

A-SMGCS 기능 위험 평가 사례 연구

Case Study for Functional Hazard Assessment of A-SMGCS

이 홍석^{1*} · 조상훈² · 최형석²

¹한국산업기술시험원 IT안전기술센터

²인천국제공항공사

Hongseok Lee^{1*} · Sanghoon Jo² · Hyungseok Choi²

¹IT Safety Engineering Center, Korea Testing Laboratory, Daejeon 305-500, Korea

²Incheon International Airport Corporation, Incheon 22382, Korea

[요 약]

안전과 관련된 CNS/ATM 시스템의 개발은 안전 평가 활동을 필요로 한다. 안전 평가에는 기능 위험 평가를 포함하며, 이는 시스템의 위험한 상황을 감소시키기 위한 시스템 안전 요구사항을 도출하는데 영향을 끼친다. 본 논문은 A-SMGCS에 대한 기능 위험 평가에 대한 사례 연구를 수행하였다. 이를 위해 관련연구인 Eurocontrol과 EMMA에서 수행한 연구를 분석하였으며 Eurocontrol 및 EMMA의 기능 위험 평가 체계를 통합하였다. FHA (functional hazard assessment) 범위뿐만 아니라 FHA를 위한 여러 가정 사항들을 인천국제공항에 대해서 정의하였다. 29개의 위험원이 식별되었고, 각각에 대해 심각도가 평가되었다. 그리고 위험원에 대한 노출빈도와 안전 목적이 이벤트 트리 분석 방법을 사용하여 분석되었다. 본 연구 결과와 EMMA의 결과에 대한 차이를 분석하였으며 또한 본 연구에서의 평가 결과에 대해서도 검토 하였다.

[Abstract]

Safety assessment is necessary to develop safety related CNS/ATM system. It includes functional hazard assessment (FHA), effects eliciting system safety requirement that mitigates system's hazardous event. This paper performs a case study for functional hazard assessment of A-SMGCS. To do this, related A-SMGCS studies from Eurocontrol and EMMA are surveyed, and assessment schemes of functional hazard from Eurocontrol and EMMA are combined. Not only FHA scope but also several assumptions for FHA are defined for Incheon airport. 29 hazards are identified and their severities are assessed. And exposures and safety objectives from hazards are analyzed using event tree analysis method. Differences between result of this study and result of EMMA are analysed, and assessment results in this study are also reviewed.

Key word : Safety assessment, Functional hazard assessment, CNS/ATM, Advanced surface movement, guidance and control system (A-SMGCS).

<http://dx.doi.org/10.12673/jant.2016.20.2.148>



This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 28 March 2016; Revised 4 April 2016
Accepted (Publication) 21 April 2016 (30 April 2016)

*Corresponding Author; Hongseok Lee

Tel: +82-10-9930-4416

E-mail: hong300@ktl.re.kr

I. 서론

항공 산업에서 항공 교통량이 증가됨에 따라 CNS/ATM (communications, navigation, surveillance/air traffic management) 장비에 요구하는 기능들이 점점 더 복잡해지고 있다. 과거에는 교통량이 적어서 사람이 직접 수행하던 업무들은 앞으로는 장비의 도움을 얻지 않고서는 많은 교통량을 처리하기에는 어려울 것이다. 이런 시대적 상황에 의해 CNS/ATM시스템에 요구되는 기능들이 증가되고 있으며, 이에 따라 시스템은 점차 복잡화되고 있다.

시스템이 다양한 기능을 수행하게 되면서 시스템의 오동작으로 인한 결과가 인간의 생명에 영향을 끼칠 수 있는 가능성 역시 증가하게 된다. 안전과 관련된 장비는 그 장비와 관련된 위험을 식별하고 그 위험이 발생했을 때 끼치는 영향들을 분석하고 그와 같은 위험이 발생하지 않도록 하기 위한 안전 평가 활동이 필요하다.

