항공용 임베디드 시스템 하드웨어 신뢰성 평가

Reliability Evaluation for the Avionic Embedded System

김병영*, 이동우*, 나종화*

Byeong-Young Kim*, Dong-Woo Lee* and Jong-Wha Na*

요 약

항공관제시스템은 안전하고 신뢰할 수 있는 공항 운영을 위해 절대적으로 높은 신뢰성이 요구된다. 본 연구에서는 서버 워크스테이션과 네트워크를 포함하는 ATM 하드웨어 시스템의 신뢰성을 분석하였다. 구체적으로 하드웨어 신뢰성 평가에 자주 사용되는 신뢰도 불록도(Reliability Block Diagram)와 고장수목분석법(Fault Tree Analysis)을 이용하여 분석하였다. 분석 실험은 Relex 사의 Reliability Studio를 이용하여 ATM 하드웨어 시스템의 신뢰도를 예측하였다.

Abstract

Air Traffic Management (ATM) system requires extremely high reliability for the safe and dependable operations in the airport. This paper reports a study on the reliability of the prototype ATM hardware system including the servers and local area networks. Reliability Block Diagram and Fault Tree Analysis on the prototype ATM hardware were performed.

Key words : Air Traffic Management, Avionic Embedded System

I. 서 론

항공관제시스템 (Air Traffic Management System)은 항공기의 이착륙 및 비행관리, 감시 등의 업무를 수행하는 공항운용의 핵심적 시스템이다. 따라서 항공관제시스템(이후 ATM)의 높은 신뢰성 및 가용성은 공항 운용의 절대적 요구사항이다. 시스템의 신뢰성을 평가하는 방법은 일반적으로 목표 시스템의 신뢰도를 설정하고, 그에 따라서 하드웨어 및 소프트웨어를 설계한다. 하드웨어의 신뢰도 목표 설정은 TMR(Triple Modular Redundancy) 또는 DMR(Dual Modular Redundancy)을 적용하여 시스템을 설계한다. 이때 DMR 혹은 TMR 구조를 이용하여 설계된 ATM의 신뢰도가 설계의 신뢰도 요구사항 (Reliability Requirement)을 만족하는지 검증하는 절차가 필요하다.

일반적으로 주어진 시스템의 목표 신뢰도를 측정하기 위하여 다음과 같은 방법들을 사용한다. (1)부품 카운트 법, (2)신뢰도 블록도법 (Reliability Block Diagram), (3)고장수목분석법 (Fault Tree Analysis), (4)상태천이도 분석법, (5)페트리 넷 분석법 등이다 [1]. 위의 검증 기법을 이용하여 ATM이 목표하는 신뢰도 수치를 만족하는지 분석하여 설계할 수 있다.

본 논문은 제안된 ATM의 신뢰도를 측정하기 위

* 한국항공대학교 항공전자공학과(School of Electronics Engineering, Korea Aerospace University)
· 제1저자 (First Author) : 김병영
· 투고일자 : 2008년 11월 28일
· 심사(수정)일자 : 2008년 12월 1일 (수정일자 : 2009년 1월 14일)
· 게재일자 : 2009년 2월 28일

하여 신뢰도 블록도 기법과 고장수목분석법 을 사용하였다. 신뢰도 계산과정은 수많은 개별 부품들의 신뢰도 값들이 연산에 적용되기 때문에 정확한 신뢰도를 측정하려면 상용 도구를 활용하는 것이 필요하다. 본 연구에서는 RELEX사의 RELEX Reliability Studio를 이용하여 제안된 ATM 시스템의 신뢰도를 산출하였다.

Ⅱ. Prototype 항공 관제 시스템

항공관제(Air Traffic Management)는 좁게는 항공교통 제어에서 크게는 공역 관리까지 아우르며, 항공관제는 크게 3가지로 분류된다. 첫째는 교통 흐름 관리(Traffic Flow Management)로서 공항 터미널 및 공항의 운송 용량을 관리한다. 둘째는 항공 교통 제어(Air Traffic Control)로서 항공기의 이착륙 및 항공기와 지상간의 통신 네트워크를 제어한다. 셋째는 공역관리(Airspace Management)로서 공항 터미널 및 해양에 대한 영토를 관리하고 확보하는 역할을 담당한다. 이러한 항공관제정보는 ATM으로 보내지고 중앙에서 항공관제의 모든 사항을 제어한다. [2].

