

論文

단일추진시스템의 ACM 설계 및 사례연구

이영진*, 이권순**, George Vachtsevanos***

A Design of Automated Contingency Management and Case Study
for Monopropellant Propulsion System

Young Jin Lee*, Kwon Soon Lee** and George Vachtsevanos***

ABSTRACT

Increasing demand for improved reliability and survivability of mission-critical systems is driving the development of health monitoring and Automated Contingency Management (ACM) systems. An ACM system is expected to adapt autonomously to fault conditions with the goal of still achieving mission objectives by allowing some degradation in system performance within permissible limits. ACM performance depends on supporting technologies like sensors and anomaly detection, diagnostic/prognostic and reasoning algorithms. This paper presents the development of a generic prototype test bench software framework for developing and validating ACM systems for advanced propulsion systems called the Propulsion ACM (PACM) Test Bench. The architecture has been implemented for a Monopropellant Propulsion System (MPS) to demonstrate the validity of the approach. A Simulink model of the MPS has been developed along with a fault injection module. It has been shown that the ACM system is capable of mitigating the failures by searching for an optimal strategy. Furthermore, the concepts of Validation and Verification (V&V) of such systems are introduced with relevant examples.

Key Words : Automated contingency management(ACM), Monopropellant propulsion system(단일추진시스템), Fault diagnosis, Validation & varification(V&V)

1. 서 론

항상 위험한 상황에 처하거나 보다 높은 안전성을 요구하는 시스템의 경우, 그 신뢰성(Reliability)과 생존가능성(survivability)을 확보하기 위하여 다양한 HM(health management)이나 고장 허용제어(fault-tolerant control)와 같은 연

구가 이루어지고 있다. 이러한 시스템은 고장발생을 감지할만한 성능이 남아있는 동안에는 고장을 항상 검출할 수 있도록 설계되어야 한다. 최근에는 이와 관련하여 NASA/DoD 등에서는 다양한 군사 또는 항공우주용 추진시스템(Propulsion system)에 적용을 위하여, 시스템의 초기단계에서 오류의 검출 및 분류 목적으로 이와 같은 기술을 접목한 많은 추진시스템의 상태 모니터링 기술들이 개발되고 있다[1-4]. ACM(Automated Contingency Management) 시스템은 특히, 차세대 항공우주 추진시스템을 위해 적응형 엔진동작 재구성의 필요성이나 강인한 고장 적응성과 갖는 높은 신뢰도를 가진 추진시스템의 설계를 가능하게 하고 이러한 기술들을 구현하여 실제 시스템에 적용할 수 있도록 해준

2008년 5월 2일 접수 ~ 2008년 6월 22일 심사완료

* 한국폴리텍 항공대학 항공전기과

** 동아대학교 전기공학과

*** Georgia Institute of Technology

저자연락, E-mail : airlee011@hanmail.net

다. 일반적으로 ACM 기술은 긴박한 시스템 오류 상태를 바로잡기 위하여 다목적(Multi-objective) 목적함수를 갖는 최적화 과정을 수행하며, Table 1과 같은 이점들을 가질 수 있다[5].

본 논문은 이러한 이점을 갖는 ACM 시스템 설계를 위하여 단일추진시스템(Monopropellant propulsion system)에 대하여 고장상태를 주입하고 시뮬레이션 수행과정을 통하여 ACM 알고리즘 자체의 평가를 위한 test bench 개발에 관하여 기술하였다. 설계된 ACM 시스템을 위하여 Matlab/Simulink와 같이 매우 보편화된 공학적 플랫폼을 적용함으로써 범용성을 가지면서 성능 좋은 추진 시스템 설계가 가능한 방법론을 제안하였다. 본 논문의 구성은 다음과 같다. 먼저, 2장에서 ACM 시스템을 설계하기 위한 일반적인 해결방안과 원리를 기술하였으며, 3장에서는 MPS(Monopropellant propulsion system)에서 ACM의 의미와 개념, 그리고 적용방안에 대하여 기술하였다. 4장에서는 시뮬레이션에 필요한 시나리오와 이를 기반으로 하는 시뮬레이션 결과를 기술하였으며, 마지막으로 5장에서는 본 논문의 결론과 향후 연구계획에 대하여 기술하였다.

Table 1. The merit of ACM system

장 점	내 용
Design safety margin	<ul style="list-style-type: none"> ■ 안전성에 대한 제한적인 설계한계점 극복을 통한 시스템 성능의 향상
Higher effective reliability	<ul style="list-style-type: none"> ■ 주어진 임무를 달성할 수 있는 높은 신뢰성 확보
Reduced human burden	<ul style="list-style-type: none"> ■ 시스템 자체의 자율성이 증가함에 따른 사람의 작업부하 경감
Accurate contingencies	<ul style="list-style-type: none"> ■ 기술적으로 적절한 유연성(contingency) 확보 (이는 시스템 운영을 정지하지 않고도 그 상태를 복원할 수 있음을 의미함)
Optimization of maintenance intervals and prioritization	<ul style="list-style-type: none"> ■ 시스템의 특정 부품에 대한 유지보수기간을 최적화할 수 있는 능력 확보 ■ 계획된 유지보수기간 동안 이루어지는 작업의 우선 순위화 가능

II. Automated Contingency Management

대부분의 동적시스템은 시스템 내부에 고장으로 발전될 수 있는 요소들을 가지고 있으며, 이러한 시스템에 있어서 신뢰성과 유효성(availability)은 시스템이 독립적으로 존속할 수 있는지의 여부를 결정짓는 중요한 요소가 된다. 만약, 독립시스템 일 경우, 유효성은 그것이 언제든지 이용될 수 있는 준비상태를 의미하며, 실행가능성 요소는 시스템이 정상적으로 동작하는 상태가 얼마나 지속적으로 제공 되어지며, 그 상태를 유지할 수 있는가를 나타낸다. 그리고 안정성은 기밀성(confidentiality)을 가능한 보존할 수 있는 상태를 의미한다[6]. 뿐만 아니라 이와 같은 시스템들의 특성들이 독립적으로 고려되질 수 있다고 하더라도, 실제 현실에서는 이들은 상호 의존적이라 할 수 있다[7]. 예를 들면, 실현할 수 없는 시스템은 바람직하지 않기 때문이다. 다시 말해 이러한 시스템은 적어도 바람직한 동작을 하지 않으며 또한 어떤 시스템이 신뢰성을 보장받기 위해서는 시스템 개발의 모든 면에서의 신뢰받는 것이 요구되고, 각 단계들은 설계 및 평가시 뿐만 아니라 실제 구현 시에도 고려가 되어야 하며, 미래에 일어날 유지보수를 위해서도 함께 고려가 되어야 한다.

