항과 같다[2]-[4].

수평 및 수직 정확도(accuracy)는 SBAS 신호를 사용하여 측위된 항공기 위치의 허용오차범위이다. 수평방향으로 16.0 m 이내, 수직방향으로 20 m 이내의 오차를 유지해야만 APV-I급 착륙 접근 절차를 밟을 수 있다.

무결성(integrity)은 SBAS를 통해 제공되는 보정정보에 대한 신뢰도이다. 표 2에서 제시하는 $1-2\times10^{-7}$/approach 는 1000만 번의 공항 착륙 접근 시도 중 무결성 오류가 2회까지만 허용된다는 뜻이다. 정확도가 떨어지는 상황이라 해도 무결성만 보장되면 사용자는 그 상황을 정확히 인지할 수 있으므로 안전성을 저해하지 않는다. 즉, 안전성 평가에 직결되는 요구사항이 바로 무결성이다.

연속성(continuity)은 서비스의 지속되는 능력을 나타낸다. 표 2에서 제시하는 $1-8\times10^{-6}$/in any 15sec 는 단위 시간(15초) 100만 번 중에 서비스 중단이 발생하는 경우가 8번까지 허용된다는 뜻이다. 가용성은 다른 성능지표를 모두 통합하여 SBAS 서비스가 가용한 시간에 대한 백분위 표시이다. KASS 에서는 현재 0.9999를 목표로 하고 있지만 확정되지는 않았다.

ICAO 표준은 SBAS 운영에 대한 경험과 지식을 바탕으로 무결성 목표를 설정했기 때문에 유사 시스템을 대상으로 선행된 최상위 안전성 평가의 결과라고 볼 수 있다. 이런 경우, 시스템이 만족해야 할 최종 안전 목표가 먼저 설정되었으므로 이를 바탕으로 개발보증레벨을 정할 수 있다.

APV-I급 무결성 조건으로 설정된 $1-2\times10^{-7}$/approach 라는 확률을 ARP4761에서 표 3과 같이 제시하는 안전 목표 확률과 비교하면, KASS의 개발보증레벨이 C임을 알 수 있다.

정량적인 확률 이외에도 정성적인 심각도 역시 고려하여 최종 개발보증레벨을 설정해야 한다. 표 2에서 무결성 조건의 단위가 'approach'를 기반으로 설정된 것을 보면 공항 접근 순간

표 3. 위해 심각도와 목표 확률의 관계 및 개발보증레벨
Table 3. Hazard severity as related to probability objectives and design assurance level.

probability	severity	DAL
10^{-9}p	Catastrophic All failure conditions which prevent continued safe flight and landing	A
10^{-7}p	Hazardous - Large reduction in safety margins or functional capabilities - Higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - Adverse effects upon occupants	B
10^{-5}p	Major - Significant reduction in safety margins or functional capabilities - Significant increase in crew workload or in conditions impairing crew efficiency - Some discomfort to occupants	C
10^{-3}p	Minor - Slight reduction in safety margins - Slight increase in crew workload - Some inconvenience to occupants	D
1	No Effect	E

이 가장 큰 위해 발생 가능 상황이라는 것을 알 수 있다.

공항에는 SBAS 이외에도 ILS (instrument landing system), GBAS (ground based augmentation system) 등 항공기 착륙을 돕기 위한 항행안전시설이 존재하는 경우가 대부분이므로 KASS의 무결성이 보장되지 않더라도 파국(catastrophic)이 발생할 가능성은 거의 없겠지만, 조종사나 관제사의 판단 실수 등에 따라 위험(hazardous) 수준의 상황은 발생할 수 있다.

따라서 안전 목표 확률과 정성적 심각도를 동시에 고려하여 KASS의 최종 개발보증레벨은 보수적으로 B로 설정한다.

Ⅲ. KASS 하위 시스템 개발보증레벨 도출

앞서 KASS 전체 시스템에 대한 개발보증레벨은 설정하였지만 해당 개발보증레벨은 KASS 운영 중 최고 심각도를 가진 위해(hazard)를 기준으로 설정되었다. KASS 하위 요소 중에는 그보다 낮은 심각도를 가진 위해에만 관련 있는 부분도 많은데, 이 요소들까지 모두 시스템 최고등급 개발보증레벨을 적용하여 개발하면 비용과 시간의 낭비가 크다.