본 연구에서 사용한 ATM 시스템의 블럭도는 그림 1에 도시되어 있다 [3]. ATM은 다음과 같은 구성요소들을 가지고 있다. (1) 감시시스템 센서, 비행자료 센서, 그리고 비행자료 터미널로 구성된 센서부, (2) 감시자료 처리시스템, 비행자료처리시스템, 현시시스템, TRS시스템 등 자료처리시스템, 그리고 (3) LAN의 세 개의 주요 블록으로 구성된다. 또한 ATM에 대한 안정성의 요구에 대응하여 외부 인터페이스 처리 시스템, 감시자료 처리시스템, 비행자료 처리시스템, TRS시스템, LAN, 녹화/재생 시스템에 다중 모듈을 추가하였다. 다중화 시스템은 시스템의 고장 발생 시 대기 중인 모듈이 현재 모듈을 실시간으로 대신함으로 시스템의 안정성을 증가시킨다.

Ⅲ. ATM 신뢰도 예측

3-1 서버모델의 신뢰성 평가

본 절에서는 ATM 시스템의 신뢰도 관련 특성인 Reliability Block Diagram (RBD)와 Fault Tree Analysis (FTA)를 이용하여 Failure Rate, Reliability,

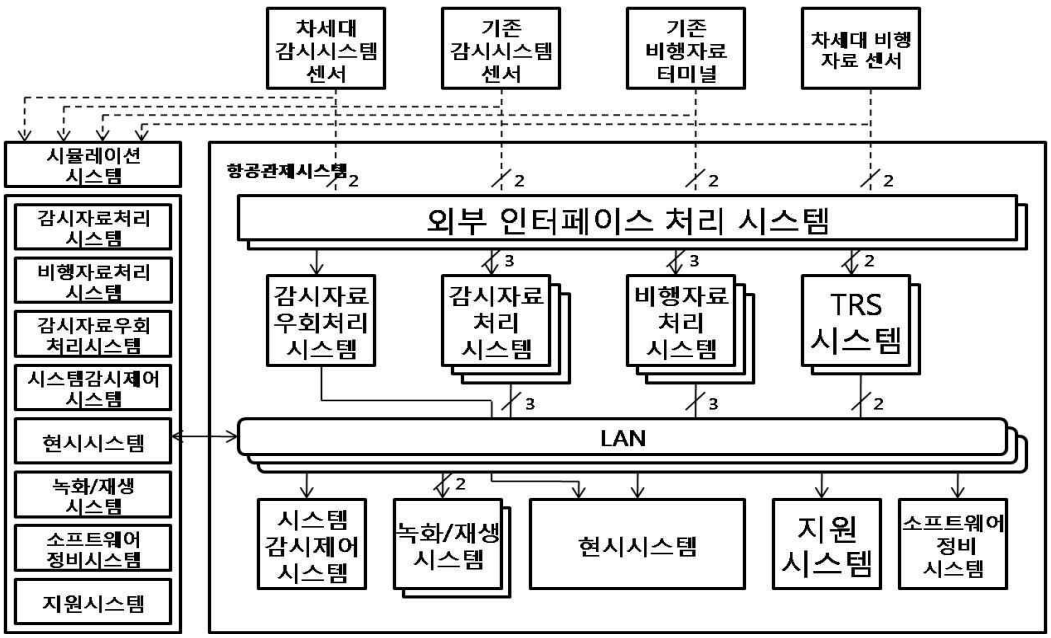

그림 1. 항공관제시스템 블록도
figure 1. Block diagram of ATM

Availability, MTBF (Mean Time Between Failure), Total downtime 등의 신뢰성 성능을 평가한다. RBD 와 FTA에 관련된 상세한 설명은 Ref [1]을 참고하기 바란다. 정확한 분석 자료를 도출하기 위하여 신뢰성 관련 도구로 유명한 RELEX사의 RELEX Reliability Studio를 이용하여 ATM시스템의 모델을 설계하고, 설계된 모델의 신뢰도, 실패율, 평균수명과 같은 신뢰성 변수를 도출하였다.