이러한 견지에서 고장의 출현함에 있어서 그 시스템이 어떤 상태에 있느냐에 따라 이를 해결하는 방법으로 고장방지(Fault Avoidance), 고장제거(Fault Removal), 고장허용(Fault Tolerance), 그리고 고장회피(Fault Evasion) 크게 4가지 방법으로 고려할 수 있다. 먼저, 고장회피는 설계 단계에서 비준(validation)과 검증(verification) 과정을 거쳐 초기단계에서부터 가장 대표적인 여러 가지 고장들을 사전에 제거하는 방법을 의미한다. 고장제거는 설계 단계에서의 검증을 거친 시스템 상에 여전히 남아있는 고장들을 제거함을 의미하고 고장허용은 시스템이 동작 중에도 발생할 수 있는 다양한 고장을 의미하며, 이때, 고장진단 시스템은 해당 고장을 진단(diagnosis), 분리(isolation), 인지(identification)과정을 통하여 이를 해결할 수 있다. 마지막으로 고장회피는 고장이 발생되기 전에 미리 예측하여 이를 회피할 수 있도록 해주며, 이를 위해서는 우수한 예방능력을 가지는 예방진단능력이 요구된다고 할 수 있다. ACM 시스템은 고장회피와 같은 예방진단능력을 지니고 있어야 하며, 고장의 허용에 대한 제어의 한 부분으로 고려될 수 있다. 따라서, 이상과 같이 언급한 4가지 기능을 모두 갖춘 고장진단 시스템에 대한 다소 복잡한 설계 과정이 이루어져야 한다.

2.1 ACM Requirements Definition

비록 시스템의 성능평가가 하나의 응용영역에서 다른 영역으로 변화되어지는 다양한 유형의 시스템에 대하여 이루어질 수 있다 하더라도, 그 시스템이 매우 중대한 산업용 프로세스에 대하여 수행되거나 설계가 행해질 경우에는 그 시스템은 적어도 다음과 같은 일반적인 필요조건이 충족되어야만 한다[5].

- Operation and support(O&S) cost: 고장 진단 시스템은 대상 시스템에 대한 막대한 비용을 줄이거나 안전에 대한 보증이 요구됨.
- Open system: 또한, 이러한 시스템은 대상 시스템이나 프로세서의 인터페이스 변화가 최소화되는 동안에 부시스템이나 구성요소의 변화, 시스템 증축 및 교환 등이 최대한 용이할 수 있는 개방형 구조의 시스템 설계가 요구됨
- RAM-D: 시스템 신뢰성, 유효성, 보수능력과 지속성 등의 요소가 필수적으로 요구됨
- Scalability: 필요한 데이터가 측정 가능해야 함
- User requirements: GUI등을 이용한 사용자 편의성 도모
- Compatibility: 센서, 구성요소, 디바이스 등의 호환성이 요구됨

※ RAM-D: Reliability, Availability, Maintainability, and Durability

Fig. 1은 시스템에 임의의 임무(mission)가 주어졌을 때 이를 수행하는 과정에서 발생될 수 있는 4가지 상태를 나타내며, 이를 극복하기 위하여, 구현된 ACM 시스템이 갖추어야 할 목표와 특징을 나타내고 있다. 그 4가지 상태는 Mission success, Safety, Reconfiguration, Fail-safe 모드로 구성되며, Mission success 상태는 시스템이 원하는 목표에 도달된 상태를 나타내며, 이때, ACM 시스템은 Safety 모드의 요구사항들을 만족하면서 Mission success를 구현하도록 구성이 되어야 한다. Reconfiguration는 시스템이 목표를 안전하게 수행하기 위하여 주어진 여러 가지 제약조건에 만족되는 가용할 수 있는 자원들에 대한 최적으로 활용하는 상태를 의미하며, 이때에는 시스템의 목표를 수정하거나 redundancy와 같은 ACM 시스템의 핵심적인 기능이 작용된다. 만약 임의의 상황에서 이들 중 어느 것 하나라도 실현 가능하지 않다면, 시스템에 예상되는 손실을 피하기 위하여 Fail-Safe 모드로의 변환이 고려되어질 것이다[8-9].

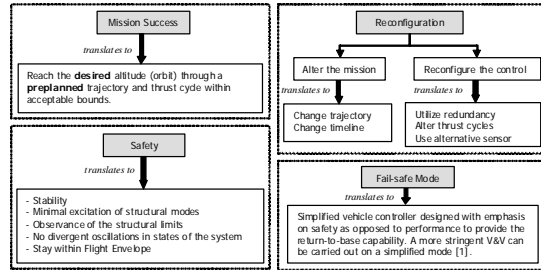


Fig. 1 Objectives and characteristics of an ACM system

본 절에서는 이러한 시스템을 개발하기 위하여 반드시 도입되어야 하는 기본적인 방법론을 상세하게 기술하고자 한다. 아래 기술된 바와 같이 ACM 알고리즘을 제약조건을 갖는 최적화 문제로서 정의할 수 있다.

"사전에 정의된 시스템 제약조건과 시스템의 현재 상태가 주어지면, 최소비용과 높은 성공 확률을 가지고 시스템이 원하는 상태에 도달될 수 있는 최적의 방법을 찾는 일"

이 최적화 문제를 정형화하기 위해서는 우리는 모든 중요한 파라미터나 제약조건을 포함하고 이를 검증할 수 있는 하나의 방법론을 제안하여야 한다.

2.2 ACM Criteria Identification

시스템 동정(Identification)에 필요한 중요한 기준들은 ACM에서 언급되어야 할 모든 기준 과정을 수용하기 위한 핵심 단계이다. Table 2에 이들 기준 중 일부가 정의되거나 분류되어져 있으며, 이 리스트는 그 시스템이 유효한 것에 대한 더 많은 정보로 확장되어 이용될 수 있다. Table 2에서 좌변은 일반적인 기준을 나타내며, 우변은 항공기 시스템 등에서 예상되는 해당 예제상황을 나타낸다. 이와 같은 기준에 대한 전 리스트가 일단 완료되어야 이에 따른 최적화 문제의 구성이 가능하다 할 수 있다.