항공기 지상이동유도 및 통제 시스템 (A-SMGCS; advanced surface movement guidance and control system)도 역시 그 기능이 고도화됨에 따라 안전에 영향을 미칠 수 있기 때문에 안전 분석 활동이 필요하다. 본 논문에서는 A-SMGCS의 안전 분석 활동 중에서 기능 위험 분석 활동에 대한 사례 연구를 수행하였다. 이 연구를 수행하기 위해 관련 연구인 Eurocontrol[1]과 EMMA(European Airport Movement Management)[2]에서 수행한 연구를 분석하였고, 이를 바탕으로 인천 공항에 설치되는 A-SMGCS에 대한 기능 위험 분석 수행 결과를 제시한다.

이 논문의 구성은 다음과 같다. 2장에서는 기능적 위험 분석 방법을 수행하기 위한 절차와 방법을 설명하고 이를 A-SMGCS에 적용한 사례를 제시한다. 그리고 3장에서는 이 연구의 의의 및 향후 연구로 끝을 맺는다.

II. A-SMGCS의 위험원 평가

본 연구의 A-SMGCS에 대한 위험원 평가는 Eurocontrol에서 수행한 자료를 기반으로 수행된 것으로, Eurocontrol에서 정의한 A-SMGCS의 안전 평가 체계를 거의 그대로 적용하였으며, 장비의 안전 목표 수준의 할당에 대해서는 EMMA의 방법을 따라 적용하였다.

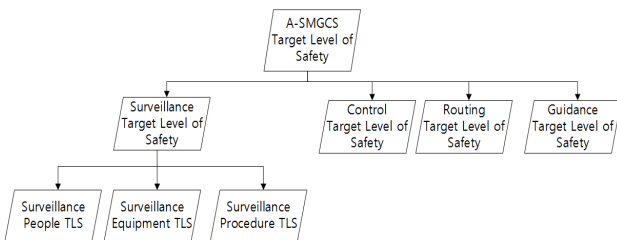


그림 1. Target Level of Safety 분해
Fig. 1. Decomposition of target level of safety.

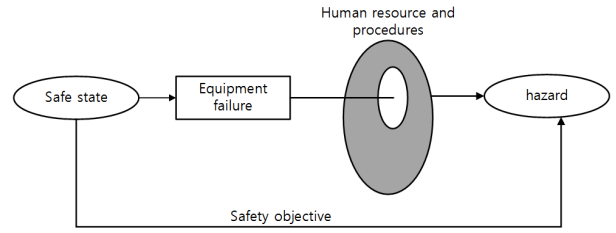


그림 2. A-SMGCS의 위험 발생 모델[2]
Fig. 2. Hazard occurrence model for A-SMGCS[2].

2-1 A-SMGCS의 안전 목표 수준

A-SMGCS의 안전 목표 수준은 ICAO에서 총 안전 목표 수준 (TLS; target level of safety)을 1.0E-08로 정의하였고[3], 각 기능별 안전 목표 수준을 표 1과 같이 예측하였다. 표 1에서 예측한 수치는 관제사의 활동과 장비의 기능을 합한 활동에 대한 안전 목표이기 때문에, 안전 목표 수준을 시스템의 안전 목표 수준과 시스템 이외의 수준으로 분해해야 할 필요가 있다.

Eurocontrol에서는 이 부분에 대한 고려가 되어 있지 않지만, EMMA에서는 그림 1과 같이 감시, 통제, 경로, 안내 각각에 대한 사람, 장비, 절차에 대한 안전 목표 수준을 분해하였다. 이는 A-SMGCS의 기능은 사람, 장비, 관제 절차의 3개 영역이 관여하여 수행되기 때문이다. 결국 CNS/ATM에서의 위험의 발생은 그림 2와 같이 시스템이 고장난 상황에서 인적 자원의 실수와 이런 상황을 대처하는 절차의 누락에 의해 발생된다고 볼 수 있다.

일반적으로 항공기 분야의 표준인 ARP 4761[4]에서는 인적 요소에 대한 위험원 발생의 기여에 대한 고려를 하지 않지만, CNS/ATM분야의 A-SMGCS에서 그와 같은 방식으로 가정하는 것은 올바른 안전평가 결과를 얻을 수 없으므로 TLS를 분해하여 일부 할당하는 것이 더 타당하다고 판단한다. EMMA에서는 A-SMGCS의 구현 수준별로 장비와 사람에 대한 TLS비율을 각각 다르게 정의하여 장비에 할당하였는데, ICAO 9830에 정의된 A-SMGCS 개발 수준[3]이 4인 경우 35%로 정의하였다 [2]. 본 연구에서도 EMMA의 방법을 적용하여 장비에 35%를 할당하였다. A-SMGCS의 각 기능에 대해 장비에 할당된 안전 목표 수준은 표 2와 같다.