따라서 KASS의 하위 시스템별 개발보증레벨을 설정하기 위해 그림 1과 같이 FHA 절차에 따라 기능 위해 식별과 심각도 판정을 수행한다.

3-1 시스템 가정 (assumption)

FHA의 시작점은 시스템 기능 및 위해 식별을 할 때 적용된

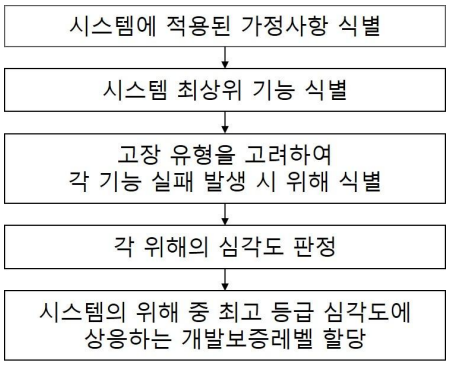

그림 1. FHA 절차에 따른 개발보증레벨 할당 흐름
Fig. 1. DAL allocation flow according to FHA process.

가정을 명시하는 것이다. 시스템은 같은 기능 실패라 해도 운영 상황에 따라 유발되는 위해의 심각도가 달라지기 때문이다.

KASS 기능 위해 식별을 위한 주요 가정 사항은 다음과 같다.

- 사용자 SBAS 수신기는 무결성을 보장 : KASS 개발·구축은 사용자 부분을 제외한 범위에서 진행되므로 사용자의 SBAS 수신기에서 발생하는 오류에 대해서는 고려하지 않는다.

- APV-I급 성능 : KASS 개발·구축 사업의 목표는 APV-I급 SBAS 이므로 해당하는 목표 성능과 시나리오에 대해서만 위해 식별을 수행한다.

- 정지궤도위성 무결성 : KASS 개발·구축 사업에서 정지궤도위성은 인증이 완료된 개체를 임차로 도입하므로 안전성 평가의 범위에서 제외한다.

3-2 KASS 기능 식별

FHA에서 시스템 위해 요소를 찾아내기 위해 제안하는 첫 번째 절차는 시스템 최상위 수준에서의 기능 식별이다. 시스템에 대해 매우 잘 알고 있는 엔지니어라 하더라도, 체계적인 절차 없이 위해 요소를 즉흥적으로 머릿속으로만 떠올려서는 모든 위해 요소를 파악하기 힘들다. 따라서 시스템이 가지는 기능을 리스트로 정리하고 각 기능과 연관되어 발생할 수 있는 위해를 빠짐없이 파악하도록 제안하고 있다. 표 1에서 하위시스템별로 요약된 기능은 최상위 기능이라고 보기에도 서술 범위가 다소 넓어 위해 식별에 바로 활용하기는 무리가 있으므로, 표 4처럼 기능을 조금 더 상세화하여 식별할 필요가 있다[5].

표 4 의 기능 리스트에서 FN-02와 FN-07의 경우, 통신 네트워크를 통한 하위 시스템 간 데이터 전달이라는 점에서 실질적으로 같은 기능이므로 하나의 기능으로 통합하여 위해 식별을 진행한다.

3-3 기능 위해 식별

FHA에서 기능 식별 이후 제안하는 단계는 각 기능에 고장 모드를 접목하여 관련된 위해를 식별하는 것이다. 기능의 고장

표 4. KASS 기능 리스트
Table 4. KASS function list.

function number	function	description
FN-01	measurements collection	KRS collects measurements from GPS satellites and GEO satellites
FN-02	measurements transfer	KRS transfers measurements to KPS through data network
FN-03	correction generation	KPS generates correction data for satellite orbit/clock and ionosphere
FN-04	integrity bound generation	KPS generates integrity bound of the correction data for satellite orbit/clock and ionosphere
FN-05	integrity bound check	KPS check the generated integrity bound data
FN-06	SBAS message generation	KPS formats SBAS message with correction data and integrity bound data
FN-07	SBAS message transfer	KPS transfers SBAS message to KUS through data network
FN-08	SBAS signal generation	KUS modulates SBAS message and PRN code into carrier signal after applying FEC(forward error correction)
FN-09	time synchronization	KUS synchronizes SBAS signal timing with GPS signal timing, and performs CCC(Code Carrier Coherence)
FN-10	SBAS signal uplink	KUS uplinks SBAS signal to GEO
FN-11	SIS integrity check	KUS checks the integrity of SIS from GEO
FN-12	system monitoring and control	KCS monitors and controls other sub-system
FN-13	data collection and analysis	KCS collects and analyzes all data from operating system

은 단순히 한 가지 유형이 아니라 3가지 고장 모드와 조합된 여러 가지 유형이 발생할 수 있다. 다음은 고장모드 3가지에 대한 설명이다.