2.3 ACM Strategy

ACM으로 보호된 시스템은 FSM(Finite State Machine)에 의하여 Fig. 2와 같이 표현될 수 있다. FSM 시스템은 Nominal state, Failure state, Fail-safe/Degraded state의 3가지 상태공간으로 나타낼 수 있으며, 시스템은 이들 상태를 오가는 다중 상태 구조를 가진다.

Table 2. Important criteria to identify before ACM design

Fault modes and their relative severity	<ul style="list-style-type: none"> - What actuators and valves can get stuck - Pressure sensors may be broken - Leakage of gas - Excessive temperature - Abnormal pressure increase - Structural failures (crack on surface, failed mechanical component) - Short circuit in electrical wiring or an open circuit
Mission critical components	<ul style="list-style-type: none"> - Constant fuel pressure in ignition chamber - Adequate thrust generation for the planned trajectory - Correct position sensing - Engine related hardware
Safety critical parameters	<ul style="list-style-type: none"> - Roll rate within bounds - Pitch rate within bounds - Smooth mode transitions - Sustainable body velocities (longitudinal, lateral and vertical) - Safety related hardware
Design specifications (sustainable material property limits for temperature, shear and compressive stress etc)	<ul style="list-style-type: none"> - Aircraft surface temperature should not rise beyond a limit. Thus speed may be altered based on atmospheric conditions - Inside air pressure should be bounded - Excitation frequencies for various critical structural modes - Rate of consumption of resources in different operating modes - Most efficient rates of consumption in nominal modes
Consumable resources and their availabilities	<ul style="list-style-type: none"> - Available fuel or any other energy sources - Available time to accomplish mission without running out any of the resources - Available computational memory, computational power and bandwidth of data channels
Available alternatives for mission critical and safety critical operations and their costs/rewards	<ul style="list-style-type: none"> - An alternative trajectory planning: may require longer time and more fuel - Re-routing a gas path to avoid stuck valve - Switching of some less important modules to conserve energy - Employ analytical redundancy to overcome dead sensors, may need more computations & bandwidth - Alternative to abort the mission and come back

Contingency는 시스템을 고장 상태로 만들 수도 있으며, 만약 임의의 상태에서 해당 시스템이 보수가 가능한 고장의 상태에 놓여있다면 시스템은 다시 정상상태로 돌아올 수 있다. 하지만, 그렇지 않은 경우 즉, 보수가 가능치 않은 시스템 고장에 대해 더 큰 위험상태를 막기 위해, 일단 시스템을 고장-안전 상태로 전환한 후 외부의 수리가 이루어질 수 있도록 시스템 상태에 대한 정보를 통보하도록 구성되어 있다.

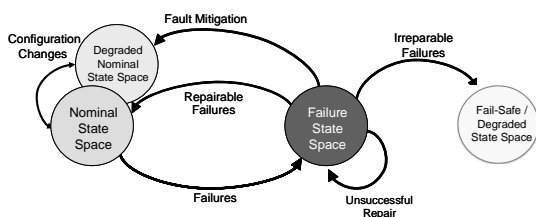


Fig. 2 ACM strategy for failure mitigation

III. 사례 연구

Fig. 3은 MPS(Monopropellant propulsion system)를 사용하는 개념적 원리가 설명된 전체적인 레이아웃을 나타낸다. 미션 레벨(Mission level)의 목표는 외부 명령들로 대응될 수 있다. 예를 들면 시스템의 다양한 입력으로 사용되어지는 거리, 증가속도, 동작 정지 명령 등을 들 수 있다. 일단 시스템에 문제가 발견되면 Stateflow Model은 적절한 비용으로 가능한 정정행위 절차를 수행하기 위하여 의사결정자에게 고장을 알리면 ACM 시뮬레이터가 구동되어 Dynamic Cost Model등을 이용하여 의사결정자는 최소비용과 같은 특별한 조건에 기준하여 결정하게 된다. 이러한 정정 동작은 시스템 모델링에 적용되어진다. 한편 Fault Simulator는 밸브 자체의 고장, 생산 라인의 조절기 오류나 추진가스의 누수와 같은 다양한 고장을 만들어 모의시험을 할 수 있도록 구성되어 있다. MPS를 위한 Simulink® model은 ACM 기능을 갖는 CBM/ PHM(Condition Based Management/Prognosis and Health Management) 개발을 위한 테스트 벤치마크로서 구현되어졌다. 이 MPS model은 NASA의 Fault Tree Handbook [10]을 기반으로 HM(Health Management) 시나리오에 적합하도록 개발되었다. Simulink Model은 ACM 시스템이 비준과 검증(V&V Verification and Validation)을 구현할 수 있도록 Fault Simulator는 다양한 고장신호를 생성하여 전체 시스템에 주입하도록 구성되어 있다.

