

무인이동체시스템 개념설계 단계에서 기능분석 결과를 활용한 Fault Tree 도출

정호전*, 장홍석*, 강지성*, 유정훈*

*한국산업기술시험원

e-mail:hjjeong@ktl.re.kr

Deriving Fault Tree Using the Result of Functional Analysis in the Conceptual Design Stage of the Unmanned Aircraft System

Ho-Jeon Jeong*, Hong-Seok Jang*, JiSung Kang*, JeongHoon You*

*Korea Testing Laboratory

요약

무인이동체시스템은 주로 영상촬영 및 레저용으로 활용되어 단순한 임무장비의 탑재와 기본적인 비행기능 및 촬영기능 정도가 요구되어왔다. 그러나 무인이동체시스템이 군사, 상업, 공공 분야에서 다양하게 활용되기 시작하면서 무인이동체 시스템에 요구되는 물리적, 기능적 복잡도 및 SW의 비중이 증가하고 있다. 우편배송을 위한 자동적재함의 탑재, 산불의 초기대응을 위한 소화탄 및 체결장치 등 탑재되는 임무장비가 증가하고 있고, 임무수행을 위한 기능이 복잡해지고, 기능의 수행을 위해 AI기반 영상분석 기술, 다양한 후처리 SW시스템과의 연계 등이 이뤄지고 있다. 기존에는 무인이동체 시스템의 운영을 제한함으로써 안전을 확보해왔으나 이와 같이 물리적, 기능적으로 복잡해지고 다양한 운영환경에서 운영되는 무인이동체시스템에 대해서는 시스템 개발단계에서부터 위험분석을 수행하여 안전을 확보할 필요가 있다. 더불어 무인이동체시스템에서 SW의 비중이 매우 높으므로 기능안전 측면에서의 안전성 확보가 필요하다. 이를 위해 본 연구에서는 대표적인 고장분석 기법인 FTA를 무인이동체시스템에 적용하기 위해 기능설계 기반의 Fault Tree 도출에 관한 연구를 수행하였다. 무인이동체시스템의 개념설계 단계에서 기능분석 결과를 바탕으로 기능의 오류를 식별하고 이를 기반으로 무인이동체시스템에 대한 Fault Tree를 도출하였다. 도출된 Fault Tree를 활용하여 무인이동체시스템에서 발생 가능한 다양한 형태의 고장을 분석하였다. 향후 무인이동체시스템에 대한 고장률 데이터가 축적되면 Fault Tree에 활용하여 무인이동체시스템에 대한 안전 목표를 설정하는데 활용 할 수 있을 것이다.

1. 서론

무인이동체는 4차 산업혁명 시대의 핵심 산업으로서, 항공·ICT·센서 등 첨단기술의 융합산업으로 4차 산업혁명 시대의 신기술들이 서로 어우러져 혁신을 이끌어낸다. 무인이동체는 민간에서는 영상촬영 및 레저용으로 주로 활용되다 점차 다양한 산업 분야에서의 활용이 이뤄지고 있다. 국내에서는 무인이동체 분야의 산업을 촉진시키기 위해 드론법 제정 등 법·제도적인 지원뿐만 아니라 공공수요를 기반으로 한 무인이동체의 연구개발이 이뤄지고 있다. 재난/재해 대응, 주요 시설 감시정찰, 우편배달 등 무인이동체 기반의 공공서비스를 제공하여 공공서비스의 질을 향상시키고 중소기업들에게 무인이동체 시장의 진출을 지원하고 있다. 이와 같이 다양한 임무를 수행하기 위한 무인이동체의 개발이 증가함에 따라 무인이동체에 대하여 요구되는 능력과 운영환경이 다양해지