- 기능의 미동작 : 기능이 아예 동작하지 않는 경우
- 기능의 오동작 : 기능이 예상되는 형태가 아닌 다른 형태로 동작하는 경우
- 기능의 지연 : 기능의 동작이 예상되는 시점보다 늦게 수행되는 경우

표 5. 식별된 위해 리스트
Table 5. List of identified hazard.

hazard number	hazard
HZ-01	KRS does not collect measurements from satellites
HZ-02	Collected measurements have errors in KRS
HZ-03	Delay exists during collecting measurements
HZ-04	KPS does not generate correction data
HZ-05	Generated correction data have errors in KPS
HZ-06	Delay exists during generating correction data
HZ-07	KPS does not generate integrity bounds
HZ-08	Generated integrity bounds have errors in KPS
HZ-09	Delay exists during generating integrity bounds
HZ-10	Safety computer does not check integrity bounds
HZ-11	Safety computer makes errors in checking integrity bounds
HZ-12	Delay exists during checking integrity bounds
HZ-13	KPS does not generate SBAS message
HZ-14	Generated SBAS message have errors in KPS
HZ-15	Delay exists during generating SBAS message
HZ-16	KUS does not generate SBAS signal
HZ-17	Generated SBAS signal have errors in KUS
HZ-18	Delay exists during generating SBAS signal
HZ-19	KUS does not perform clock synchronization & CCC
HZ-20	KUS makes errors in performing clock synchronization & CCC
HZ-21	Delay exists during performing clock synchronization & CCC
HZ-22	KUS does not uplink SBAS signal
HZ-23	KUS makes errors in uplinking SBAS signal
HZ-24	Delay exists during uplinging SBAS signal
HZ-25	KUS does not check SIS integrity
HZ-26	KUS makes errors in checking SIS integrity
HZ-27	Delay exists during checking SIS integrity
HZ-28	KCS does not monitor and control other sub-systems
HZ-29	KCS makes errors in monitoring and controling other sub-systems
HZ-30	Delay exists during monitoring and controling other sub-systems
HZ-31	KCS does not collect and analyze system operation data
HZ-32	KCS makes errors in monitoring and controling other sub-systems
HZ-33	Delay exists during monitoring and controling other sub-systems
HZ-34	Loss of transferring data between sub-systems
HZ-35	Errors in transferred data between sub-systems
HZ-36	Delay of transferring data between sub-systems

표 4 기능 리스트의 각 기능과 3가지 고장 모드를 조합하면 표 5와 같이 총 36가지의 위해를 식별할 수 있다. 앞서 언급했듯이 FN-02와 FN-07은 실질적으로 중복된 기능이므로 하나의 기능으로 통합하여 위해를 식별했으므로 기능 리스트 갯수의 3배가 아닌 36가지의 위해가 식별되었다. 일반적으로 식별된 각 위해는 각자 다른 수준의 심각도를 가지며, 심각도가 '영향 없음 (no effect)'으로 판단되는 위해의 경우 더 이상 안전성 평가에서 고려 대상이 아니다.

3-4 위해의 심각도 판정

KASS는 지상시스템이므로 KASS가 발생시킬 수 있는 위해들이 사용자(항공기)에 직접적으로 다양한 형태의 위험을 전달하지는 않는다. 항공기와 KASS 간의 인터페이스를 생각해보면 정지궤도위성을 통해 전달되는 SBAS 신호와 KASS 운영센터로부터 시작되는 NOTAM (notice to airman) 2가지 밖에 없다. 즉, 사용자는 이러한 제한된 인터페이스를 통해 전달받은 데이터에 의해서 몇 가지 제한된 상황에 직면하게 된다. 그림 2에서 이러한 상황의 종류를 정리하고 있으며, 식별된 위해의 심각도는 서비스 사용자인 항공기가 그 중에서 어떤 상황에 이를 수 있는가를 기준으로 판정하게 된다.