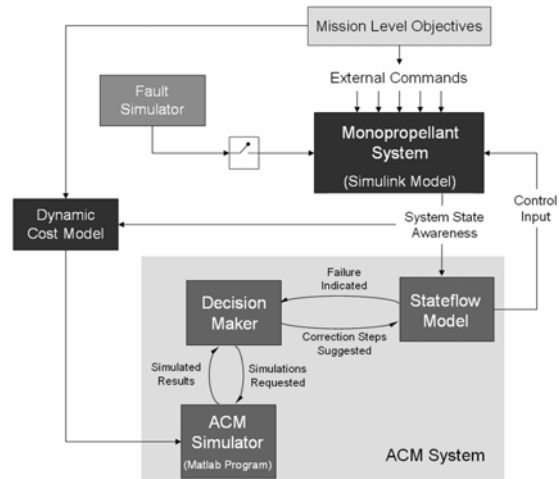


Fig. 3 PACM Test bench using MPS

3.1 Monopropellant Propulsion System(MPS)

본 연구에서 적용한 MPS는 과산화수소(H₂O₂)가 촉매를 통과하여 산소, 물, 그리고 열로 재구성하는 과정을 통하여 원하는 추력을 발생하는 구조로 설계되었다. 이 시스템은 압력 조절기인 RG에 밸브 IV1을 통해 공급하는 비활성 가스의 저장 탱크를 가지고 있다. 그 압력 조절기는 압력 감소를 감지하고 주어진 설정값에서 압력을 유지하기 위하여 밸브를 열거나 닫도록 구성되어 있다. 그 고압가스는 스러스트(thrust) 분리 밸브 IV2와 스러스트 챔버(thruster chamber) 분리 밸브 IV3를 투입경로를 통해 주입된다. MPS가 점화되어 추진력을 갖기 위해서는 일차적으로 밸브 IV1과 IV2가 열려 TK 탱크로부터 고압가스가 분출되어 PT에 압력을 가해 PT 내의 H₂O₂를 투입할 수 있도록 마련된다. 이후 MPS는 보호 장치를 갖추고 난 후에 밸브 IV3를 열고 스러스트 챔버에 들어가기 위해 H₂O₂ 투입을 허용하며, 이때, 고압가스가 촉매를 운반하기 때문에 생산된 산소, 수증기, 열로 분해되게 된다. 뜨겁게 팽창된 가스의 혼합은 스러스트를 차례로 생산하는 스러스트 노즐을 통해 주입되며 추력을 만들게 된다. 하지만, 이 과정에서 밸브 IV2와 IV3사이의 압력이 과도하게 증가하게 되면 밸브 RV1-4를 통하여 비활성가스를 빠져나가 안정된 압력을 조절할 수 있도록 설계되어 있다. Fig. 4는 이상의 MPS의 동작 구조를 나타낸다.

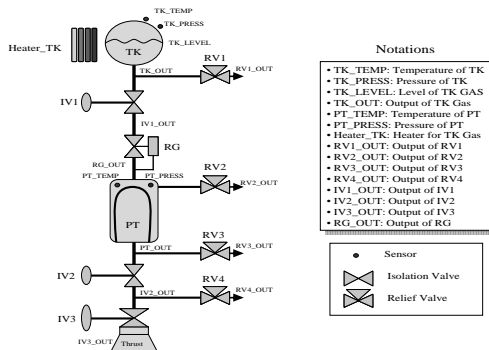


Fig. 4 The monopropellant propulsion system schematic

3.2 Simulink Modeling of Monopropellant Propulsion System

시뮬레이션을 위하여 Fig. 4의 MPS 모델은 ACM을 구현할 수 있도록 범용성과 유연성을 가진

MATLAB의 simulink를 이용하여 시뮬레이션 모델을 구현하였다. 이 모델은 시뮬레이션과 실험을 통하여 설계된 ACM 시스템의 성능을 검증하기 위하여 다음과 같은 세가지 모듈로 구성하였으며, 각 모델과 시뮬레이터 등은 Monopropellant Block, Fault Simulator Block과 Indicator Block등으로 Fig. 5와 같이 구성하였다.

- 시스템 모델: Monopropellant Block
- 가상 고장 시뮬레이터: Fault Simulator Block
- 지시기(주의 및 경보): Indicator Block

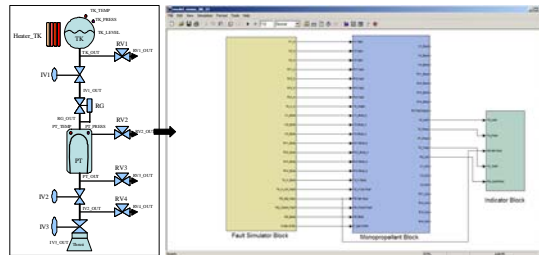


Fig. 5 MPS model using MATLAB Simulink®

시스템 모델은 가상의 추진시스템을 시뮬레이션하기 위한 것으로서 이 모델은 Fig. 6과 같이 다시 탱크 시스템, 탱크를 가열하는 보일러시스템, 압력을 조절하는 압력 조절기 시스템, 그리고 추력을 조절하는 밸브 시스템으로 구성된다.

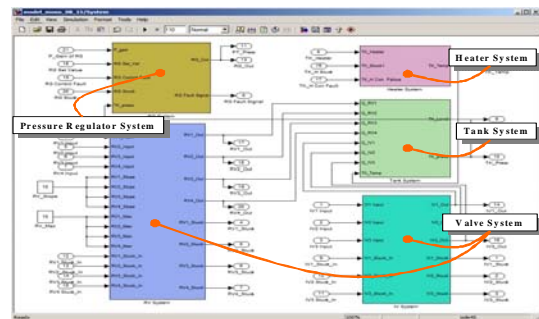


Fig. 6 Monopropellant Block

이 모델에서 사용된 각종 파라미터들은 완전한 시스템의 구성성분의 반응을 변화시킬 수 있도록 손쉽게 수정될 수 있는 구조로 설계 되어졌다. 가상 고장 시뮬레이터는 MPS에 필요한 고장을 생성 투입하여 ACM 시뮬레이션이 가능하도록 하는 역할을 맡고 있다. 지시기는 온도, 압력등과 같은 다양한 센서로부터 얻어진 시스템의 상태를 나타낸다.

Table 3. Assumptions for MPS Simulink® model

Components	Elements	Assumptions	Functional Description
Heater system	TK heater	<ul style="list-style-type: none"> Current(I) = constant Resistance(R) = constant Heat(Q) depends on on/off time t 	
		<ul style="list-style-type: none"> Transfer function is used for temperature system 	
Tank system	<ul style="list-style-type: none"> TK level TK pressure TK temp 	<ul style="list-style-type: none"> Tank volume(V)=constant Tank pressure(P) depends on temperature(T) and number of moles of gas(n) 	
		<ul style="list-style-type: none"> Tank level(L_T) is related to propellant consumption(\dot{n}) by opening of IV3 and RV1-4. Initial Tank level(L_{ini}) =100 	
Regulator system	RG	<ul style="list-style-type: none"> Output gas pressure(P_o) depends on input gas pressure(P_i) and set point(P_{sp}) 	
Valve system	<ul style="list-style-type: none"> IV1-3 RV1-4 	<ul style="list-style-type: none"> Each valve only has simplified as on/off status and the flow(n) depends on on/off time t The flow of gas or propellant (f_c) = constant 	

Simulink로 이상의 시스템을 구현함에 있어 Table 3과 같은 몇몇 추론들이 모델링 작업을 단순화하기 위하여 도입되었다. 시뮬레이션을 위하여 고장발생 모듈을 사용하여 가상의 두 고장상태를 만들었으며, 이때 ACM 시스템은 주어진 고장 상황에 대해 최적의 해를 도출하여 고장 상태를 해결하도록 설계하였다.

3.3 Fault Scenarios

본 연구에서 고려한 MPS상의 두 가지 고장상태로서 조절기의 고장과 가열 시스템의 고장에 대한 두 가지 예상 시나리오를 다음과 같이 고려하였다.