표 1. Doc 9830에서 예측한 안전 목표 수준
Table 1. Estimated TLS in Doc 9830.

A-SMGCS function	TLS
Surveillance	3.00E-09
Routing	1.00E-09
Guidance	3.00E-09
Control	3.00E-09
Sum	1.00E-08

표 2. 안전 목표 수준의 분해

Table 2. Decomposition of target level of safety.

A-SMGCS function	Equipment's TLS	Others' TLS	TLS contribution (equipment)	TLS contribution (others)
Surveillance	1.05E-09	1.95E-09	35%	65%
Routing	3.50E-10	6.50E-10	35%	65%
Guidance	1.05E-09	1.95E-09	35%	65%
Control	1.05E-09	1.95E-09	35%	65%
Sum	3.50E-09	6.50E-09		

2-2 A-SMGCS의 개발 범위와 기능

그림 3은 인천국제공항의 관제 환경 및 A-SMGCS의 개발 범위를 나타낸다. 관제사는 운항정보, 기상정보, 레이더 정보를 별도의 화면에서 확인할 수 있으며, 공항 지상 감시 레이더 (ASDE; airport surface detection equipment)를 통해 지상이동항공기를 모니터링 할 수 있다. A-SMGCS에서 제공되는 화면은 운항, 기상, 레이더 정보를 인터페이스 하여 하나의 화면으로 제공받을 수 있다. 관제사는 운항정보 관제사 운영 좌석(CWP; controller working position), 기상정보 CWP, 자동 레이더 터미널 시스템(ARTS; automated radar terminal system) CWP, ASDE CWP를 통해 레이더의 감시 및 통제 기능을 제공받을 수 있다.

또한 관제사는 음성 통신 제어 시스템 (VCCS; voice communication control system)을 통해 항공기 이동지역 내의 이동체에 대한 수동 감시, 통제, 경로, 안내 기능을 수행할 수 있으며, 지상 이동 유도 차량에 대해서는 주파수 공용 통신시스템 (TRS; trunked radio system)를 통해 수동 경로 기능을 제공할 수 있다. 관제사는 등화제어소를 통해 항공기 이동 지역 내의 표시, 등화제어를 수동으로 수행할 수 있으며, 관제사와 제어소는 유선통신으로 통신할 수 있다.

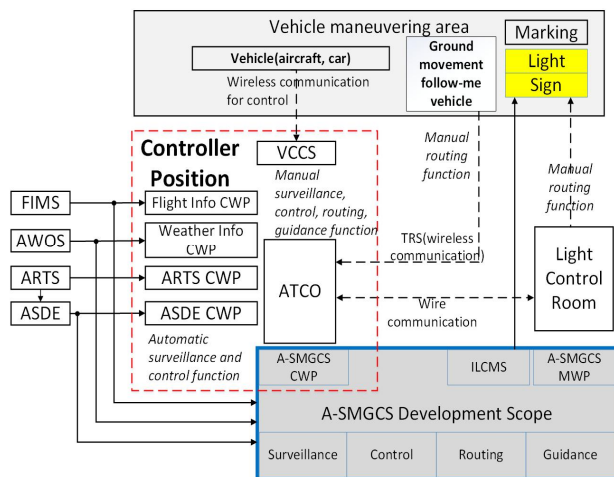


그림 3. 인천국제공항의 관제 환경 및 A-SMGCS 개발 범위
Fig. 3. Control environment in Incheon international airport and development scope of A-SMGCS.

본 연구의 A-SMGCS의 개발은 레이더 센서와 정보를 퓨전 하지 않으며, 레이더 정보를 인터페이스 하여 지상 이동체의 정보를 획득한다. 따라서 안전 평가 범위에서는 레이더가 정상적인 데이터를 생성함을 가정하였다.

