JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항행 및 항법

J. Adv. Navig. Technol. 20(4): 285-291, Aug. 2016

항행 안전 시스템을 위한 안전 목표 수준 기반 위험 평가 방법론

Hazard Assessment Methodology Based on Target Level of Safety for CNS/ATM System

이 홍 석[1*] · 조 상 훈[2]
[1]한국산업기술시험원 시스템검증센터
[2]한국항공대학교 항공운항관리학과

Hongseok Lee[1*] · Sanghoon Jo[2]
[1]System Verification Center, Korea Testing Laboratory, Seoul 08389, Korea
[2]Aviation Management, Korea Aerospace University, Gyeonggi-do 10540, Korea

[요 약]

CNS/ATM 분야에서 안전 평가는 시스템을 개발하는데 반드시 필요한 개발 활동이다. 현재까지, 안전 평가와 관련된 많은 참고할 만한 자료들이 있으나 CNS/ATM분야에서 무엇을 어떻게 적용해야 할지 명확하게 명시된 자료는 없다. 또 다른 문제는 DO-278A기반으로 소프트웨어를 개발하기 위해서는 개발하고자 하는 소프트웨어에 대한 소프트웨어 보증 수준이 결정되어 있어야 한다. 하지만 개발 보증 수준을 결정하는 체계도 또한 정의되어 있지 않다. 이와 같은 문제를 해결하기 위해 본 논문에서는 ICAO Doc 9689에 정의된 안전 목표 수준을 기반으로 한 위험 평가를 수행하기 위한 방법을 제시한다. 항행 안전 시스템에서 일반적으로 적용 가능하도록 하기 위해 위험 평가 수행 절차를 수학적으로 표현하였으며 위험 평가를 위해 필요한 위험원의 심각도 분류, 발생 확률, 시스템 안전 목표 수준 등을 정의하고 위험 평가를 수행하기 위해 이벤트 트리 분석 절차를 적용하는 방법을 설명하였다.

[Abstract]

Safety assessment is an essential activity for developing a system in the CNS/ATM domain. Up to now, there are many reference materials, but there is nothing that definitely specifies what to do and how to apply in the CNS/ATM. Another problem is that software assurance level has to be determined for a software under development. But there is nothing that defines a determination scheme of software assurance level. To solve these problems, this paper proposes a method to conduct a hazard assessment based on target level of safety defined in ICAO Doc 9689. To be applied generally in CNS/ATM domain, it mathematically defines procedures of hazard assessment. And it defines severity classification, probability, and safety objective of a system, which are necessary for hazard assessment, and it describes a method to apply event tree analysis process in order to conduct a hazard assessment.

Key word : Safety assessment, Functional hazard assessment, DO-278A, Assurance level determination, Communications navigation surveillance/air traffic management.

http://dx.doi.org/10.12673/jant.2016.20.4.285

Received 13 June 2016; **Revised** 20 July 2016
Accepted (Publication) 12 August 2016 (30 August 2016)

***Corresponding Author; Hongseok Lee**

Tel: +82-10-9930-4416
E-mail: hong300@ktl.re.kr

Ⅰ. 서 론

항공 교통 분야의 트래픽이 계속 증가됨에 따라 CNS/ATM (communications, navigation, surveillance/air traffic management) 장비의 기능은 점점 더 복잡해지고 있다. 장비의 기능이 복잡해짐에 따라 구현해야 하는 복잡도 또한 필연적으로 증가하고 있다. 과거에 사람이 직접 수행하여 왔던 활동들을 앞으로 장비가 자동으로 수행하게 된다면, 이로 인해 발생하는 시스템 오동작이 인간의 생명에 영향을 끼칠 수 있는 가능성이 앞으로 증가할 가능성이 높다. 항공 선진국에서는 이러한 안전과 관련이 있는 비항공용 장비를 개발하기 위해 소프트웨어 개발 프로세스 표준을 만들어 안전관련 기술을 개발하기 위한 지침으로 삼아왔다. 항공 분야의 소프트웨어 개발 프로세스 표준으로는 DO-178C[1]와 DO-278A[2]가 있는데 DO-178C는 항공기 탑재용 소프트웨어 개발을 위한 표준인 반면, DO-278A는 비항공장비의 소프트웨어 개발을 위한 표준이다.