3.3.1 Regulator Failure

일반적으로 시스템이 정상상태일 때에는 조정된 압력(P_{out})이 탱크 내부의 설정 압력값(P_{set})에 추종할 수 있도록 설계되어진다. 하지만, 연료탱크 내부의 압력 P_{in} 이 설정값 이하로 떨어지게 되면 압력 조절기는 원하는 압력을 만들 수 없게 되며, 이때의 출력값은 다음과 같이 나타낼 수 있다.

$$P_{in} > P_{set} \rightarrow P_{out} = P_{set}$$

$$P_{in} < P_{set} \rightarrow P_{out} = P_{in}$$

정상 상태에서 수행이 끝날 때까지 그 가스탱크는 충분한 압력을 제공할 정도의 가스를 포함한다고 가정한다면, Fig. 7에서 보는 바와 같이 P_{in} 은 마지막으로 수행될 때까지 P_{set} 보다 항상 더 커야 한다는 것을 알 수 있다. 조절기의 고장은 임무의 수행 동안 발생할 수 있으며, 이때, 그 조정된 압력 P_{out} 은 낮은 값으로 떨어지게 된다. 여기에서 제안된 고장완화 방법은 조정된 압력을 설계단계 후의 단계에서 설정값을 증가시키는 것이다.

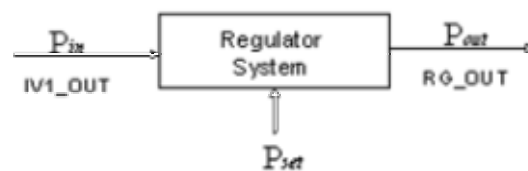


Fig. 7 Schematic of the simulated regulator system

하지만, 조절기 출력압력 저하에 대하여 즉각적인 설정값에 대해 중대한 경제적 비용과 관계가 있다면, 미션의 진행률과 탱크에 남겨진 가스의 잔량 등을 통하여 설정값을 언제, 얼마나 많이 조절해야 하는지에 대한 결정을 내릴 필요가 있을 것이다.

Fig. 8에서 보는 바와 같이 설정값의 증가는 탱크의 가스 압력이 떨어질 때 또 다른 문제를 야기시키게 되며 이때는 레귤레이터가 그 압력조절 기능을 상실하게 될 것이다. 이러한 상황을 극복하기 위하여 ACM 시스템은 탱크의 히터를 가열하는 등 온도와 비활성 가스탱크에서 가스의 압력을 높게 된다. 하지만, 히터를 켜게 되면 그 과정에서 에너지 소비가 증가하게 되므로 불필요한 가열을 최소화하기 위하여 언제 히터를 꺼야 하는지도 결정하여야 한다. 더구나 ACM은 단지 가스압력의 안전단계가 미션을 해결하는 것에 이르게 되었다면 히터를 언제 정지할지도 결정하여야 할 것이다.

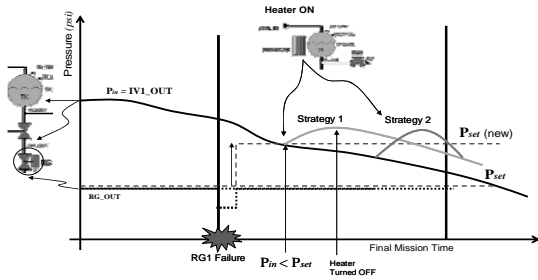


Fig. 8 Simulated regulator failure scenario

3.3.2 Heater Failure

Fig. 9는 조절기 고장에 의해 구동된 히터의 고장 시나리오를 보여준다. 그 고장은 히터가 ACM 시스템에 의하여 꺼지도록 명령 받았을 때 발생한다. 즉, 이때의 탱크압력은 높은 단계인 위험 수위까지 증가하며, 이 상황에서 ACM은 초과된 압력을 낮추기 위하여 리릴프 밸브(RV)의 하나를 열어 해결하게 될 것이다. 일단 여기에서 그 밖의 결정이 RV의 개방을 결정하는 것이라면 언제, 얼마나 길게 개방하는 가도 결정되어야만 한다.

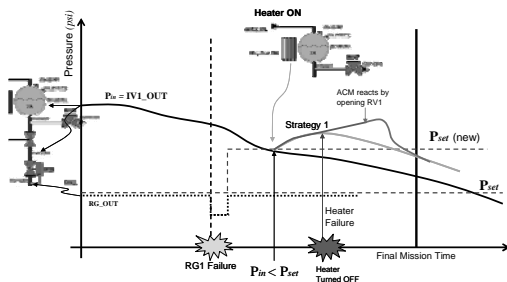


Fig. 9 Simulated heater failure scenario

3.4 Cost Modeling

위의 시나리오에 따른 ACM 적용을 위하여 Fig 10과 같은 cost model을 설정하였다. 이 모델은 모든 값을 계산하는 것에서 두 가지 요소를 가져온다. 장애가 발생할 때마다 이 값들은 차후의 모든 시간 동안 계산되며, 이 동작은 이 값들의 합이 최소가 될 때마다 발생한다. Fig. 10에서 보는 바와 같이 고려된 두 가지 요소는 히터가 "ON"일 때의 시간과 미션을 완료할 때까지 남은 시간의 값으로 구성되어 있다.

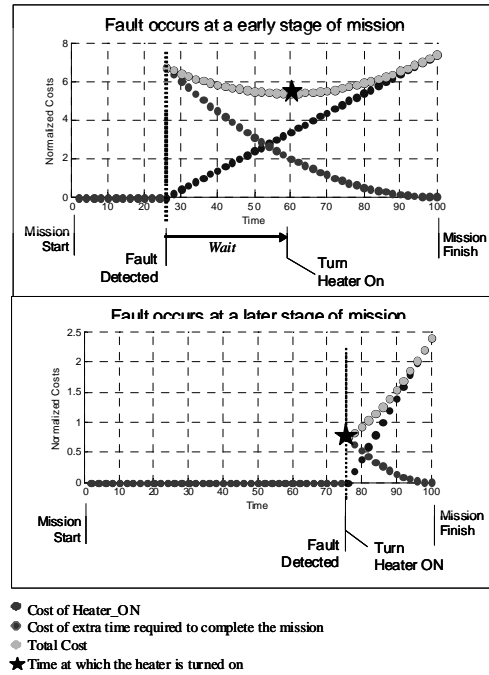


Fig. 10 Costs are dynamically computed and change depending on the current mission stag