2-3 위험원 평가의 가정사항 및 전제조건

위험원 평가를 수행하기 위해 몇 가지 사항들에 대한 가정을 하였다. 이 가정의 일부는 Eurocontrol의 자료에 근거하였다.

첫 번째 가정사항은 10NM 범위 내 항공기 정보는 ASDE로부터 수집된다는 것이다. 이는 레이더의 정상적인 동작을 의미하며 합리적인 가정이다.

두 번째는 조종사 및 차량 운전자는 관제사의 지시 또는 시스템의 관제 지시에 따른다. 이미 2-1에서 장비와 장비 이외의 대상에 대한 안전 목표 수준을 분해하였기 때문에 분해되어 할당된 장비 내에서의 인적 요소의 실수에 의한 위험 상황에 대한 고려는 하지 않으며, 이는 합리적이라고 판단한다.

세 번째는 지상감시 레이더 시스템, 운항정보 시스템, 기상정보 시스템이 별도로 존재한다. 이는 인천국제공항의 관제 환경이며, 별도의 보조적 시스템이 존재함을 가정하는 것을 의미한다.

네 번째는 레이더를 통한 위치, 감시 데이터는 정상적으로 전달된다. 본 연구에서의 개발 범위에서는 레이더에 대한 개발이 포함되지 않으므로, 레이더가 올바른 데이터를 생성하는지에 대한 여부는 판단할 수 없기 때문에, 레이더가 생성하여 전달하는 데이터에 대해서는 정상적이라고 가정한다.

다섯 번째는 기능 고장에 대한 관제사의 탐지 확률은 단일 기능 고장보다 다수 기능 고장이 더 높다. 즉 고장의 개수가 많을수록 혹은 노출 빈도가 높을수록 관제사가 관제활동을 수행하면서 장비의 고장 탐지 확률이 더 높다는 가정은 타당하다고 볼 수 있다. 여섯번째 관제사는 잘 훈련되어 있으며 실수를 하지 않는다. 즉 관제사의 실수에 의한 위험원 발생에 대해서는 고려하지 않는다. 이 가정사항 역시 2번째 가정사항과 유사하게 인적 요소에 의한 위험은 고려하지 않음을 의미하며 합리적이라고 판단한다.

마지막으로, 식별된 위험원에 대한 사고의 기여도는 동등하다고 가정한다. 이 가정사항에 대해서는 2-6에서 다시 언급하도록 하겠다.

2-4 조건(시정 조건, 도로 타입)별 노출빈도

시정 조건은 ICAO 9830, Eurocontrol의 기능 위험원 분석에서와 같이 1단계에서부터 4단계까지 정의하였으며, 각 단계에 대한 설명은 표 3과 같다. 시정 조건에 대한 노출빈도는 2014~2015년 인천국제공항 기상정보를 기준으로 노출빈도를 분석하여 설정하였다. 실제 데이터에서는 시정조건 1이 98% 이상을 차지하였으나, 노출빈도 값을 보수적인 관점에서 Eurocontrol 프로젝트와 같이 96%로 조정하였다.

표 3. 시정 조건의 분류 기준 및 노출 빈도[1]

Table 3. Visibility classification and exposure[1].

Visibility condition (exposure)	Description
Vis 1 (96%)	Visibility sufficient for the pilot to taxi and to avoid collision with other traffic on taxiways and at intersections by visual reference, and for personnel of control units to exercise control over all traffic on the basis of visual surveillance
Vis 2 (3%)	Visibility sufficient for the pilot to taxi and to avoid collision with other traffic on taxiways and at intersections by visual reference, but insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance
Vis 3 (0.99%)	Visibility sufficient for the pilot to taxi but insufficient for the pilot to avoid collision with other traffic on taxiways and at intersections by visual reference with other traffic, and insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance. For taxiing this is normally taken as visibilities equivalent to a RVR less than 400m but more than 75 m
Vis 4 (0.01%)	Visibility insufficient for the pilot to taxi by visual guidance only. This is normally taken as a RVR of 75 m or less

도로의 타입은 Eurocontrol에서 활주로와 그 외 유도로 및 계류장 이동 구역 2가지로 분류하고 있으며, 각각의 노출빈도를 8%와 92%로 정의하였다. 여기서의 노출빈도는 항공기가 공항의 도로의 점유율에 대한 비율을 의미하는 것으로, 유도로 및 계류장 이동구역이 92%라는 의미는 해당 공항에서 항공기가 도로를 점유할 때에 평균적으로 92%를 유도로 및 계류장 이동구역에 위치하고 있음을 의미하는 것이 된다. 본 연구에서의 노출빈도는 인천국제공항의 그리드 맵을 토대로 분석한 결과, 활주로는 8%, 유도로 및 계류장 이동 구역은 92%가 나왔으며, 이 수치는 Eurocontrol에서 정의한 값과 같았다.