우선 그림1의 prototype ATM 시스템을 기준으로 하여 각 모듈 및 모듈의 구성 부품들의 신뢰도 모델을 개발하였으며, 그 모델을 기반으로 RBD와 FTA를 수행하여 제시된 ATM 시스템의 신뢰성을 분석하였다. 그림에서 ATM 시스템을 구성하는 여러 서브 모듈에 대한 RBD 및 FTA 모델을 개발하고, 최종적으로 최상위 모델인 prototype ATM 모델의 신뢰도를 산출하였다. 그림에서 각 서브 모듈 시스템의 하드웨어는 서버 시스템을 의미하며 서브 모듈간의 네트워크는 근거리 통신망 (LAN)을 의미한다.

주어진 시스템에 대한 정확한 신뢰도를 산출하기 위해서는 하드웨어, 소프트웨어의 분석뿐만 아니라 운영환경, 시스템 사용자의 숙련도, 사후관리 계획 등의 시스템에 관련된 모든 제반 요소들, 즉 설계단계에서 운영관리 전 분야에서 사용되는 모든 요소들이 평가에 고려되어야 한다. 그러나 이러한 평가모델은 너무 광범위하므로 본 연구에서는 1차적으로 하드웨어 측면에 대해서만 평가된 결과를 보고한다.

실제 서버 하드웨어의 메인보드의 부품 목록을 이용하여 보드에서 사용되는 각각의 IC, 저항, 콘덴서, 소켓 등의 부품의 부품 리스트를 찾아서 부품번호를 정리하여 Relex에 입력한다. 부품의 신뢰도는 다음 절에 설명되어 있다. Relex에 입력되는 사항은 부품번호, 카테고리, 기준설명, 부품의 개수를 입력하며, 시스템은 신뢰도 데이터베이스에서 단위 고장률 및 전체 고장율을 출력한다. 64비트 마이크로프로세서