고장이 발생한 후에 thrust level은 낮은 압력으로 인해서 원하는 출력을 유지할 수 없게 되며, 미션의 진행 과정은 서서히 늦어져 마지막 단계에는 멈추게 되어 미션을 실패하게 된다. 만약 개정된 동작이 바로 이루어지지 않는다면, 그 미션은 지정된 시간에 완성할 수가 없게 될 것이다. 이러한 수정된 행위는 임의의 비용을 야기시키며, 다음 식의 비용을 최소화 되도록 설계하였다.

$$Total\ Cost = 0.0009 \cdot t_{Heater_ON}^2 + 0.05 \cdot (t_{final} - t_{scheduled})^2 \quad (1)$$

즉, Fig. 10은 두 가지 시나리오가 시스템 수행에서

초기시간에 발생했을 때와 정상상태 단계에서 발생했을 때의 비용을 보여주고 있다. 그림에서 보는 바와 같이 만약 장애가 미션의 후반에서 발생한다면 히터가 즉시 켜져야 되는 것에 반하여 만약 그 장애가 미션의 전반부에서 발생한다면 그 히터는 즉시 꺼질 필요는 없을 것이다. 이러한 결정은 히터를 켤 때의 비용과 미션을 완료하는데 요구되는 잔류시간에 대한 비용 두 가지를 고려하여 총비용이 최소가 되는 방향으로 결정될 때의 이루어지는 결과이다.

3.5 ACM Model

MPS의 고장시 이를 감지 제어하는 ACM model은 Matlab Stateflow toolbox를 사용하여 개발하였다. Fig. 11은 위에 묘사된 고장 시나리오에 대한 신호흐름 선도를 보여준다. 시스템의 상태가 정상모드에서 고장모드로 바뀔 때마다 그에 해당되는 비용은 계산되며, 이때 그 비용이 최소가 되는 방향으로 시스템이 동작되도록 구성되어 있다. 이 Stateflow 모델은 직접 그 시스템의 상태에 접근하는 Simulink Model과 상호작용할 수 있도록 설계가 되어있다. 압력, 온도, 임무수행의 정도, 연료등급 등과 같은 변수들은 연속적으로 모니터링되며, 어떤 요소가 정상상태를 벗어나자마자 시스템의 운전은 이들 불규칙한 동작들이 충분히 개선될 때까지 이루어진다.

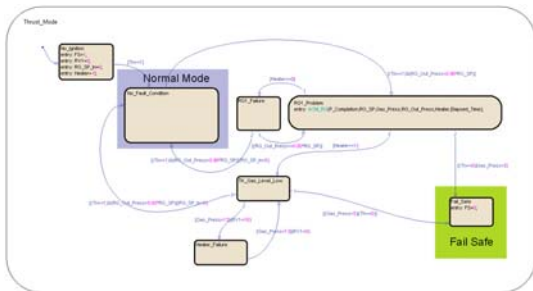


Fig. 11 ACM model in State flow

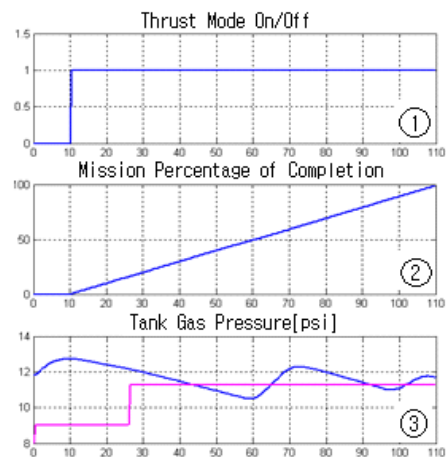
IV. 시뮬레이션 결과

설계된 ACM 시스템의 유효성을 검증하기 위하여 3가지 시나리오를 설정하여 시뮬레이션을 수행하였다. 첫 번째 시나리오는 스러스트의 동작 중에 압력 조절밸브(RG)의 고장에 따른 회복 동작특성을 시뮬레이션 하였으며, 두 번째 시나리오는 역시 스러스트의 동작 중 압력조절밸브(RG) 고장이 전단부 및 후단부에서 연속적으로 야기된 경우의 고장회복 특성

을 시뮬레이션 하였고, 마지막 시나리오는 압력조절밸브(RG)의 고장이후에 발생하는 히터의 잇다른 고장에 대한 시나리오 상의 시스템 성능평가를 시뮬레이션 하였다.

4.1 Scenario 1

Fig. 12는 첫 번째 시뮬레이션 시나리오에 대한 시스템에서 발생하는 변화를 나타내었다. 그 중 첫 번째 그림은 시스템이 추진되어 thrust 모드가 시간 $t=10[\text{sec}]$ 에서 동작됨을 보여준다. 미션이 진행되는 과정은 두 번째 그림에 나타나 있으며, 세 번째 그림은 thrust가 동작됨에 따라 탱크내부의 압력이 떨어지는 상태를 보여주고 있다. Fig. 12의 4번째 그림은 조절기 고장이 시간 $t=26[\text{sec}]$ 에서 발생되어 그 압력이 떨어짐을 보여주고 있다. Fig. 12의 나머지 두 그림은 각각 탱크내의 가스 온도와 레벨을 각각 나타내고 있다. 이때 ACM 시스템은 Fig. 12의 3번째 그림에서 보는 바와 같이 압력이 $11.5[\text{psi}]$ 에서 $9[\text{psi}]$ 로 떨어질 때 $t=27[\text{sec}]$ 에서 즉각적으로 반응을 함을 볼 수 있다. 이때의 조정 압력이 정확함을 확인할 수 있었다. 약 $t=42[\text{sec}]$ 부근에서 가스 압력은 새로운 설정값 주변으로 떨어지며, 조정된 압력은 다시 떨어지기 시작한다. 이때, ACM 시스템은 $t=59[\text{sec}]$ 부근에서 압력을 증가시키기 위하여 히터 가열을 시작하게 된다. 이렇게 가열되던 히터는 일정 압력이상에 도달하게 되면 $t=69[\text{sec}]$ 부근에서 다시 가열을 멈추게 된다. 하지만, $t=92[\text{sec}]$ 에서 그 압력은 다시 떨어지게 되고 히터는 $t=94[\text{sec}]$ 에서 다시 가동이 되며, 이러한 과정은 압력조절을 위하여 계속적으로 반복될 수 있을 것이다. 이 시뮬레이션 시나리오는 고장이 발생되었을 때 미션 레벨에 따라서 ACM 시스템의 결정은 사전에 정의된 비용함수에 따라 변화되어지게 된다.



