ATM(Air Traffic Management) 시스템과 같은 복잡 시스템의 안전 분석 및 설계 모델

박중용*
한국항공우주연구원

Safety Analysis and Design Model for a Complex System like ATM(Air Traffic Management) System

Joong-Yong Park**

Korea Aerospace Research Institute, 45 Eoeun-Dong, Yuseong-Gu, Daejeon 305-333, Korea

Abstract : A complex system like ATM(Air Traffic Management) has safety problem emerging from complex interactions between systems. In complex systems, malfunctions of components are not the only causes of critical accidents. To resolve this problem many researchers have proposed new safety analysis models for complex systems. This research is a way of improving safety analysis model focusing on systems engineering design model for ATM.

Key Words : Safety(안전), Complex system(복잡 시스템), Air Traffic Management(항공교통관제), Systems Engineering(시스템엔지니어링)

1. 서론

항공교통 수요의 증가에 대처하고 보다 효율적이며 안전한 항공교통체계 구축을 위해서 국제민간항공기구(ICAO)는 위성항법기술과 디지털 통신 기술을 기반으로 한 차세대 위성항행시스템(CNS/ATM)으로의 전환을 선언했다.[1]

CNS/ATM은 차세대 항공통신시스템(Communication), 위성항법시스템(Navigation), 차세대 항행감시시스템(Surveillance) 및 항공교통관제(ATM) 관련 기술로 구분할 수 있다. 미래 개념에서 ATM이란 단순한 항공교통관제(Air Traffic Control)의 의미 그 이상이며 실제로 좀 더 넓은 범위를 포괄하는 관리의 시스템적 개념을 말한다. 즉, 항공교통서비스(ATS), 항공교통흐름관리(ATFM, Air Traffic Flow Management), 공역관리(ASM, Air Space Management)와 기타 비행운영과 관련된 모든 업무가 포함된다.

따라서, ATM은 그 복잡도가 상상할 수 없을 정도로 커질 것으로 예상되며 최우선적으로 안전한 시스템을 구성해야 한다는 요구사항에 직면하게 되었다. 항공기 시스템에 대한 안전 분석 기법은 어느 정도 체계가 잡혀 있다. 예를 들면, SAE에서 발간한 ARP 4761은 민간 여객기의 안전 평가를 수행하기 위한 지침과 방법을 서술하고 있는데, Functional Hazard Assessment (FHA), PSSA(Preliminary System Safety Assessment), 그리고 SSA(System Safety Assessment)를 순서

* 교신저자 : parkjy@kari.re.kr

대로 수행할 것을 제시하고 있다.[2] ATM(Air Traffic Management)과 같은 여러 시스템으로 구성된 SoS(System of Systems)나 복잡 시스템의 경우도 기본적으로는 ARP 4761의 방법을 채택하여 안전 분석을 수행하고 있으나[3], 시스템과 시스템 간에 발생하는 창발성(emergent property) 때문에 적용이 쉽지 않은 실정이다.

본 논문에서는 먼저 EUROCONTROL이 제시한 ATM의 안전 분석 기법과 이 기법의 문제점을 극복하고자 제시된 Felici[4]의 점증적 안전 분석 기법을 간단히 분석하였다. Felici의 모델은 Safety Case를 시스템의 수명주기 동안 진화시키면서 설계 모델을 위주로 된 기존 안전 분석 모델의 대안을 제시했으나, 구체적인 모델이나 구현 도구를 제시하지 못했고 safety case 자체가 아직 표준화되지 않았다는 한계가 있다.

이에, 박중용[5]이 제안한 바 있는 안전중시 시스템을 위한 동시공학적 설계 모델을 ATM과 같은 복잡 시스템의 전 수명주기 동안 적용할 수 있음을 입증하고자 한다.

2. 기존 연구 분석

2.1 EUROCONTROL의 SAM 모델

EUROCONTROL은 ATM에 대한 안전 평가 방법론(SAM : Safety Assessment Methodology)을 제시하였는데, 이 방법론은 Table 1에 나타낸 바와 같이 Functional Hazard Assessment (FHA), PSSA(Preliminary System Safety Assessment), 그리고 SSA(System Safety Assessment)의 3단계로 구성되어 있다.