항공용과 비항공용 시스템에 탑재되는 소프트웨어의 규제환경의 차이로 인해 CNS/ATM시스템의 소프트웨어 개발 표준인 DO-278A에서는 '인증'에 대한 모든 참조사항이 DO-178C와 달리 존재하지 않지만, CNS/ATM분야의 안전과 관련된 소프트웨어를 개발하기 위해서는 DO-278A 표준을 준수할 필요가 있다.

DO-278A기반으로 소프트웨어를 개발하기 위해서는 대상 소프트웨어의 보증 수준이 결정되어 있어야 한다. 소프트웨어는 하드웨어 신뢰성과 같은 방식으로 정량화된 지표가 존재하지 않는다. 대부분 기능 안전과 관련된 소프트웨어의 개발은 해당 시스템의 안전성에 대한 수준에 따라 소프트웨어의 보증 수준이 결정되며, 보증 수준에 따라 개발 절차의 엄격성의 정도가 달라진다.[1]-[5] 즉, 안전과 관련된 시스템일수록 소프트웨어 보증 수준이 높으며, 소프트웨어의 보증 수준이 높아질수록 소프트웨어의 개발 프로세스는 더 엄격해진다.

하지만 DO-278A 프로세스 표준에서 직접적으로 참조되는 시스템 개발 및 시스템 안전 평가 표준이 존재하지 않기 때문에 어떤 방법을 사용할지가 문제이다. 항공기 탑재용 소프트웨어 개발 표준인 DO-178C[1]에서는 시스템 개발 프로세스 및 시스템의 안전 평가 프로세스로 각각 ARP4754A[6] 및 ARP4761[7]을 참조하며, 소프트웨어의 보증 수준은 기능 위험 평가 및 시스템 설계의 결과에 따라 소프트웨어의 보증 수준이 결정된다.

비항공 소프트웨어 표준인 DO-278A 프로세스는 ARP4761 표준을 안전 평가 프로세스에 활용할 경우 적용상의 어려움이 있다. 항공용 시스템은 고장 조건에 대한 공통된 정의가 존재하는 반면 비항공용 CNS/ATM시스템은 고장 조건에 대해 널리 받아들여지는 공통적인 정의가 존재하지 않으며 항공용과 비항공용 시스템은 사용되는 환경이나 시스템의 특성이 차이가 있다. 따라서 비항공용 시스템의 안전 평가를 ARP표준으로 적용하는 데는 어려움이 있을 수 있다.

이러한 안전 평가 수행을 위한 관련 연구로는 안전 목표 수준(TLS; target level of safety)에 근거한 기능 위험 평가 방법론이 있으며, ICAO Doc 9689[8]에서 TLS기반의 평가 절차를 6단계로 정의하였다.

첫 번째 단계는 시스템을 정의한다. 해결되어야 하는 문제와 개발 대상 시스템 및 항공기를 정의하고 범위를 설정한다. 두 번째 단계는 평가 기준을 수립한다. 허용 가능한 최대 리스크를 결정하고 평가되어야 하는 안전 기준을 선정한다. 세 번째 단계는 위험원을 식별한다. 시스템의 사고를 유발할 수 있는 위험원을 식별한다. 네 번째 단계는 발생확률을 예측하고 결과를 모델링한다. 각각의 위험원에 대한 발생 가능성을 예측한다. 다섯 번째 단계는 리스크를 예측하고 평가한다. 리스크 예측 및 평가의 객관성을 위해 사전 정의되어야 한다. 여섯 번째 단계는 리스크 평가 결과에 대한 수용 여부를 판단한다. 만약 평가된 리스크가 받아들일 수 없는 수준인 경우 리스크를 낮추기 위한 수단을 정의하고 세 번째 단계에서부터 다시 수행한다.

ICAO Doc 9689[8] 평가절차 중에서 첫 번째에서 세 번째 단계는 시스템 분석 및 위험을 평가하는 일반적인 단계이기 때문에 적용하는데 어려움이 없다. 하지만 네 번째와 다섯 번째 단계는 평가를 위한 구체적인 기준과 체계가 정의되어야만 적용할 수 있다.

따라서 본 논문에서는 안전 목표 수준에 근거한 기능 위험 평가 절차의 네 번째 단계 및 다섯 번째 단계를 수행하기 위한 구체적인 방법을 제시하고자 하며, 이를 통해 기능적 안전 목표 수준 기반의 위험 평가를 수월하게 수행할 수 있을 것으로 기대한다. 또한 이 연구는 기능 위험 평가에 대한 기존 연구[9]를 비항공 시스템에 적용할 수 있도록 기능 위험 평가 체계를 일반화한 것에 그 의의가 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기능 위험 평가 방법을 수행하기 위한 절차와 방법을 제시한다. 3장에서는 2장에서 제시한 방법론을 A-SMGCS에 적용한 사례를 제시하고 4장에서는 이 연구의 의의 및 향후 연구로 끝을 맺는다.