2-5 심각도 및 심각도에 따른 사고 발생 확률

심각도의 분류 체계는 Eurocontrol에서 정의한 것과 같이 설정하였으며, 각 등급에 대한 정의는 표 4와 같다. 각 심각도 등급별로 해당 사건 발생 시 사고 발생 확률이 정의되어 있다. 심각도 등급이 1인 경우 사고 발생 가능성은 100%이며, 심각도 등급이 하나 증가할수록 이전 심각도의 100배로 사고 발생 가능성은 감소한다.

즉 심각도 2에 해당하는 사건이 발생할 경우, 그 사건이 사고로 이어질 확률은 1%에 해당하며, 심각도 3에 해당하는 사건이 발생하는 경우, 그 사건이 사고로 이어질 확률은 0.01%에 해당한다.

표 4. 심각도 분류 체계[1]

Table 4. Severity classification scheme[1].

Severity level	Description	Accident rate
5	No impact on safety	1E-08
4	Minor impact on workload or system functionality but all participants (i.e. controllers and aircrew) still believed the situation to be 'safe'	1E-06
3	Higher impact on workload or system functionality but one or more participants (i.e. controllers and aircrew) believed the situation to have moved from 'safe' to a less safe situation	1E-04
2	Significant impact on safety with a high probability of an accident	1E-02
1	Accident (i.e. loss of life or collision between mobiles)	1

2-6 기능별 위험원 식별

위험원은 Eurocontrol, Hong[5]의 연구를 토대로 위험원을 식별하였으며, 총 29개의 위험원을 식별하였다. 표 5~8에서 감시, 통제, 경로, 안내 기능과 관련된 식별된 위험원에 대해 설명하였다.

표 5의 H01은 감시 기능의 완전 정지를 의미하며, 시스템이 다운된 것과 같이 감시와 관련된 모든 기능을 수행하지 않는 상태를 의미한다. 표 6, 7, 8의 H11, H20, H25는 그와 유사하게 각각 통제, 경로, 안내 기능에 대한 시스템의 완전 정지를 의미한다.

표 5. 감시 기능의 위험 요소

Table 5. Hazards of surveillance.

ID	Hazard
H01	Total loss of surveillance function
H02	Loss of the position function for one aircraft
H03	Loss of the position function impacting multiple aircraft
H04	Corruption of the position function for one aircraft
H05	Corruption of the position function impacting multiple aircraft
H06	Total loss of the identification function
H07	Loss of the identification function for one aircraft
H08	Loss of the identification function impacting multiple aircraft
H09	Corruption of the identification function for one aircraft
H10	Corruption of the identification function impacting multiple aircraft

표 6. 통제 기능의 위험 요소

Table 6. Hazards of control.

ID	Hazard
H11	Total loss of conflict prediction function
H12	Loss of the conflict prediction function impacting multiple aircraft
H13	Corruption of the conflict prediction function
H14	Total loss of conflict detection function
H15	Loss of the conflict detection function impacting multiple aircraft
H16	Corruption of the conflict detection function
H17	Total loss of the conflict resolution function
H18	Loss of the conflict resolution function impacting multiple aircraft
H19	Corruption of the conflict resolution function

표 7. 경로지정 기능의 위험 요소

Table 7. Hazards of routing.

ID	Hazard
H20	Total loss of routing function
H21	Loss of the routing function for one aircraft
H22	Loss of the routing function impacting multiple aircraft
H23	Corruption of the routing function for one aircraft
H24	Corruption of the routing function impacting multiple aircraft

표 8. 안내 기능의 위험 요소

Table 8. Hazards of guidance.