이러한 개념은 ARP 4761에서 제시한 구도를 그대로 수용한 것으로 안전 평가 프로세스의 기본적인 원리를 서술하고 있지만, 특정 정황이나 프로젝트에 어떻게 적용해야하는지에 대한 정보는 충분히 제공하지 않는다는 한계가 있다. 또한, 민간 여객기의 안전 평가를 수행하기 위한 지침과 방법으로 개발된 ARP 4761이므로 창발성이 발현되는 복잡 시스템에 그대로 적용하기에는 무리가 있다.

Table 1 Concept of SAM

단계	목적	수행 시기
FHA	시스템의 전체적인 안전 요구사항 결정. 시스템의 안전 목표 규정	개발 또는 개조 착수 시
PSSA	시스템 아키텍쳐가 FHA 에서 규정된 안전 목표를 달성 가능한지 시연	설계 또는 개조 착수 시
SSA	구현된 시스템이 적절한 리스크를 감수할 수 있고, FHA에서 규정된 안전 목표를 만족하는지 시연	구현 착수 시

2.2 점증적 안전 분석 모델

Felici는 ATM과 같은 복잡 시스템의 안전 분석이 화학, 또는 원자력 플랜트에 비해 어려운 이유로 시스템 간 복잡한 상호작용을 들었다. 복잡한 상호작용이란 익숙하지 않은 일의 연속, 계획하지 않았거나 기대하지 않았던 일의 연속, 또는 가시적이지 않거나 즉각적으로 이해되지 않는 것을 뜻한다. ATM은 개방되고 역동적인 환경에서 운용되는 시스템이다. 그러한 이유로 ATM 정황 속에서 시스템 간 상호작용의 전체적인 그림을 식별하기가 쉽지 않다. Felici가 식별한 주요 상호작용은 다음과 같다.

- 비행기 통제와 ATM의 안전 기능 간의 복잡한 상호작용
- 복잡한 언어와 절차를 사용하는 인간이 불러일으키는 상호작용
- 업무 수행과 시스템이 지속적인 개선에 대한 요구와 문화에 상응하여 빠르게 진화

Felici는 2002년 7월 Tupolev TU 154M 비행기와 Boeing B757 비행기가 충돌하여 탑승객 전원이 사망하는 사고를 예로 들어 복잡한 상호작용의 위험성을 설명하였다. 두 비행기는 유사한 충돌방지 시스템인 TCAS를 장착하고 있었으며, 기체에는 어떠한 고장도 없었던 것으로 조사되었지만, 치명적 사고를 일으켰다. 두 항공기의 승무원이 관제사의 지시를 수행하는데 있어 시간적인 간격이 사고를 불러일으켰음이 밝혀졌다.

이 사고를 분석하면, 시간선과 지식(또는 정보)이 사고에 있어 중요 요인임을 알 수 있다. 사고 시나리오는 복합적인 상호작용(인간과 기계 간의 상호작용, 인간과 인간 간의 상호작용)을 포함

하는 사건의 시간대별 연속으로 구성된다. 이러한 사건의 연속은 끊임없이 지식을 재분배한다. 즉, 지식은 인간의 행동과 상호작용의 결과로 인해 지속적으로 진화하는 것이다. 사고 예에서 보듯이 같은 상황에서도 교통관제사와 승무원은 다른 지식을 보유하고 상황인식을 다르게 할 수 있는 것이다. 중요 상황에서 리스크 인지를 하는데 있어서 인식의 측면이 중요한 역할을 하는 것이다.

결론적으로, 사전 예방적이면서도 반복적인 리스크 분석, 안전 분석이 복잡한 상호작용을 규정하는 미묘한 운영상의 측면을 설명할 수 있을 것이다. 이러한 분석 결과를 반영하여 새로운 프레임워크인 점증적 안전 분석 모델을Fig.1과 같이 제시하였다.