Ⅱ. 정량적 위험원 평가 체계

이 장은 시스템의 위험원을 정량적으로 평가하는 방법에 대해서 기술한다. ICAO Doc 9689[8]의 평가 단계 중 세 번째 단계인 시스템 위험원을 식별하는 활동까지는 이미 수행된 것으로 가정하였다. 시스템의 위험원 식별에 대해서는 관련 연구들[10,11]을 참조한다.

2-1 위험원 식별 및 발생확률 모델링

위험원이 시스템에 미치는 영향을 평가하기 위해서는 심각도 분류 체계가 정의되어야 한다. 여러 문헌[7],[12]에서 심각도에 대한 분류 기준을 각각 다양한 방법으로 정의하였다.

Eurocontrol[12]은 심각도에 대한 분류 기준을 발생 가능성에 대한 확률을 심각도에 대한 함수로 정의한 반면, ARP4761[7]에

표 1. 심각도 분류 체계[12]
Table 1. Severity classification scheme[12].

Severity level	Description
5	No impact on safety
4	Minor impact on workload or system functionality but all participants (i.e. controllers and aircrew) still believed the situation to be 'safe'
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
2	Significant impact on safety with a high probability of an accident
1	Accident (i.e. loss of life or collision between mobiles)

서는 발생 가능 확률을 심각도에 무관하게 정의하였다. 다만 각각의 심각도에서 허용 가능한 발생 가능 확률을 정의하였다.

두 가지 방법은 각기 장단점을 가지고 있다. 심각도와 사고 발생확률을 연계한 접근법은 심각도가 판정되면 즉시 해당 위험에 대한 사건 발생 확률을 도출할 수 있다는 장점이 있다. 하지만 위험에 대한 심각도를 판정할 때 심각도에 대한 판단이 두 가지 관점이 존재한다. 즉 심각도 분류 체계로 판정을 할 수도 있지만, 위험에 대한 사고 발생 가능성에 대한 확률을 감안하여 심각도를 판단할 수도 있다. 이는 평가 결과에 대한 일관성이 부족할 가능성이 있다는 단점이 된다.

한편 심각도를 발생확률과 관련 없이 정의하는 방법은 관련 위험에 대한 심각도를 판단할 때 심각도 분류체계에 따라 판단하기만 하면 되기 때문에 일관성을 보일 수는 있지만, 해당 위험에 대한 발생확률을 계산하기 위한 체계가 없기 때문에 확률 계산에 대한 근거 혹은 타당성이 부족할 수 있다는 문제가 있다.

심각도에 따른 분류 체계는 대체로 여러 문헌에서 표 1과 유사한 형태로 분류하지만 각 분야별로 분류 체계는 상이할 수 있다. 표 1에서는 심각도를 5가지 등급으로 분류하였다. 가장 낮은 심각도 등급은 5이며 이는 안전에 아무런 영향을 미치지 않는 등급을 의미한다. 가장 높은 심각도 등급은 1이며 이는 이동체간 충돌이나 생명을 잃을 수 있는 사고가 발생함을 의미한다.

본 논문에서는 위험에 대한 사고 발생 확률을 심각도와 연계하여 정량적으로 정의하는 접근법[12]을 채택하였다. 즉, 심각도 등급 s에 해당하는 사건이 사고로 이어질 확률 $p(s)$는 다음과 같이 정의한다.

$$p(s) = \begin{cases} 10^{-2(s-1)} & 1 \le s \le 4 \\ 0 & otherwise \end{cases} \quad (1)$$

2-2 위험원에 대한 시스템 안전 목표 수준(Safety objective) 정의

시스템이 만족해야 하는 TLS가 정의되고, 위험원이 식별되었으며 각 위험원에 대한 발생 가능성과 심각도가 결정되었다면, 각 위험원별로 시스템에 의해 달성되어야 하는 안전 목표 수준(SO; safety objective)[13]을 명세해야 한다. 임의의 시스템 x와 x와 관련된 위험원 집합 H에 대해, 시스템 x의 허용 가능한 최대 TLS는 $TLS_{MaxTol}(x)$로 다음과 같이 정의한다.

$$TLS_{MaxTol}(x) = \sum_i tls(h_i) \quad (2)$$

여기서 $tls(h_i)$ 는 위험원 집합 H에 속한 위험원이 만족해야 하는 안전 목표 수준이다. 시스템의 허용 가능한 최대 안전 목표 수준은 시스템에 부과된 TLS보다 작거나 같아야 한다. 식 (2)로부터 각 위험원에 대해 만족해야 하는 안전 목표 수준이 결정되며, 이로부터 SO를 구할 수 있다. SO는 이벤트 트리 분석법(ETA; event tree analysis)을 이용하여 구할 수 있다.