ID	Hazard
H25	Total loss of guidance function
H26	Loss of the guidance function for one aircraft
H27	Loss of the guidance function impacting multiple aircraft
H28	Corruption of the guidance function for one aircraft
H29	Corruption of the guidance function impacting multiple aircraft

H02와 H03은 하나 혹은 여러 항공기의 위치 식별 기능의 손실은 항공기가 실제로 존재하지만, 시스템에서는 인지하지 못

하는 상황을 의미한다. H04, H05의 하나 혹은 여러 항공기의 위치 식별의 손상은 항공기의 존재는 인식하지만, 잘못된 위치에 있다고 파악하는 고장을 의미한다. 그 외의 다른 위험원들에 대해서는 위에 언급한 것과 유사하게 각 기능의 잘못된 동작을 의미한다.

각각의 위험원에 대한 안전 목표(TLS)는 각 기능의 할당된 총 TLS에 대해 식별된 위험원의 개수를 나눈 값으로 결정하였다. 그와 같이 계산한 이유는 각 위험원으로 인한 사고의 기여도는 알려져 있지 않으며, 알 수도 없기 때문이다.

어떤 위험원에 대한 가중치를 부여하는 행위는 수행하게 된 타당한 근거를 제시할 수 있어야 하는데, 그렇게 제시하는 것은 사실상 매우 어렵기 때문에 적절하지 않다고 판단한다. 또한 Eurocontrol에서도 각 위험원에 대한 기여도를 동등하게 가정하여 분할하였기 때문에, 본 연구에서도 동등한 기여도로 가정하여 각각의 위험원 당 안전 목표를 설정하는 것이 합리적이라고 판단하였다.

2-7 위험원 평가

각 위험원에 대해 이벤트 트리 분석 기법을 활용하여 시정 조건, 도로 조건, 위험원에 대한 관제사의 탐지 확률 등의 환경에서 심각도를 평가하였고, 각 기능에 할당된 안전 목표로부터 발생확률과 안전 목표(SO; safety objective)을 계산하였다.

그림 4는 위험원 H01에 대한 이벤트 트리 분석 결과를 나타낸다. H01의 이벤트 트리 분석 결과로부터 위험원에 대한 노출 빈도는 1.0E-06이 되며 이 값의 의미는 H01이 발생할 확률을 의미한다. H01의 안전 목표 (safety target) 수준은 표 2의 장비에 할당된 감시 기능의 TLS인 1.05E-09에서 식별된 위험원이 표 5의 10개이므로 1.05E-10이며, SO는 TLS에서 노출확률을 나눈 값인 1.1E-04가 된다. 이와 같이 각각의 위험원들에 대한 노출 빈도 및 SO는 표 9와 같다.

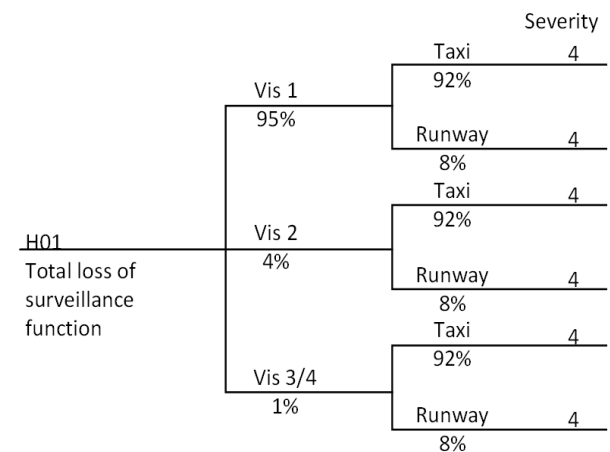


그림 4. 위험원 H01에 대한 이벤트 트리 분석 결과
Fig. 4. Event tree analysis result for hazard H01.

표 9. 위험원 평가 결과 요약

Table 9. Summary of hazard assessment result.