그림에서 보는 바와 같이 시스템 모델링 전환(SMT : System Modelling Transformation), 안전 분석 모델링 전환(SAMT : Safety Analysis Modelling Transformation), 운용 모델링 전환(OMT : Operational Modelling Transformation)의 세 단계로 구성되어 있는 프레임워크는 개발된 시스템의 운용을 통해 식별된 안전 문제를 재반영하여 설계 모델까지 수정하는 진화의 특성을 보유하고 있다.

Felici는 설계 단계에서 사용된 시스템 모델은 안전이나 리스크 분석을 지원하는데 있어서는 한계가 있다고 지적했다. 설계 단계에서 정의된 기존 모델을 안전 및 리스크 분석에 채택하여 재사용하기 때문이다. 보통은 조직상 문제나 비용 문제 때문에 목적에 맞는 모델을 채택하는 것에 관해 무감각해지는 경우가 많은데, 설계 모델은 시스템 설계자의 업무를 지원하고자 만들어진 것이다. 두 비행기의 충돌 사례에서 알 수 있듯이 기능 고장이 아닌 상호작용 때문에 사고가 발생하는 ATM의 특성은 결국 운용을 통해 드러난 문제점을 반영한 모델의 진화를 필요로 한다.

Felici는 안전 분석의 기법으로 Safety Case를 채택하였다. 기존의 Safety Case가 개발 초기에 작성되고 업데이트가 안 되는 문제점을 가지고 있다고 지적하고, 주요 수명주기 별로 Safety Case를 수정 보완할 것을 주장하였다. Safety Case 표현 방법으로는 GSN(Goal Structuring Notation)을 사용했다. GSN은 Kelly[6]가 제안한 체계적인 Safety Case 관리 기법에서 채택한 모델링 방법으로서 안전 문제를 다루기 위해 안전의 목적을 하향식으로 분해해가면서 입증방안을 제시한다. 이 때 각 그래픽의 정의와 규칙이 존재한다. 하지만, GSN과 같은 방법이 Safety Case를 작성하는 표준이 아님에 한계가 있다. 이 연구는 운용 시 식별된 문제점을 안전 분석에 반영함으로써 다시 설계 모델까지 수정하는 반복하여 진화하는 모델을 제공하고, 한 번 구축된 Safety Case가 재활용될 수 있음을 보여 주었으며, 사례를 통해 사고의 주요 원인이 기대하지 않았던 복잡한 상호작용에 있음을 밝혔다. 하지만, Felici의 주장대로 설계

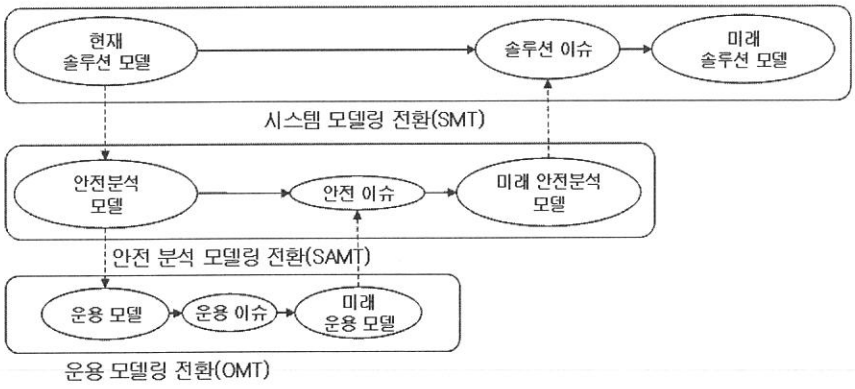

Fig.1 A framework for modelling evolutionary safety analyses

모델이 과연 안전 분석을 함에 있어 부적절한지의 여부 판단은 좀 더 검토를 필요로 한다. 또한, Safety Case의 표준이 없는 상황에서 안전 분석의 방법으로 Safety Case만을 부각시킨 것도 본 연구의 한계라 할 수 있다.