2-3 이벤트 트리 분석

1) 개요

이벤트 트리 분석법은 잠재적 사고 시나리오와 관련된 이벤트들의 식별 및 발생확률을 평가하는 분석법[11]이다.

표 2. 이벤트 트리 분석 프로세스[11]
Table 2. ETA process[11].

Step	Task	Description
1	Define the system	Examine the system and define the system boundaries, subsystems, and interfaces.
2	Identify the accident scenarios	Perform a system assessment or hazard analysis to identify the system hazards and accident scenarios existing within the system design.
3	Identify the initiating events	Refine the hazard analysis to identify the significant IEs in the accident scenarios.
4	Identify the pivotal events	Identify the safety barriers or countermeasures involved with the particular scenario that are intended to preclude a mishap.
5	Build the event tree diagram	Construct the logical ETD, starting with the IE, then the PEs, and completing with the outcomes of each path.
6	Obtain the failure event probabilities	Obtain or compute the failure probabilities for the PEs on the ETD. It may be necessary to use FTs to determine how a PE can fail and to obtain the probability.
7	Identify the outcome risk	Compute the outcome risk for each path in the ETD.
8	Evaluate the outcome risk	Evaluate the outcome risk of each path and determine if the risk is acceptable
9	Recommend corrective action	If the outcome risk of a path is not acceptable, develop design strategies to change the risk.

ETA는 표 2와 같은 절차에 의해 수행된다. ETA를 통한 위험원 평가를 위해서는 이벤트를 MECE(mutually exclusive correctively exhaustive)적으로 정의해야 하고 각 이벤트의 발생조건에 대한 노출빈도를 정량화시킬 수 있어야 한다. ETA에서의 시나리오는 해당 시나리오에서 정의된 각각 이벤트들에 대한 조건들의 곱으로 표현이 되며 해당 시나리오의 노출빈도는 각 이벤트 조건의 노출빈도의 곱으로 표현이 된다.

2) 이벤트 트리의 정의

이벤트 트리 (ET; event tree)는 6가지의 구성요소들로 이루어져 있으며 ET = <H, S, E, Y, T, δ>와 같이 정의된다. 여기서,

- H는 위험원의 집합
- S는 심각도의 집합
- E는 중요 이벤트의 집합
- Y: E → ∑+는 중요 이벤트에 대한 결과의 집합이며, ∑+는 공백문자열을 제외한 모든 문자열을 의미한다.
- T: Y(E1) × Y(E2) × ⋯ × Y(En) × S, 여기서 Ei(1≤i≤n) ∈ E
- δ: E × Y → R+는 중요 이벤트가 어떤 결과가 되는 노출빈도 함수. R+는 양의 실수의 집합이다.

이후 논의의 편의를 위해 임의의 ET = <H, S, E, Y, T, δ>에 대한 $t = (y_1, y_2, \dots, y_n, s)$, t∈ T에 대해, t^i를 t의 i번째 요소로 정의한다. 즉 t^i는 y_i $(1 \le i \le n)$이다.

3) 위험원에 대한 발생 확률 계산

임의의 시스템 x에 대한 ET(H, S, E, Y, T, δ)에 대해, 시스템 x에서 발생할 수 있는 임의의 위험원 h∈H에 대한 발생확률 *p(h)*는 다음과 같이 정의된다.

$$p(h) = \sum_{t \in T} \left(\prod_{i=1}^{n} \delta(E_i, k_j) p(s) \right) \tag{3}$$

여기서, $E_i = Y^{-1}(t^i)$, $k_j = Y(E_i)$이다.

4) 위험원에 대한 SO 계산

임의의 위험원 h와 h가 만족해야 하는 안전 목표 수준인 tls(h)가 있다고 할 때, SO는 다음과 같이 정의된다.

$$\phi(h) = tls(h) / p(h) \tag{4}$$

식 (4)로부터 위험원 h의 안전 목표 수준은 위험원 h의 발생확률과 h의 SO값의 곱으로 구할 수 있다.