ID	Hazard	Exposure	SO
H01	Total loss of surveillance function	1.0E-06	1.4E-04
H02	Loss of the position function for one aircraft	1.1E-07	1.2E-03
H03	Loss of the position function impacting multiple aircraft	2.0E-08	6.8E-03
H04	Corruption of the position function for one aircraft	2.9E-08	4.7E-03
H05	Corruption of the position function impacting multiple aircraft	1.3E-06	1.1E-04
H06	Total loss of the identification function	8.9E-08	1.5E-03
H07	Loss of the identification function for one aircraft	8.9E-08	1.5E-03
H08	Loss of the identification function impacting multiple aircraft	4.0E-08	3.4E-03
H09	Corruption of the identification function for one aircraft	9.3E-08	1.5E-03
H10	Corruption of the identification function impacting multiple aircraft	6.1E-07	2.2E-04
H11	Total loss of conflict prediction function	1.3E-08	1.2E-02
H12	Loss of the conflict prediction function impacting multiple aircraft	1.3E-08	1.2E-02
H13	Corruption of the conflict prediction function	1.0E-08	1.5E-02
H14	Total loss of conflict detection function	1.3E-08	1.2E-02
H15	Loss of the conflict detection function impacting multiple aircraft	1.3E-08	1.2E-02
H16	Corruption of the conflict detection function	1.3E-08	1.2E-02
H17	Total loss of the conflict resolution function	1.0E-08	1.5E-02
H18	Loss of the conflict resolution function impacting multiple aircraft	1.0E-08	1.5E-02
H19	Corruption of the conflict resolution function	1.0E-06	1.5E-04
H20	Total loss of routing function	6.0E-08	1.5E-03
H21	Loss of the routing function for one aircraft	1.0E-08	9.0E-03
H22	Loss of the routing function impacting multiple aircraft	6.0E-08	1.5E-03
H23	Corruption of the routing function for one aircraft	1.0E-08	9.0E-03
H24	Corruption of the routing function impacting multiple aircraft	6.0E-08	1.5E-03
H25	Total loss of guidance function	1.0E-06	2.7E-04
H26	Loss of the guidance function for one aircraft	1.0E-08	2.7E-02
H27	Loss of the guidance function impacting multiple aircraft	1.0E-06	2.6E-04
H28	Corruption of the guidance function for one aircraft	6.0E-08	4.5E-03
H29	Corruption of the guidance function impacting multiple aircraft	2.0E-08	1.4E-02

2-8 관련 연구 결과와의 비교

본 연구의 결과에 대해 Eurocontrol의 기술자료와 EMMA의 기능 위험 분석 결과를 비교 검토하였다. 타 연구와의 위험도 분석의 차이가 나는 원인에 대해 논의한 결과는 표 10에 기술되었다. 위험도 분석의 차이가 나는 첫번째 이유는 안전 평가의 범위와 관련이 있다. EMMA에서 평가한 심각도가 높은 위험원들은 본 연구의 과업범위 밖인 레이더와 관련된 고장으로 인한 것이다. 두 번째 이유는 시스템 운영 환경과 관련이 있다. 인천 국제공항의 운영 환경에서는 부가적인 감시 장치가 있는 반면, EMMA에서는 그와 같은 장치가 존재하지 않는다.

III. 연구 결과에 대한 논의 및 결론

본 논문은 A-SMGCS 시스템에 대한 기능적 위험 분석 수행에 대한 사례 연구이며, 이 연구를 수행하기 위한 목적은 안전 필수적인 시스템의 안전성을 보증하기 위해서이다. 기능적 위험 분석의 결과로 위험원들에 대한 심각도 및 안전 목적(SO)을 도출하였다. 기능 위험 분석을 수행한 과정을 요약하면 다음과 같다. 첫째로 타 연구 사례를 분석하여 각 연구에서의 접근법을 정리하였고, 본 장비의 운영 환경과 개발 범위를 정의하였다.

표 10. EMMA[2]의 기능 위험 분석 결과 검토

Table 10. Discussion of functional hazard assessment in EMMA[2].

Hazard	Severity	Discussion
HZ-02	2	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-03	3	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-05	2	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-06	1	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-07	1	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-11	3	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-12	3	Radar is out of our development scope, and we assumed that radar operates normally.
HZ-17	2	Additional flight plan display device exists in controller room
HZ-18	3	Additional flight plan display device exists in controller room

두 번째로 기능 위험 평가 수행을 위한 가정들을 정의하였고, 정량적 평가 수행을 위한 시정 조건별 노출빈도, 도로별 노출빈도, 심각도의 정의 및 심각도별 사고 확률을 정의하였다.