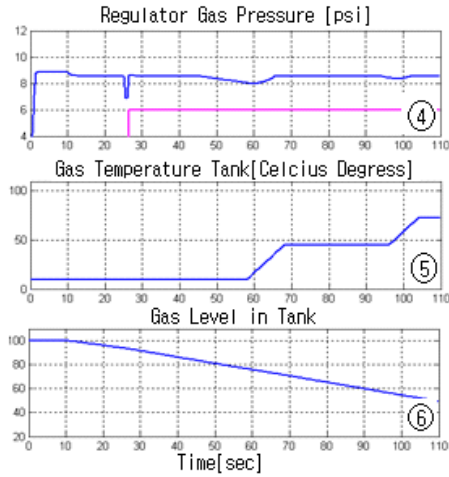


Fig. 12 Regulator fault scenario simulation

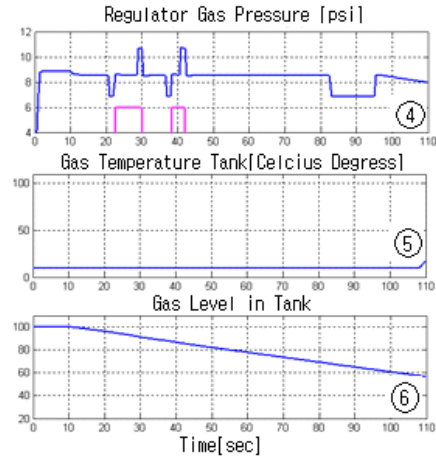
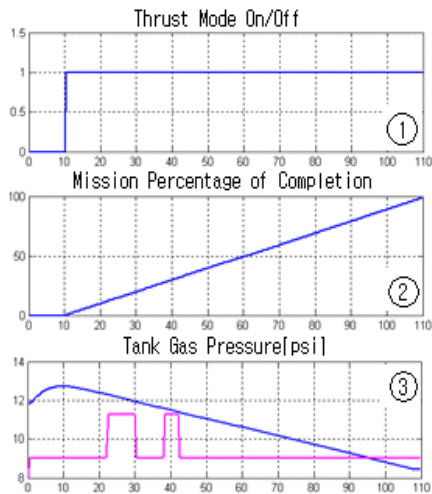


Fig. 13 ACM continuously monitors the system

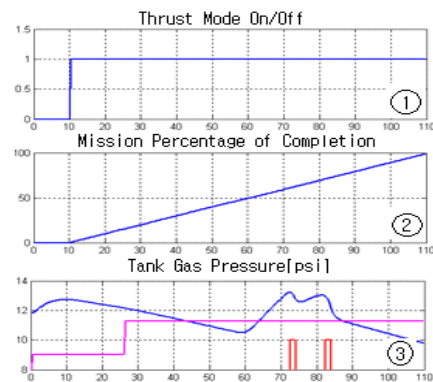
4.2 Scenario 2

두 번째 시뮬레이션은 ACM이 연속적으로 시스템을 모니터링하면서 고장발생시에 즉각적으로 이에 반응하는 것을 보여주고 있다. 만약 고장이 미션의 후단부에서 발생이 되었다면 정확한 교정을 통한 시스템 운전의 어려움이 예상되며, 미션을 완수하는데 소요되는 여분의 시간에 대한 비용이 상대적으로 증가하게 될 것이다. 두 번째의 경우는 주로 소량의 임무만이 중단에서 수행되기 때문에 정상동작시의 비용과 비교했을 때 시스템 성능을 저하시킬 수 있는 다소 추가시간이 필요하게 된다.



4.3 Scenario 3

이 절에서는 조절기 고장 이후에 발생하는 히터의 잇다른 고장에 대한 시나리오 상에서 시스템의 성능 평가를 시뮬레이션하였다. 시뮬레이션 결과에서 예상 출력으로는 탱크 내에서의 온도와 압력의 상승을 들 수 있다. Fig. 14의 3번째 그림에서 볼 수 있듯이 시간 $t=69[sec]$ 에서 히터 고장으로 온도가 급격히 지속적으로 증가함이 발생되는 것을 알 수 있으며, 이는 ACM에 의하여 심각한 고장상태로 인식될 것이다. 그 결과 ACM은 시간 $t=72[sec]$ 부근에서 릴리프밸브 RV1을 약 1초간 열면서 반응을 시작한다. 이와 관련된 결과는 6번째 그림에 나타나 있는 바와 같이 가스의 레벨이 감소하여 안정된 상태를 추구하고 있음을 확인할 수 있다. 이때, 시스템의 온도는 여전히 증가하고 있기 때문에, 탱크내부의 압력은 안전한 레벨까지 떨어지며, 시간 $t=82[sec]$ 부근에서 RV1은 다시 열려 약간의 가스압력을 조절하게 된다.



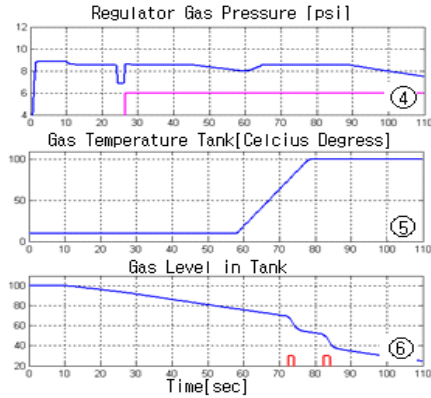


Fig. 14 Regulator and heater faults in succession scenario

V. ACM Validation

비록 ACM 시스템이 주어진 고장 시나리오에 대하여 최적으로 수행되기 위하여 설계되었다 하더라도 4장에서 보여진 결과들은 최적이라고 단정하기 어렵다. 즉, 이런 문제점을 해결하기 위해 우선 타당성 과정을 거치게 되는데 이 때 고장이 발생한 시간을 무작위로 추출하여 최적화된 ACM 시스템의 성능과 비교하게 된다.