2-4 소프트웨어 개발 보증 수준 결정

각각의 식별된 위험원에 대한 심각도 판단 및 SO 명세가 종료된 이후 시스템의 설계 및 시스템 예비 안전 평가를 통해 아이템을 정의하고, 안전 요구사항을 도출한다[13]. 여기서 아이템은 잘 정의된 인터페이스를 가지는 하드웨어나 소프트웨어로 이루어진 요소[6]를 의미한다.

시스템을 여러 개의 아이템으로 분할한 경우 하나의 아이템이 다른 아이템에게 영향을 미칠 수도 있기 때문에 할당된 안전 목표 수준 (safety objective)만을 고려하는 것이 아니라 공통 원인 분석이나 의존성 분석을 통해 대상 아이템에 영향을 미치는 다른 아이템의 존재유무를 확인해야 한다.

시스템 x와 시스템 x와 관련된 위험원 집합 H에 대해, 소프트웨어에 할당된 기능과 관련된 위험원 H'⊆H일 때 소프트웨어 개발 보증 수준 결정 det(H')은 다음과 같이 정의된다.

$$\det(H') = \underset{h \in H'}{Max}(AL(\phi(h))) \tag{5}$$

여기서, SO에 대한 DO-278A 개발 보증 수준(DAL; development assurance level) 결정 함수 AL(x)는 표 3과 같이 정의하였다. 표 3의 SO의 값은 Eurocontrol의 위험 분류 체계[14]를 참고로 하여 작성하였다. Eurocontrol[14]에서는 5가지의 심각도에 대한 안전 목표 수치만 정의되어 있으며, 이 기준은 표 1의 심각도 분류 기준으로 1:1 매핑을 할 수 있다. 하지만, 표 3에서 볼 수 있듯이 DO-278A의 경우 보증 수준이 6단계로 정의되어 있어서 표 1에 정의된 심각도 분류 등급 및 위험 분류 체계[14]에 정의된 등급과 상이하다. 그래서 본 논문에서는 심각도 3 또는 4인 경우 AL4로 적용할 수 있도록 제안한다.

이 의미는 임의의 위험이 심각도 3으로 판단된 경우 그 위험과 관련된 소프트웨어를 DO-278A기반으로 개발할 때, 해당 소프트웨어의 보증 수준이 너무 엄격하다고 판단되는 경우 AL4로 낮출 수 있음을 의미하기도 한다. 또한 임의의 또 다른 위험이 심각도 4로 판단되었으나 그 위험에 대한 소프트웨어 개발을 AL5보다는 조금 더 엄격하게 개발되어야 할 필요가 있다고 판단되는 경우 AL4로 높일 수 있음을 의미하기도 한다.

표 3. DO-278A 개발 보증 수준 결정 함수
Table 3. Determination function of DAL for DO-278A.

Software Failure Effect Category	DO-278A Assurance Level	Severity classification scheme (table 1)
Catastrophic	AL1	1
Hazardous	AL2	2
Major	AL3	3
Less than major, more than minor	AL4	Not defined
Minor	AL5	4
No effect	AL6	5

표 4. DO-278A 개발 보증 수준 결정 함수
Table 4. Determination function of DAL for DO-278A.

Safety objectives(SO)	DO-278A Development assurance level AL(x)
$x < 10^{-8}$	AL1
$10^{-8} \le x < 10^{-5}$	AL2
$10^{-5} \le x < 10^{-4}$	AL3, AL4
$10^{-4} \le x < 10^{-2}$	AL4, AL5
$10^{-2} \le x \le 1$	AL6

Ⅲ. A-SMGCS의 위험원 평가 적용 사례

이 장은 II장에서 제시한 일반적인 방법론이 구체적으로 어떻게 적용될 수 있는지 설명하기 위해 A-SMGCS 기능 위험 평가 사례연구[9]를 참조하였다. A-SMGCS의 위험원을 식별하는 방법은 이 장에서 다루지 않으며 이미 식별되었다고 가정한다.

각각의 위험원이 다양한 환경에서 어떠한 심각도를 갖는지 판단하기 위해서는 이벤트 집합을 정의하여야 한다. 이벤트 집합은 위험과 관련된 주변 환경을 의미하며 이에 대한 구체적인 사례는 다음과 같다.