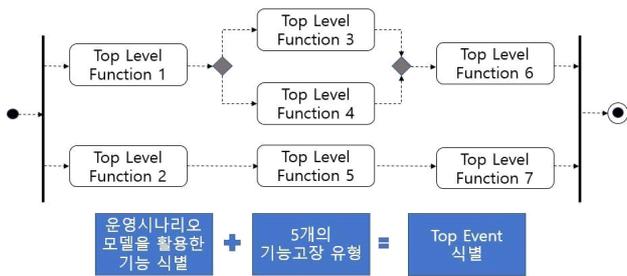
고 있다. 이에 따라 기존의 무인이동체에 요구되던 기능보다 더 많고 복잡한 기능들이 요구되고 있으며, 이로 인해 기능적·물리적 복잡도가 증가하고 있다. 기능적·물리적 복잡도가 증가한 무인이동체의 개발 및 운영을 위해서는 기존의 운영상의 제약을 통해 안전성을 확보하는 것에서 나아가 무인이동체에 대한 안전설계를 통해 시스템 안전성을 확보하는 것이 요구된다. 이를 위한 본 연구에서는 무인이동체시스템의 개념설계단계에서 수행되는 기능분석 결과를 활용하여 대표적인 위험분석 기법인 FTA를 적용하기 위한 Fault Tree 도출방안에 대해 연구하였다.

2. 기능분석 기반의 Fault Tree 도출 방법

2.1 운영시나리오 모델을 활용한 Top Event 결정 방법

운영시나리오는 대상시스템의 최상위의 기능모델이라 할

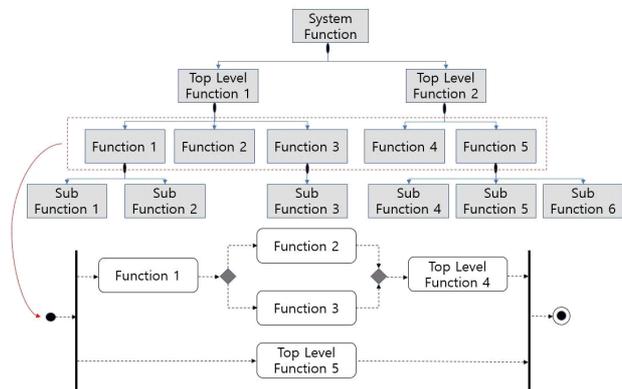
수 있기 때문에 설계초기에 도출된다. 그림 1은 SysML의 Activity Diagram을 활용하여 생성한 운영시나리오 모델의 예시를 나타내고 있다. 생성한 운영시나리오 모델로부터 최상위 수준의 기능을 식별하고 기능들의 순서, 기능 간 상관관계를 분석할 수 있다. 이를 활용하여 Fault Tree의 Top Event를 결정한다. Top Event는 앞서 분석된 기능에 대한 정보를 바탕으로 분석한 기능오류로 정의 할 수 있다.



[그림 1] SysML 기반 운영시나리오 모델

2.2 기능분석 결과를 활용한 기능기반 Fault Tree 생성 방법

개념설계단계에서 기능분석을 수행함으로써 도출되는 대표적인 산출물은 기능구조와 기능의 거동모델이라 할 수 있다. 기능구조는 운영시나리오 모델에서 식별된 최상위 수준의 기능들을 분해하여 어떠한 기능들의 조합을 통해 최상위 수준의 기능이 수행 될 수 있는지를 파악할 수 있도록 상하위 기능들 간의 추적성을 제공한다. 기능구조를 활용하여 하위 기능들의 오류의 조합으로 상위 수준의 기능의 오류가 발생한다는 것을 파악할 수 있다. 이를 근거로 Fault Tree의 Event를 분해해 나갈 수 있다.



[그림 2] 기능 구조 및 거동모델

거동 모델은 기능들 간의 상호관계, 즉 기능간의 인터페이스를 식별하는데 활용 할 수 있다. 인터페이스 정보는 Event를 분해하는 또 다른 정보로 활용 할 수 있다. Fault Tree에서 상하 Event는 and, or gate로 조합이 이뤄지게 된다. 동일 수준의 기능들 간의 인터페이스 분석을 통해 and, or gate 중 어떤 gate가 적절한지 식별할 수 있게 된다.