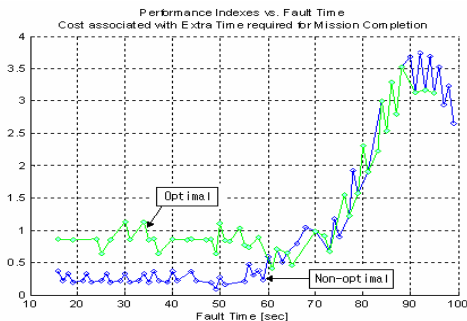


Fig. 15 Cost of extra time, given a failure in the pressure regulator

Fig. 15는 미션을 정상적으로 마무리하기 위한 여분의 시간에 대한 비용의 결과를 나타내고 있다. 그림에서 보는 바와 같이 즉, 이는 두 ACM 시스템은 압력 조절 실패에 대한 효과를 완화시키는 것이 가능하였음을 나타낸다. 최적 contingency 전략인 히터

의 사용과 여분의 시간에 대한 평균 비용을 유지함으로써 전자와 연관된 비용은 높게 기대될 것이다. 이는 최적전략에 대한 효과가 미션의 초기에 출현한 고장에 대해서도 충분히 작용할 수 있다는 것을 의미한다.

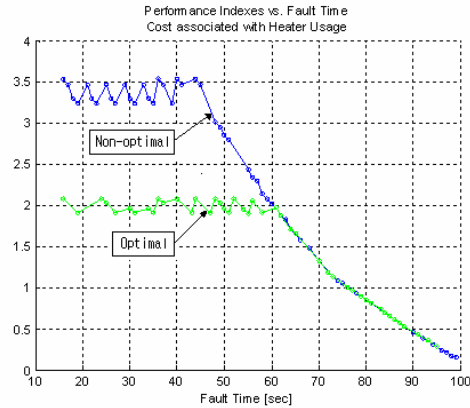


Fig. 16 Cost associated with heater usage, given a failure in the pressure regulator

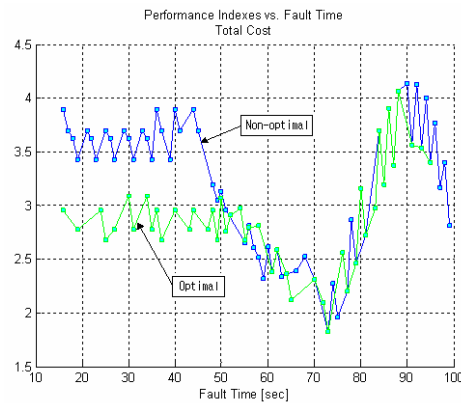


Fig. 17 Total cost, given a failure in the pressure regulator

Fig. 16은 히터 사용 비용에 대한 비준결과를 보여준다. 이로부터 최적의 경로가 충분한 에너지를 절약하면서 동일한 시간 내에서 근사적으로 미션을 성공적으로 마무리 가능함을 확인할 수 있다. 최종결과로부터 알 수 있듯이 Fig. 17은 최적화되지 않은 ACM과 최적화된 ACM 시스템의 전체 비용에 대한 비교를 보여주고 있으며, 이는 비준의 결과가 최적화 루틴이 원래의 목적을 제대로 수행하고 있음을 의미한다.

VI. 결 론

본 논문에서는 개발에 필요한 일반적인 프로토타입 테스터 벤치 소프트웨어와 PACM(Propulsion Automated Contingency Management)이라 불리는 개선된 추진 시스템을 위한 기준을 포함하는 ACM 시스템을 제안하였다. 제안한 알고리즘에 대한 검증 을 위하여 설계된 ACM 시스템은 MPS에 적용하였으며, 그 결과 ACM 시스템은 최적의 완화 전략의 탐색과 미션 단계에 대한 시간에 따라 변화하는 전략에 의하여 고장을 효과적으로 완화시키는 것을 확인할 수 있었다. 본 연구에서는 이러한 시스템 개발에 적합한 일반적인 해결방안을 기술하였으며, 앞서 언급한 몇몇 예제를 통하여 검증이 되었다고 사료된다. 뿐만 아니라 이러한 시스템에 대한 기준의 개념이 관련 예제를 통하여 도입이 되었으며, 이상의 ACM 설계 메카니즘은 항공기를 비롯한 각종 플랜트 제어 및 운영에 응용될 수 있을 것으로 기대된다.

후 기

본 연구는 한국과학기술부(MOST) 지정 국가지정연구실사업(NRL)의 지원과 2005년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원과 을 받아 수행된 연구임.(KRF-2005-214-과제번호)

참고문헌

- [1] I. Tumer, and A. Bajwa, "A Survey of Aircraft Engine Health Monitoring Systems", *35th Joint Propulsion Conference; June 1999; AIAA-99-2528*.
- [2] Liang L. Tang, Gregory G. J. Kacprzynski, Michael M. J. Roemer, GeorgeVachtsevanos G. Vachtsevanos, and Ann A. Patterson-Hine, "Automated Contingency Management Design for Advanced Propulsion Systems", *infotech@Aerospace*, Arlington, Virginia, pp. 26 - 29 September 2005.
- [3] C. S. Byington, M. Watson, M. J. Roemer, T. R. Galie, and J. J. McGroarty, "Prognostic enhancements to gas turbine diagnostic systems," *IEEE Aerospace Conference*, pp. 3247-3255, 2003 3247 - 3255
- [4] C. Boller, "Next generation structural health monitoring and its integration into aircraft design," *Int. J. of Systems Science*, vol. 31, no. 11, pp. 1333-1349, 2000.
- [5] G. Jianhua M. J. Roemer, and G. Vachtsevanos, "An automated contingency management simulation environment for integrated health management and control", *Proc. of the IEEE Aerospace Conference*, pp. 3725-3732, 2004.
- [6] J. C. Laprie, *Dependability: Basic Concepts and Terminology*, Vienna, Springer-Verlag, 1992.
- [7] W. L. Heimerdinger, and C. B. Weinstock, "A conceptual framework for system fault tolerance", *CML/SEI-92-TR-33*, Software Engineering Institute, Carnegie Mellon University, 1992.
- [8] P. C. William and P. P. Nayak, "A Model-based Approach to Reactive Self-configuring systems". *Workshop on Logic-Based Artificial Intelligence*, Washington, DC, June, 1999
- [9] A. J. Bateman, C. R. Elks, D. G. Ward, and J. D. Schierman, "New Verification and Validation Methods for Guidance- Control of Advanced Autonomous Systems", *AIAA 2005-7117*, Arlington, VA, September 2005,
- [10] W. Vesely, M. Stamatelatos, J. Dugan, J. Fragola, J. Minarick, and Railsback, *Fault tree handbook with aerospace applications*, 2002.