3-1 이벤트 정의

A-SMGCS 사례 연구에서 정의한 이벤트는 시정 조건, 도로의 타입, 위험원에 대한 탐지이다. 시정 조건과 도로의 타입에 대한 이벤트의 경우에는 인천국제공항에 특화된 데이터로 다른 공항에 A-SMGCS를 설치하고자 하는 경우에는 해당 공항의 실정에 맞는 데이터를 사용해야 한다. 어떤 위험원의 경우에는 시스템을 사용하는 사용자에 의해 탐지가 가능할 수도 불가능할 수도 있다. 이런 판단은 실제 시스템을 사용하는 사용자에 의해 결정되어야 한다.

3-2 시정 조건

시정 조건은 ICAO 9830[15], Eurocontrol[12]에서와 같이 1단계에서부터 4단계까지 정의하였으며, 각 단계에 대한 설명은 표 5와 같다. 그리고 시정 조건에 대한 노출빈도는 2014~15년의 인천국제공항 기상정보[16]를 기준으로 한 노출빈도를 나타낸다. 실제 데이터에서는 시정조건 1이 98 % 이상을 차지하였으나, 보수적인 관점에서 노출빈도 값을 조정하였다.

3-3 도로의 타입

도로의 타입은 활주로와 유도로로 분류할 수 있다. 도로의 타입에 대한 노출빈도에서는 이동체가 활주로의 점유하는 시간이 동일하다는 가정을 바탕으로 하고 있다.

A-SMGCS가 설치되는 공항마다 활주로와 유도로의 배치가 각각 다르기 때문에 기능 위험 평가를 수행하고자 하는 각 공항별로 도로 분석을 수행하여 도로의 노출빈도를 도출해야 한다. 참고문헌 [9]의 연구에서 인천국제공항의 공항 레이아웃을 분석하여 활주로와 유도로의 노출빈도를 각각 8 %와 92 %로 계산하였다.

3-4 심각도 및 심각도에 따른 사고 발생 확률

심각도의 분류는 표 1과 같은 분류체계를 사용하였으며, 심각도에 따른 사고 발생 확률은 식 (1)과 같이 정의하였다.

표 5. 시정 조건의 분류 기준 및 노출 빈도
Table 5. Visibility classification and exposure.

Vis. cond. (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 400 m 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

3-5 A-SMGCS의 안전 목표 수준

ICAO 9830에서는 A-SMGCS의 총 TLS를 1.0E-08로 정의하였으며, 각 기능별 안전 목표 수준을 표 6와 같이 예측하였다. A-SMGCS의 개발 수준(A-SMGCS implementation level)이 4인 경우[15], 장비뿐만 아니라 사람에 의해서도 A-SMGCS기능이 구현 될 수 있기 때문에 표 4의 TLS값을 장비와 사람에 대해서 분할해야 한다. EMMA[17]의 연구에서 A-SMGCS의 개발 수준이 4인 장비의 TLS비율을 35 %로 정의하였기 때문에, 본 연구에서도 표 4에 대한 안전 목표 수준의 35 %에 해당하는 값을 장비에 할당하였다.

3-6 위험원에 대한 심각도 평가

위험원은 A-SMGCS 사례연구[9]에서 29개의 위험원을 식별하였다. 각 위험원에 대한 심각도 평가는 여러 가지 이벤트들의 발생을 조합하여 수행하며 해당 분야의 전문지식을 가지고 있는 사람이 평가해야 한다. A-SMGCS의 기능 위험 평가에서는 관제사가 그 역할을 수행할 수 있다.

표 6. Doc 9830에서 예측한 TLS 수준
Table 6. Estimated TLS level in Doc 9830.

A-SMGCS function	Target level of safety
Surveillance	3.00E-09
Routing	1.00E-09
Guidance	3.00E-09
Control	3.00E-09
Total	1.00E-08

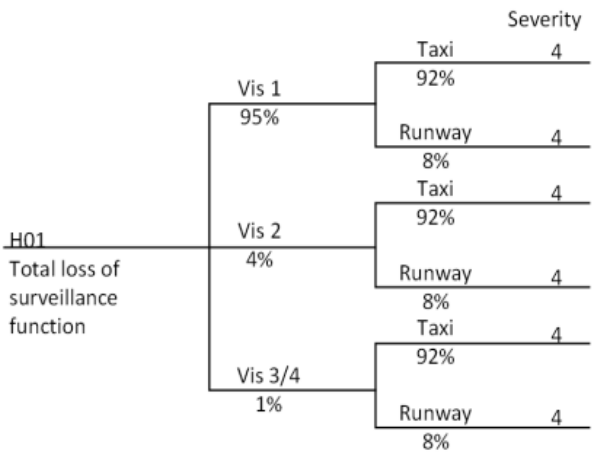

그림 1. 위험원 H1에 대한 이벤트 트리 분석 결과[9]
Fig. 1. Event tree analysis result for hazard H1[9].