그림 2에서 case3의 경우, 무결성 문제가 있지만 SBAS 메시지에 포함된 무결성 보장 정보 혹은 NOTAM 등을 통해 문제를 인식하고 즉시 SBAS 외 다른 항행안전시설을 활용한 항행이 가능하므로 위해 심각도 분류에서 경미(minor)에 해당한다. case4의 경우 무결성 문제 상황을 모르고 계속 비행하게 되므로 위해 심각도 분류에서 위험(hazardous)에 해당한다. Case2는 정상적인 일반 상태이며 case1은 일종의 false alarm이지만 사용자의 위험을 만들지는 않으므로 영향 없음(no effect)로 볼 수 있다. 앞서 식별된 위해들은 결국 이 4가지 case 중 한 가지로 연결되며, 그 것이 어느 case이냐에 따라 결국 위험, 경미, 영향 없음 중 하나를 판정받게 된다.

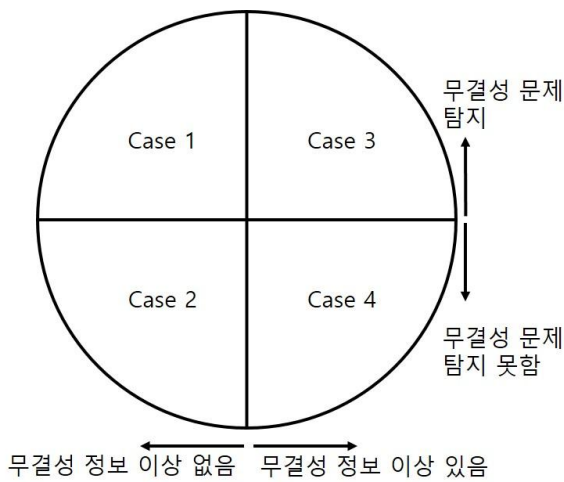

그림 2. 사용자(항공기) 조건 분류도
Fig. 2. Diagram of user(aircraft) conditions.

표 6. 위해의 심각도 판정 결과
Table 6. Severity of hazards.

severity	hazard number
Hazardous	HZ-02, HZ-10, HZ-11, HZ-12, HZ-17, HZ-20, HZ-25, HZ-26, HZ-27
Minor	HZ-01, HZ-03, HZ-04, HZ-05, HZ-06, HZ-07, HZ-08, HZ-09, HZ-13, HZ-14, HZ-15, HZ-16, HZ-18, HZ-19, HZ-21, HZ-22, HZ-23, HZ-24, HZ-28, HZ-29, HZ-30, HZ-34, HZ-35, HZ-36
no effect	HZ-31, HZ-32, HZ-33

예를 들어, HZ-31부터 HZ-33은 보정 정보나 그 탐지에 대해 아무런 영향을 못 미치므로 case1 또는 case2 에 해당되어 영향 없음을 부여받게 된다. HZ-4 혹은 HZ-5의 경우 보정 정보 이상을 초래하므로 위험에 해당한다고 생각할 수 있지만, KPS의 safety computer를 통해 무결성 감시 과정에서 탐지되므로 case3에 해당되어 경미를 부여받게 된다. HZ-11의 경우, 혹은 HZ-17과 HZ-26이 동시에 발생하는 경우는 case4에 해당되어 위험을 부여받게 된다. 여러 기능의 조합 실패인 경우 이와 같이 높은 심각도 판정을 받을 수 있으므로 주의하여 식별해야 한다.

앞서 식별된 모든 위해에 대해 심각도 판정을 수행한 결과는 표 6과 같다. 위험에 해당하는 위해들을 살펴보면 중앙처리국, 위성통신국 및 기준국에서 수행되는 기능임을 알 수 있다. 즉, 이 3가지 하위시스템은 경미나 영향 없음으로 분류된 위해들과 무관하게 개발보증레벨 B를 할당받는다. 경미에 해당하는 위해들을 살펴보면 모든 하위시스템의 기능들이 포함되어 있다. 즉, 아직 개발보증레벨을 할당받지 못한 통합운영국과 통신 네트워크는 레벨 D를 할당받는다.

영향 없음으로 분류되는 HZ-31, HZ-32, HZ-33는 통합운영국의 기능에 속하는데, 이 기능을 담당하는 구성요소가 통합운영국 내 다른 부분과 구분(partitioning) 설계된다면 이 부분에 대해서는 안전성 평가를 더 이상 진행하지 않아도 되고 일반적인 품질보증 활동을 통해 개발을 수행하면 된다. 구분 설계는 안전성 평가 방법론 중 한 가지인 공통 원인 분석을 통해 수행되어야 하지만 본 논문의 범위를 벗어나므로 추가적인 설명은 진행하지 않는다.