3. 설계 모델의 안전 분석에의 적용

3.1 안전중시 시스템을 위한 설계 모델

박중용이 제안한 안전중시 시스템(Safety Critical System)을 위한 동시공학적 설계 모델은 시스템, 하부 시스템, 구성품 수준으로 하향식으로 설계가 진행될 때 필요한 모델이다. 각 단계의 설계 시 적절한 안전분석 방법을 제시하고 분석 결과가 다음 단계의 설계에 반영되도록 했다. 동시에, 업무 분석 결과도 설계에 반영토록 하여 인간이 행할 수 있는 과오를 고려할 수 있도록 한 바 있다.

ATM의 사고 원인이 시스템 간의 복잡한 상호작용에 있음이 알려졌고, 그 중에서도 항공기 승무원과 관제사 간의 상호작용이 가장 큰 원인이므로 안전중시 시스템을 위한 설계 모델을 ATM에 대해 적용하기 위해서는 업무 분석이나 인간의 과오 분석 부분이 적합한지를 검토해야 할 필요가 있다.

3.2 인간의 과오 분석

인간의 과오는 비고의적인 과오와 고의적인 과오 두 분류로 나뉠 수 있다. ATM에서 발생하는 안전 사고는 주로 비고의적인 과오와 관련된 경우가 많다. 고의적인 과오는 보안 문제와도 관련이 있는 것으로 별도의 고려가 필요하다. Felici의 연구에서 사례로 든 두 항공기의 충돌 사고에서도 항공기 승무원이 관제사의 지시에 대해 늦게 반응한 것이 원인이 되었듯이 비고의적인 과오가 치명적인 사고를 이끌어낸다.

인간의 과오를 분석하는데 있어, 안전중시 시스템을 위한 설계 모델에서 권장한 방법은 Table 2에 나타낸 HAZOP(Hazard and Operability Analysis)에서 채택한 지침어와 같이 과오의 종류를 칭하는 핵심어를 활용하는 방법이다.[7]

위 표와 같이 인간의 과오를 분류하여 이를

Table 2 Classification of Human Error

	인간 과오의 종류
1	너무 이르거나 늦은 행동
2	완전 또는 부분 생략
3	과다 또는 과소의 행동
4	너무 길거나 짧은 행동
5	잘못된 방향으로의 행동
6	잘못된 목표에 따른 올바른 행동
7	올바른 목표에 따른 잘못된 행동
8	정보 획득 실패
9	잘못된 정보 획득
10	조정 불량(인간과 기계의 과오 동시 발생)

ATM의 기능분석 또는 운용개념 분석 시 적용하여 안전 분석을 수행한다면 ATM을 구성하고 있는 시스템 간의 복잡한 상호작용 중 인간의 과오 때문에 발생할 수 있는 위험을 줄이는데 상당 부분 기여할 수 있다.

3.3 사례 연구

Felici의 연구에서 언급한 두 항공기의 충돌 사고를 사례로 하여 인간 과오 분석 측면을 강조한 설계 모델이 안전 분석을 효과적으로 수행할 수 있는지 입증하고자 한다. Felici가 정리한 항공기 충돌 사고의 시나리오는 Table 3과 같다.

이 사고를 다루기 위해서는 ATM 시스템의 경계를 먼저 정의하는 것이 중요하다. Felici는 설계 모델을 안전 분석에 사용할 경우 대상 경계가 맞지 않아 그대로 사용하는데 어려움이 있다고 분석한 바 있다. 그러나, 시스템엔지니어링 원리에 따라 최상부 시스템에서부터 하부 시스템까지 운용개념이나 기능분석을 수행한다면 이러한 문제점을 극복할 수 있다.

본 사례에서는 Fig.2와 같이 관제사, 두 항공기의 승무원과 충돌방지시스템인 TCAS가 주요 구성요소이다. 이중에서 항공기 TU 154M을 주요 분석 대상으로 선정하여 기능분석을 수행하면 Fig.3과 같다. 항공기의 승무원과 충돌방지시스템, 그리고 근처 공항의 관제사가 구성요소이다. FFBD(Functional Flow Block Diagram)을 통해 기능분석한 결과만 보면 별 다른 이상이 없어 보인다. 하지만, 위험 분석을 수행하면, 다른 결과가 도출될 수 있다.