그림 1은 A-SMGCS 사례연구[9]에서의 위험원 H01에 대한 이벤트 트리 분석 결과를 나타내고 있다. H01은 감시 기능의 완전 손실에 대한 위험을 의미한다. 그림 1에서 H01이라는 위험원에 대해 2가지의 이벤트가 있으며, 이는 시정조건과 도로상태이다. 시정 조건은 3가지의 경우가 있고, 도로 상태는 2가지의 경우가 있기 때문에 총 6가지의 경우의 수가 존재하게 된다. H01에 대한 위험원 평가를 위해서는 6가지 모두에 대한 심각도를 평가해야 한다. 위험원에 대한 노출빈도는 시정조건의 노출빈도, 도로 상태의 노출빈도, 심각도의 수준에 따르는 사고확률을 곱한 값이 된다. 즉, 시정 조건이 1이고 도로의 상태가 유도로이고 심각도가 4인 경우 95 % × 92 % × 1E-07이 된다. 나머지 5가지 경우에 대해서도 이와 같이 계산을 하여 식 (3)과 같이 그 값들을 더하면 그 값은 H01에 대한 위험원의 발생확률이 된다.

H01의 발생확률은 1.0E-06이 되며, H01에 할당된 tls(식 (2) 참조)에 발생확률을 나누면 그 값이 식 (4)에서 기술한 H01의 SO값이 된다. H01에 대한 안전 목표 수준의 명세는 **'감시기능의 완전 손실 위험은 1.4E-04이하가 되어야 한다'** 와 같이 표현된다. 각각의 위험원에 대해서도 위의 방법에 따라 이벤트 분석을 수행한다.

3-7 소프트웨어 보증 수준 결정

A-SMGCS 사례연구[9]에서는 각 위험원에 대한 SO가 1.0E-02 ~ 1.0E-04수준에서 값이 나왔다. 시스템 설계 단계에서 아이템을 식별하고 아이템의 기능을 할당할 때, 안전과 관련된 아이템과 안전과 무관한 아이템으로 분리하도록 설계하여 일부 아이템에 대해서만 안전과 관련된 표준을 따르도록 할 수 있다.

하지만 A-SMGCS사례에서는 각 아이템이 다른 아이템과 서로 밀접한 영향을 끼치는 방식으로 설계가 되었기 때문에 특정 아이템에 한정해서 안전 관련 속성을 할당하는 것이 어렵도록 설계 되었다. 그렇기 때문에 A-SMGCS의 기능 위험 평가 결과로 도출된 SO 중에서 가장 엄격한 기준으로 개발되어야 하는 수준을 시스템 내 소프트웨어로 개발해야 하는 모든 아이템에 적용되어야 했다. 그래서 식 (5)에 의해 모든 소프트웨어 개발 아이템에 대해 AL4로 개발하기로 결정되었다.

Ⅳ. 연구에 대한 논의 및 결론

본 연구에서는 항행 안전 시스템의 TLS기반 위험 평가 및 위험 평가결과에 대해 소프트웨어 보증 수준을 결정하기 위한 방법을 제시하였고 A-SMGCS 개발 과제의 사례를 통해 연구의 접근방법이 일반적인 항행 안전 시스템에 적용 가능함을 보였다. 하지만, 본 연구는 다음과 같은 한계를 지니고 있다.

첫 번째로 CNS/ATM 분야의 안전 평가를 위해서는 운영 개념을 기반으로 해야 할 필요가 있다. 그 이유는 CNS/ATM 시스템은 어떤 기능을 수행하기 위해 그 기능과 관련된 사람들과 그들의 업무 절차, 그리고 장비가 융합되어 있기 때문이다. 하지만 본 논문에서의 접근법은 개발 중인 장비에만 집중을 하였기 때문에 관련된 사람이나 업무 절차에 대해 고려하지 않았다.

두 번째로 이벤트 트리 접근법과 같은 방식으로 하기 위해서는 정의하고자 하는 이벤트들은 서로 독립적이어야 한다. 또한 식별된 위험원에 대한 다양한 조건을 고려하기 위해서는 다양한 이벤트가 정의되어야 한다. 그렇게 될 경우 너무 많은 경우의 수가 생성되어 분석하기 쉽지 않을 수도 있다. 이러한 경우에는 우선순위를 부여하여 보다 심각할 가능성이 있는 조건을 우선적으로 분석하는 방식으로 해결할 수도 있다.