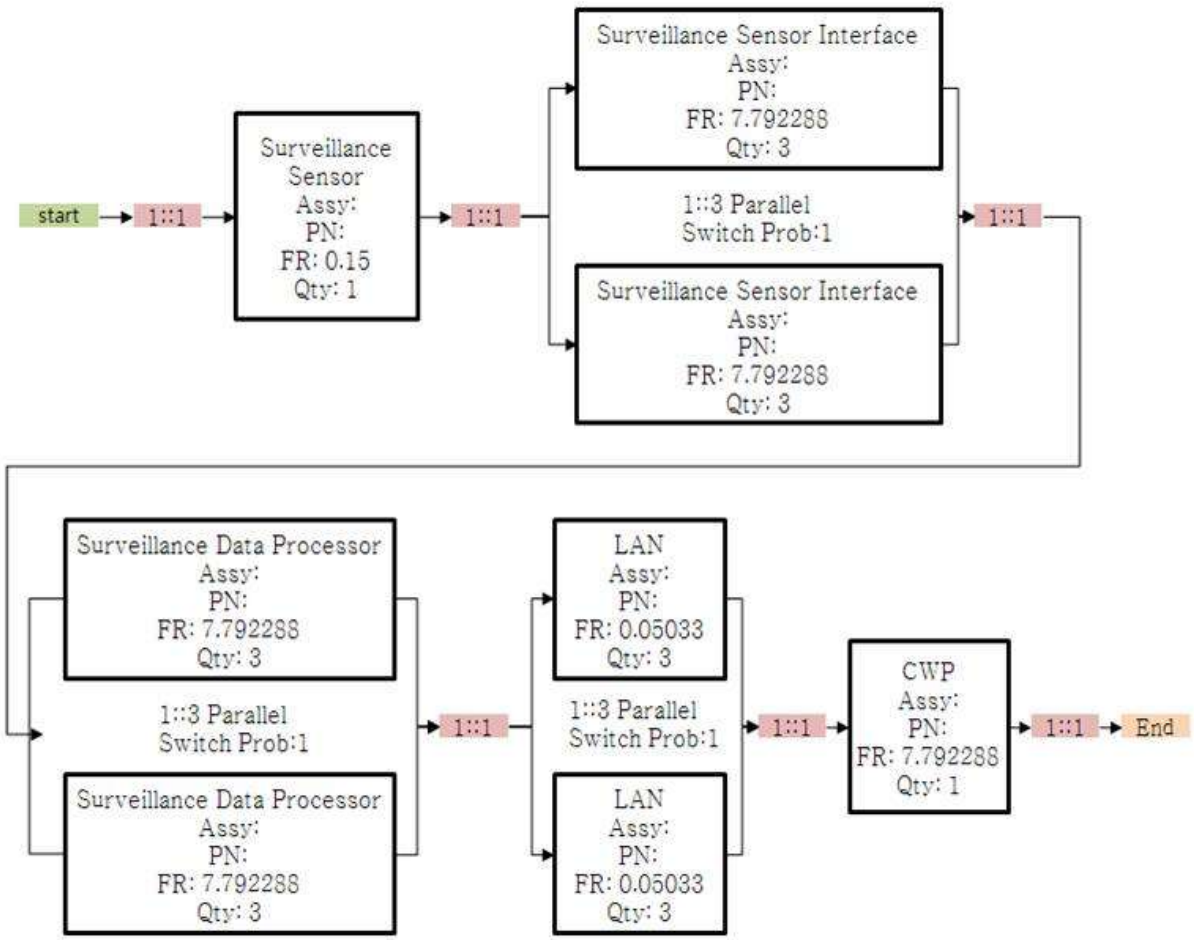

그림 2. 감시자료 처리시스템의 Reliability 블록도
figure 2. Relliability block diagram of SDP

의 경우 79RV4600 부품을 이용하였으며, 이 부품의 고장률은 1.189164 FIT 그리고 MTBF는 840,924 시간의 값을 갖는다. FIT 는 Fault in Time 의 약자로서 100만 시간 동안에 발생하는 오류의 수(MIL-HDBK 기준) 를 의미한다. 이러한 방법으로 서버의 모든 부품들의 고장률 및 MTBF를 구하였으며 이를 이용하여 서버 모델의 신뢰도를 측정하였다. 계속적인 분석작업의 수행을 통해 각 파트들의 신뢰도, 실패율과 수명, 뿐만 아니라 이러한 부품들로 이루어진 서버 모델의 신뢰도를 평가하였다. 분석결과 서버모델의 Failure Rate는 7.792288, MTBF는 123,332 hrs의 결과가 나왔으며, 동일한 절차에 의해 평가한 근거리 통신망 환경은 Failure Rate 0.050330, MTBF 19,868,726 hrs의 결과를 도출 하였다. 이러한 결과는 실온 30도에서 운용할 경우, 서버의 신뢰도의 정량적인 수치를 산출한 결과로서 운용 온도의 변경 또는 서버 또는 LAN 환경의 part list의 변경에 따라 변경 될 수 있다.

3-2 부품 신뢰도 데이터

ATM의 여러 서브 모듈들의 신뢰도를 예측하려면 각 서브 모듈의 부품들의 신뢰도가 필요하다. 이 부품들의 신뢰도 데이터 값들은 여러 가지 자료에서 구할 수 있다. 먼저 가장 널리 사용되는 자료는 MIL-HDBK -217이다 [4]. 이는 전자 장비의 신뢰도 예측을 위한 핸드북으로서 Rome 연구소와 신뢰도 분석센터 (Reliability Analysis Center)의 연구를 기반으로 미 국방성에서 편찬하였다. 신뢰도 예측을 위한 또 다른 방법은 Bellcore의 TR-332[5]이다. Bellcore는 벨 통신 연구소의 이름을 인용한 것으로서 이전에는 신뢰성 예측을 위해 MIL-HDBK-217을 많이 사용하였으나, 1985년 그들의 현장 경험을 보다 더 잘 반영시키기 위해 모델을 수정하였고, 상업적인 전자 제품들에 보다 더 응용 적절한 Bellcore 신뢰도 예측 절차를 개발하였다. 이 밖에도 HRD[6](영국), Siemens[7](독일), NIT[8](일본), Italtel[9](이탈리아), CNET[10]