Table 3 Accident Scenario

시간	행위자	사건
T1	$TCAS_B$, C_B $TCAS_T$, C_T	양쪽 비행기의 TCAS가 충돌 경보를 보냄.
T2	ATCer, C_T	교통관제사가 TU 154M 승무원에게 지시 : 비행고도 350으로 하강하라. 서둘러라. 충돌할 수 있다.
T3	$TCAS_B$, C_B $TCAS_T$, C_T	양쪽 비행기가 TCAS의 결의 경고를 받음. B757 승무원은 이에 동의했으나, TU 154M 승무원은 여전히 비행고도 360을 유지함.
T4	ATCer, C_T	교통관제사가 TU 154M 승무원에게 하강하라고 재차 지시하고 TU 154M 승무원은 이에 동의함.
T5	$TCAS_B$, C_B	"하강하라"
T6	C_B, ATCer	B757 승무원은 교통관제사에게 TCAS 하강 중이라고 보고함.
T7	$TCAS_T$, C_T	"상승하라"
T8		충돌
ATCer : 교통관제사, $TCAS_B$: B757 충돌방지시스템, C_B : B757 승무원, $TCAS_T$: TU 154M 충돌방지시스템, C_T : TU 154M 승무원		

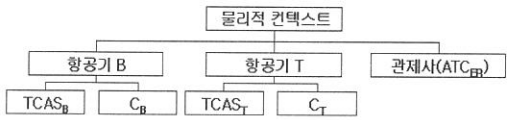

Fig.2 Physical Context of ATM Example

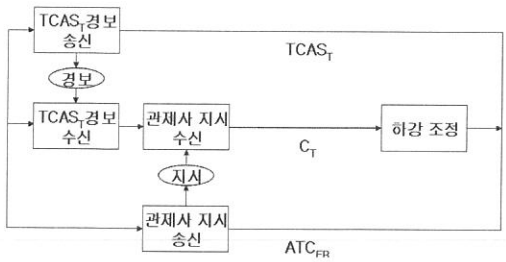

Fig.3 Functional Flow of Collision Protection

본 사례에서 승무원을 비롯한 항공기의 시스템은 기능상 문제를 일으키지는 않았지만, 승무원이 관제사의 지시에 다소 늦게 대응하는 비고의적 과오를 행함으로써 두 비행기는 동시에 하강하여 충돌하였다. 위의 FFBD에서 항공기의 승무원이 관제사의 지시를 수신한 후 빠른 대응을 했거나, 아니면 충돌방지시스템이 다시 한 번 경고를 했으면 사고를 피할 수 있었다.

설계 모델에서 이러한 관계를 구축하는데 있어서 Fig.4와 같은 스키마를 필요로 한다. Fig.3의 기능이 어떤 위험을 내포하고 있는지, 특히 인간 과오의 측면에서 가능한 위험이 무엇인지를 Table 2에서 분류한 인간 과오의 종류별로 식별한다.

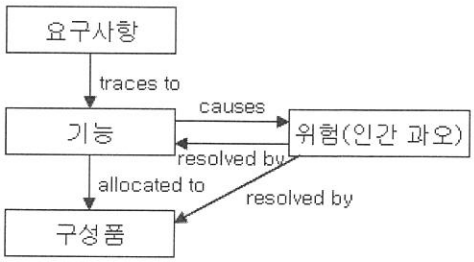

Fig.4 The Schema for safety analysis

식별된 각 위험을 해소할 수 있는 방안을 기능이나 구성품에 추가하면 위험 분석의 결과를 설계에 반영하게 된다. 인간 과오에 대한 일반적인 해결책으로 Kirwan이 정리한 것은 다음과 같다.[8]

- 업무를 자동화하거나 연동장치 또는 거동 측면에서 기능을 강화
- 피드백을 활용하거나 절차를 점검하고 성능을 자동으로 모니터링
- 절차, 훈련, 인터페이스 설계를 개선함으로써 과오의 가능성 축소

본 사례에 위의 일반적 해결방안을 적용하면 우선적으로 고려할 수 있는 것이 충돌방지 절차의 교육 강화와 절차서의 개정이 될 수 있다. 즉, 승무원이 충돌방지시스템의 경고와 관제사의 지시에 따라 업무를 수행하기 직전 다시 한 번 항공기의 고도와 위치가 다른 항공기의 경로와 문제없는지 확인하는 절차를 의무화하는 것이 한 해결책이 될 수 있다. 충돌방지시스템의 기능을 강화하여 타 항공기의 경로가 변경되었을 시 이를 즉각적으

로 탐지하여 승무원에게 새로운 정보를 실시간으로 제공하고 경고를 보낼 수 있게 하는 방안도 필요하다.