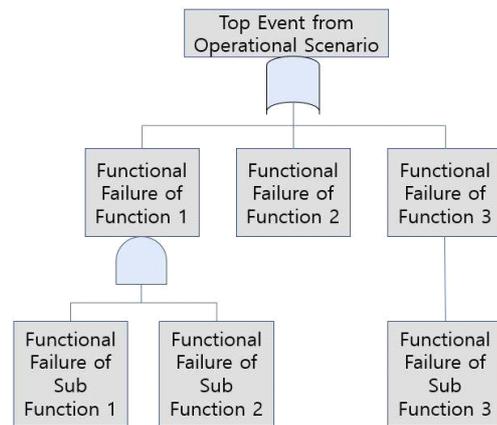
그림 2는 System Function 에 대해 Top Level Function부터 SubFunction 까지 식별한 기능구조와 Function Level의 기능에 대한 거동모델을 도출한 예이다.

Fault Tree를 도출하기 위해 Event를 분해 및 조합하는 절차는 다음과 같다.

첫째, 기능구조를 통해 최상위 수준의 기능이 분해된 기능들을 식별한다. 그 후 식별된 기능들 각각의 오류를 식별한다. 식별된 각각의 오류들은 Top Event 아래의 Intermediate Event가 된다.

둘째, 앞 단계에서 식별한 Intermediate Event들 간의 조합을 또 다른 산출물인 거동 모델을 통해 식별한다. 즉 개별 기능의 오류는 or gate로, 여러 기능들의 조합은 거동모델을 기반으로 병렬연결 되는 기능이 동시에 수행되는 것인지, 어느 하나가 수행되는 것인지를 식별하여 전자의 경우 or gate, 후자의 형태는 and gate로 조합을 한다.

위의 두 단계에 따라 점차 Event를 식별하고 분해해가며 기능트리의 가장 하위의 기능에 관련된 Event를 식별할 때까지 반복적으로 수행한다. 그림 3는 기능구조와 거동모델 분석결과를 기반으로 Fault Tree를 도출한 예이다.



[그림 3] 기능 기반 Fault Tree

3. 결론

본 논문에서는 물리적, 기능적으로 복잡해진 무인이동체시스템의 안전성을 설계단계에서부터 확보하기 위해 개념설계

단계에서 기능설계 결과를 활용하여 Fault Tree를 생성하는 방법을 도출하였다. 현재는 무인이동체시스템의 기능 고장 및 시스템을 구성하는 구성품에 대한 고장률 데이터가 충분히 축적되지 않아 정량적인 평가까지는 수행이 안 되지만, 향후 신뢰할 수 있는 데이터가 축적되면 정량적인 평가까지 수행이 가능할 것이다. 이를 통해 설계단계에서부터 허용 가능한 수준의 위험수준으로 통제된, 안전이 확보된 설계를 수행하고 구현함으로써 지금과 같이 제한된 지역에서의 운영뿐만 아니라 다양한 지역에서의 활용을 위해 안전성이 확보된 무인이동체시스템의 설계 및 구현이 가능 할 것 이다.

참고문헌

- [1] 항공우주연구원, “4차 산업혁명의 도래와 드론”, Aviation Issue No.13, pp. 1-5, 1월, 2017년
- [2] 이준원, 강왕구, 김명집, “국내 무인이동체 산업실태 조사 연구”, 항공우주산업기술동향, Vol.16, No.2, pp. 27-35, 2018년
- [3] Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission Standard, IEC 61508,2010.
- [4] A. Scharl, K. Stottlar, R. Kady, "Functional hazard analysis methodology tutorial," in Proc. International System Safety Training Symposium, St.Louis, MO, Aug. 4-8, 2014, pp. 1-17.
- [5] R. B. Stone, I. Tumer, M. Van Wie, "The function-failure design method," Journal of Mechanical Design, vol. 127, no. 3, pp. 397-407, Jul. 12, 2004.