세 번째로 개발 대상에 대한 위험원을 식별하였고, 이벤트 트리 분석 방법을 활용하여 각 시나리오에 대한 심각도 평가를 하였으며, 위험도에 대한 발생확률 및 안전 목표(safety objective)를 계산하였다. 마지막으로 계산 결과에 대한 관련 연구결과와의 비교 검토를 통해 계산 결과를 확인하였다.

본 연구에서 수행한 국내용 A-SMGCS의 평가 결과는 인천 국제공항에 해당하는 결과로 인천국제공항외의 다른 공항에 A-SMGCS를 개발하려고 하는 경우 해당 공항별로 운영절차 및 방법에 차이가 있을 수 있다. 그러므로 기능 위험 분석 단계 중 두 번째 단계부터 다시 수행해야 한다.

본 연구의 한계는 TLS 접근 방식에 대한 것으로, TLS 방식은 안전 목표 수준을 분할하여 배정하게 되는데, 그 배정하는 방식에 대한 당위성을 보장할 수 없는 한계를 가진다. 즉, 전체 위험에 대해 위험에 대한 배정 방식은 오류가 있을 수 있다는 점이다 [6]. EMMA에서도 TLS의 이런 문제를 인식하고 있어서 수학적 충돌 확률 모델을 정의하여 검증하는 접근법을 택하였다. 그러나, 수학적 충돌 확률 모델을 활용한 접근법의 경우 확률 모델에 대한 검증이 쉽지 않다는 문제가 있다.

향후 연구로는 국내용 A-SMGCS에 대한 안전 요구사항 도출, 시스템 예비 안전 평가, 시스템 안전 평가 등을 통해 A-SMGCS시스템의 안전성을 입증하기 위한 활동을 수행할 예정이다.

감사의 글

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었습니다(과제번호:15ATRP-C069188-03).

참고 문헌

- [1] P. Adamson, A-SMGCS Level 1 and 2 Preliminary Safety Case, Brussels, Belgium, Technical Report Edition 2.0, 2006.
- [2] S. Paul, Functional Hazard Assessment and very Preliminary System Safety Assessment Report, THALES, Braunschweig, Germany, Technical Report D139 FHAvPSSA V.1.0, 2006.
- [3] ICAO, Advanced surface movement guidance and control system (A-SMGCS) manual, ICAO, Montreal, Canada, ICAO DOC 9830, 2004.
- [4] SAE International, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE, ARP 4761, 1996.
- [5] S. B. Hong, S. H. Choi and Y. C. Choi, "A Study on the Hazard Identification for the Implementation of A-SMGCS," *Journal of Advanced Navigation Technology*, Vol. 19, No. 1, pp. 41-47, Feb. 2015.
- [6] L.F. Vismari, L. Flavio and J. B. Camargo Junior, "A safety assessment methodology applied to CNS/ATM-based air traffic control system," *Journal of Reliability Engineering & System Safety*, Vol. 96, Issue 7, pp. 727-738, July, 2011.



이 홍 석 (Hongseok Lee)

2011년 2월 : 아주대학교 전자공학과 (공학박사)
2010년 9월 ~ 현재 : 한국산업기술시험원 선임연구원
※ 관심분야 : 시스템 안전평가, 기능 안전 소프트웨어, 소프트웨어 V&V



조 상 훈 (Sanghoon Jo)

2013년 2월 : 한국항공대학교 항공운항관리학과 (이학석사)
2016년 2월 : 한국항공대학교 항공운항관리학과 박사수료
2014년 12월 ~ 현재 : 인천국제공항공사 전문연구원
※ 관심분야 : CNS/ATM, 운항관리, 시스템 안전평가, 시스템 V&V



최 형 석 (Hyungseok Choi)

2004년 2월 : 영남대학교 전기공학과 (공학사)
2003년 11월 ~ 2006년 7월 : LG화학 테크센터 전기차 배터리 솔루션
2006년 8월 ~ 현재 : 인천국제공항공사 과장
※ 관심분야 : Surface & Terminal ATM, CNS/ATM, 전기공학