절차서도 항공기의 군수지원품목 중의 하나로서 물리적 아키텍쳐의 한 종류가 되므로 절차가 개선된 사항을 Fig.4의 스키마를 이용해 전산지원도구에 저장하게 되면 위험 분석의 결과가 설계에 어떻게 반영되었는지를 데이터베이스화 할 수 있다. 이를 위해서는 상용 시스템엔지니어링 도구를 선정하여 Fig.4와 같은 스키마를 구축하고, 인간과오와 같은 엘리먼트에 가능한 인간 과오 데이터베이스를 기입하여 활용하면 된다. CORE를 이용한 모델의 실제 구축의 예는 선행 연구에서 이미 소개한 바 있다.[5]

결론적으로 Felici가 Fig.1로 제시한 운용 모델링, 안전 분석 모델링, 시스템 모델링을 모두 포함하는 모델을 기존의 동시공학적 설계모델의 스키마를 활용하여 구체적으로 구현할 수 있음을 알 수 있다.

4. 결론

안전 분석을 위한 모델은 설계를 위한 모델과는 차별화되어야 하며, 이를 위해 Safety Case를 운용 단계에서도 업데이트하여 그 결과를 설계 모델에 적용해야 한다는 선행 연구에 대해 시스템엔지니어링 기법을 적용한 설계 모델을 인간 과오 분석을 강조하여 수행함으로써 안전 분석 결과까지 반영할 수 있다는 것을 입증하였다. 선행 연구에서는 큰 틀의 모델만 제시하고 구체적 모델에 대해서는 언급하지 않는데 반해, 본 논문에서는 운용 결과 산출되는 safety case 데이터를 설계 모델에 반영하여 통합 모델을 구축하는 프로세스를 간단한 예를 통해 보였다.

향후에는 기존의 안전중시 시스템 개발용 동시공학적 설계 모델을 더욱 개선시켜 ATM 시스템 개발에 적합하도록 할 것이며, 이를 위해 AF(Architecture Framework)와 Enterprise 아키텍쳐의 연구 성과를 접목시킬 예정이다. 또한, 통합 모델에서 Safety Case를 효과적으로 활용하기 위한 방안도 중요 연구대상이다.

후기

본 연구는 산업자원부 한국형헬기 민군겸용구성품개발사업 수행 결과의 일부이며, 지원에 감사드립니다.

참고문헌

1. Joong-Won Bae, Overview of Communication Technologies for CNS/ATM, KARI Technical Memo KARI-AV-TM-2004-010-v.1-rev.0, 2004.
2. Society of Automotive Engineers, ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.
3. EUROCONTROL, Air Navigation System Safety Assessment Methodology, 1st ed., 2000.
4. Massimo Felici, Capturing emerging complex interactions : Safety analysis in air traffic management, Reliability Engineering and System Safety, Vol. 91, pp. 1482-1493, 2006.
5. Joong-Yong Park and Young-Won Park, Model-based Concurrent Systems Design for Safety, Concurrent Engineering : Research and Applications, Vol. 12, No. 4, pp.287-294, 2004.
6. T. P. Kelly, Arguing Safety - A Systematic Approach to Managing Safety Cases, Ph.D. Thesis, University of York, pp. 3, 1998.
7. F. Redmill and J. Rajan, Human Factors in Safety-critical Systems, Butterworth Heinemann, pp. 51, 1997.
8. A. Hussey and B. Atchison, Technical Report No. 00-18: Hazard Analysis of Interactive Systems, Software Verification Research Centre, School of Information Technology, The University of Queensland, pp.9, 2000.