마지막으로 본 논문에서 제시한 접근법을 적용하기 위해서는 안전 목표 수준이 해당 시스템에 할당되어 있어야 하는데, 그 기준이 없는 경우에는 적용하기 쉽지 않다는 문제도 있다.

하지만 본 연구는 일반적인 CNS/ATM 시스템의 기능 위험 평가에도 적용할 수 있도록 CNS/ATM 분야의 기능 위험 평가 체계를 정립했다는 점과 DO-278A기반의 소프트웨어 보증 수준을 결정하기 위한 방안을 제시했다는 점에서 그 의의가 있다고 볼 수 있다.

향후 연구로는 CNS/ATM 시스템에 대한 시스템 예비 안전 평가 및 시스템 적합성 평가를 수행하기 위한 방법에 대한 연구를 수행할 예정이다.

참고 문헌

[1] RTCA, Software considerations in airborne systems and equipment certification, RTCA, Washington, USA, RTCA DO-178C, 2011.

[2] RTCA, Software integrity assurance considerations for communication, navigation, surveillance and air traffic management(CNS/ ATM) systems, RTCA, Washington, USA, RTCA DO-278A, 2011.

[3] IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC, Switzerland, IEC 61508, 2010.
[4] ISO, Road vehicles-functional safety, ISO, Switzerland, ISO 26262, 2011.
[5] IEC, Medical device software-Software life cycle processes, IEC, Switzerland, IEC 62304, 2006.
[6] SAE international, Guidelines for development of civil aircraft and systems, SAE international, Warrendale, USA, Aerospace recommended practice(ARP) 4754A, 2010.
[7] SAE international, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE International, Warrendale, USA, Aerospace recommended practice(ARP) 4761, 1996.
[8] ICAO, Manual on airspace planning methodology for the determination of separation minima, ICAO, Montreal, Canada, ICAO Doc 9689, 1998.
[9] H. S. Lee, S. H. Jo and H. S. Choi, "Case study for functional hazard assessment of A-SMGCS," *The Journal of Korea Navigation Institute*, Vol.2, No.19, pp.148-154, Apr. 2016.
[10] H. H. de Jong, H. A. P. Blom and S. H. Stroeve, " How to identify unimaginable hazards?," in *Proceeding of the 25th International System Safety Conference (ISSC2007)*, Baltimore: MD, pp. 13-17, 2007.
[11] Ericson Clifton A, Hazard analysis techniques for system safety, Hoboken, NJ: John Wiley & Sons, 2005,
[12] P. Adamson, A-SMGCS level 1 and 2 preliminary safety case, Brussels, Belgium, Technical report edition 2.0, 2006.
[13] Eurocontrol, Assessment of the EATM 'air navigation system safety assessment methodology' as a means of complicane with ESARR 4, EUROCONTROL, Belgium: BE, SRC doc 12, 2009.
[14] Eurocontrol, The establishing a risk classification scheme for the design of the ATM functional system, Eurocontrol, Belgium: BE, Technical report edition 0.6, 2008.
[15] ICAO, Advanced surface movement guidance and control system(A-SMGCS) manual, ICAO, Montreal, Canada, ICAO Doc 9830, 2004.
[16] Ubiquitous korea aeronautical information system(UBIKAIS) [Internet]. Available: http://ubikais.fois.go.kr
[17] S. Paul, Functional hazard assessment and very preliminary system safety assessment report, THALES, Braunschweig, Germany, Technical report D139 FHAvPSSA V.1.0, 2006.
[18] S. B. Hong, S. H. Choi and Y. C. Choi, "A Study on the hazard identification for the implementation of A-SMGCS," *The Journal of Korea Navigation Institute*, Vol. 19, No. 1, pp. 41-47, Feb. 2015.

이 홍 석 (Hongseok Lee)
2011년 2월 : 아주대학교 전자공학과 (공학박사)
2010년 9월 ~ 현재 : 한국산업기술시험원 선임연구원
※관심분야 : 시스템 안전평가, 체계 공학, 기능 안전 시스템, 시스템 V&V

조 상 훈 (Sanghoon Jo)
2013년 2월 : 한국항공대학교 항공운항관리학과 (이학석사)
2016년 2월 : 한국항공대학교 항공운항관리학과 박사수료
※관심분야 : CNS/ATM, 운항관리, 시스템 안전평가, 시스템 V&V