결론적으로 KASS 지상 하위 시스템에 대해서는 그림 3 과 같이 개발보증레벨이 할당된다.

그림 3. 하위 시스템 개발보증레벨(DAL)
Fig. 3. DAL of sub-systems.

Ⅳ. 결 론

본 논문에서는 시스템 안전성평가 표준인 ARP4761을 기반으로 한국형 SBAS인 KASS의 개발보증레벨 설정을 수행하였다. KASS 전체 시스템에 대해서는 성능적합증명 기준 즉, ICAO에서 제시하는 SBAS 무결성 목표값을 기반으로 개발보증레벨을 설정하였고, 하위 시스템에 대해서는 FHA 절차에 따라 기능 위해 식별 및 심각도 판정을 수행하여 개발보증레벨을 도출하였다.

본 논문에서 수행된 FHA는 최상위 수준의 기능을 기반으로 수행된 것이고, 실제 하위 시스템과 SW/HW 모듈 개발까지 연결되기 위해서는 각 하위시스템의 기능을 더욱 세분화하여 기능 리스트를 작성하고 시스템 수준의 FHA를 다시 수행할 필요가 있다. 하위 시스템 내부에서도 구분 설계 개념을 적용해 하위 시스템 내 모듈별로 서로 다른 개발보증레벨을 가질 수 있으므로, 개발 비용 및 시간 절감을 위해 낮은 개발보증레벨로 개발해도 되는 구성요소를 가능한 식별해내는 것이 좋다. 시스템 수준의 FHA 수행 중 새로운 위해가 발견되거나 그 심각도가 해당 하위시스템에 할당된 것보다 높은 경우 최상위 FHA로 피드백을 주어 업데이트할 필요가 있다.

KASS 가 만족해야 할 무결성 기준인 $1\text{-}2\times10^{-7}$/approach은 FTA 등의 기법을 통해 각 하위 시스템의 목표 안전 확률로 할당되고, 또 다시 하위 시스템 내 각 SW/HW 모듈로 더욱 나뉘어 할당될 것이며, FTA 최하위 수준의 모듈과 기능들은 FMEA 등을 통해 위해 제거 및 경감 활동을 수행하여 목표 안전 확률을 달성할 수 있도록 해야 한다.

ARP4761에서 FHA 다음 단계로 제시하고 있는 PSSA 에서는 각 위해를 제거 혹은 경감시키기 위한 안전 요구사항을 설정하여 KASS 시스템 설계에 반영하고 확인하는 작업을 수행한다. FHA에서 식별된 위해는 이러한 PSSA 절차의 시작점으로 활용되며, FHA -> PSSA -> SSA로 이어지는 추적성을 확실하게 유지해야 한다.

위와 같은 내용들은 각각이 SBAS에 대한 전문성과 경험을 바탕으로 노력을 필요로 하는 작업으로서 KASS 개발·구축 사업단에서 추가적인 안전성 평가를 지속적으로 수행할 필요가 있다.

감사의 글

본 연구는 국토교통부 항공안전기술개발사업의 연구비(14ATRP-A085964-01) 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

참고 문헌

[1] SAE International, ARP4761 – Guideline and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE Inc., Dec. 1996.

[2] Korea Government, Aviation Act, Article 80-2, “Performance conformity certification of navigation safety facilities,” Mar. 2013.

[3] MOLIT, Public Notice, Article 2015-305, “Technical standards for inspection of performance conformity certification of navigation safety facilities,” May. 2015.

[4] ICAO, Annex 10 to the convention on international civil aviation, Volume 1 – Radio Navigation Aids, International Standards and Recommended Practices, 6th edition, p.3-70, Jul. 2006.

[5] KASS Program Office, Final report of the foundation study for KASS development and construction, Korea Agency for Infrastructure Technology Advancement, Jun. 2014.

배 동 환 (Dong-Hwan Bae)

2007년 2월 : 서울대학교 기계항공공학부 (공학사)
2009년 2월 : 서울대학교 기계항공공학부 (공학석사)
2009년 2월 ~ 2015년 4월 : 삼성전자 무선사업부 책임연구원
2015년 5월 ~ 현재 : 한국정보통신기술협회 SW시험인증연구소 선임연구원
※관심분야 : 항행안전시설 개발/검사/인증, 시스템 안전성 평가