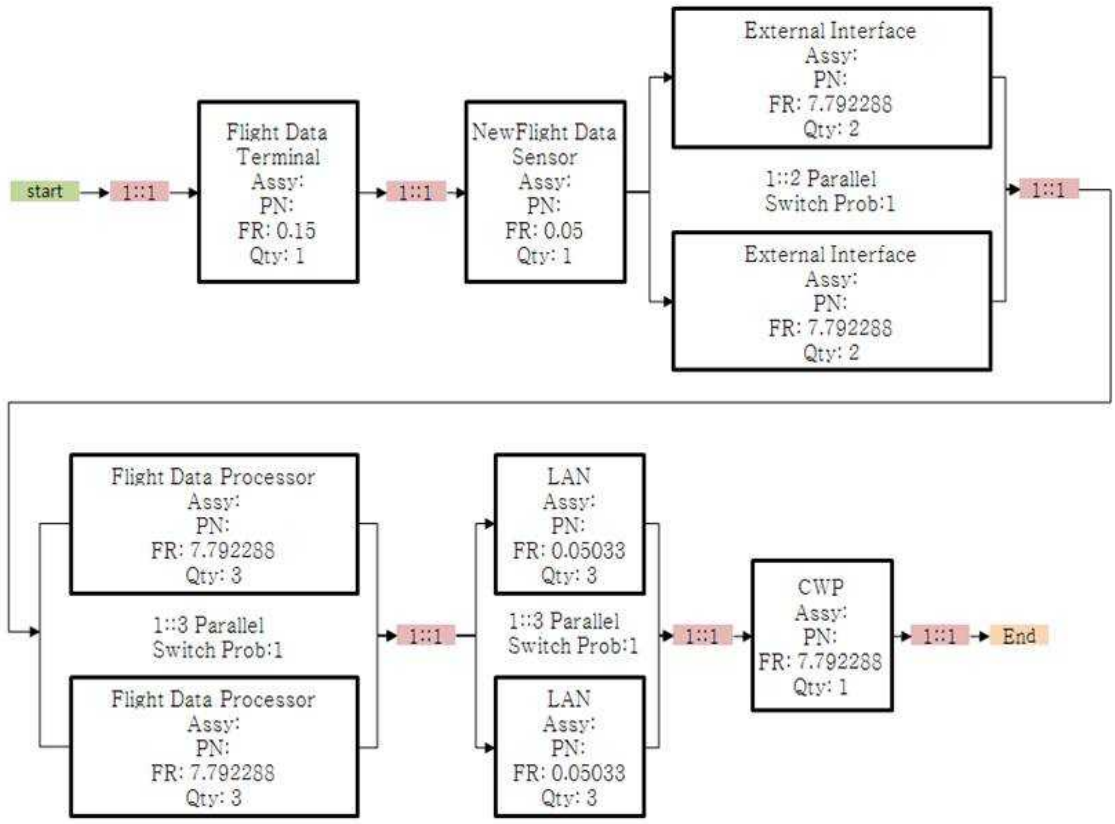

그림 3. 비행자료 처리시스템의 Reliability 블록도
figure 3. Reliability block diagram of FDP

(프랑스) 등의 신뢰도 예측 방법들이 있고 각 나라마다 그들에게 맞는 방법을 적용하고 있다.

본 논문에서는 ATM 시스템의 부품들이 MIL 규격에 준하는 신뢰도를 요구하므로 MIL-HDBK-217을 이용하여 ATM 시스템을 설계하였고 신뢰도 블록도법 및 고장수목분석법을 이용하여 고장율을 예측하였다.

3-3 Reliability Block Diagram

3-3-1 감시자료 처리시스템 Reliability Block Diagram

그림 1의 Prototype ATM에서 감시자료 처리시스템 (Surveillance Data Processing or SDP)의 동작은 감시센서의 데이터가 감시자료 처리시스템을 지나서 최종적으로 현시시스템으로 전달되는 과정으로 구성된다. 이와 같은 과정은 그림 2에 RBD으로 표현 하였다. 단일의 감시 시스템 센서인 Surveillance Sensor와, TMR로 구성된 외부 인터페이스 처리 시스템 (Surveillance Sensor Interface or SIF), 감시자료 처리시스템, 근거리 통신망 시스템, 그리고 단일의 현시시스템 (Controller Working Position or CWP)를 직렬로 연결하였다. 각각의 서브 시스템에는 failure rate 값을 입력해야 한다. 감시자료 처리시스템의 RBD는 앞절에서 제시한 서버 모듈과 근거리 통신망 의 failure rate값을 적용하였다. 즉 SIF, SDP, CWP는 서버 모듈의 failure rate인 7.792288FIT을 적용하였고, 근거리 통신망은 0.050330FIT을 적용하였다. Surveillance Sensor는 분석된 자료가 없어, 임시로 failure rate값 0.15FIT을 적용 하였다. 분석 결과를 통해 시간에 따

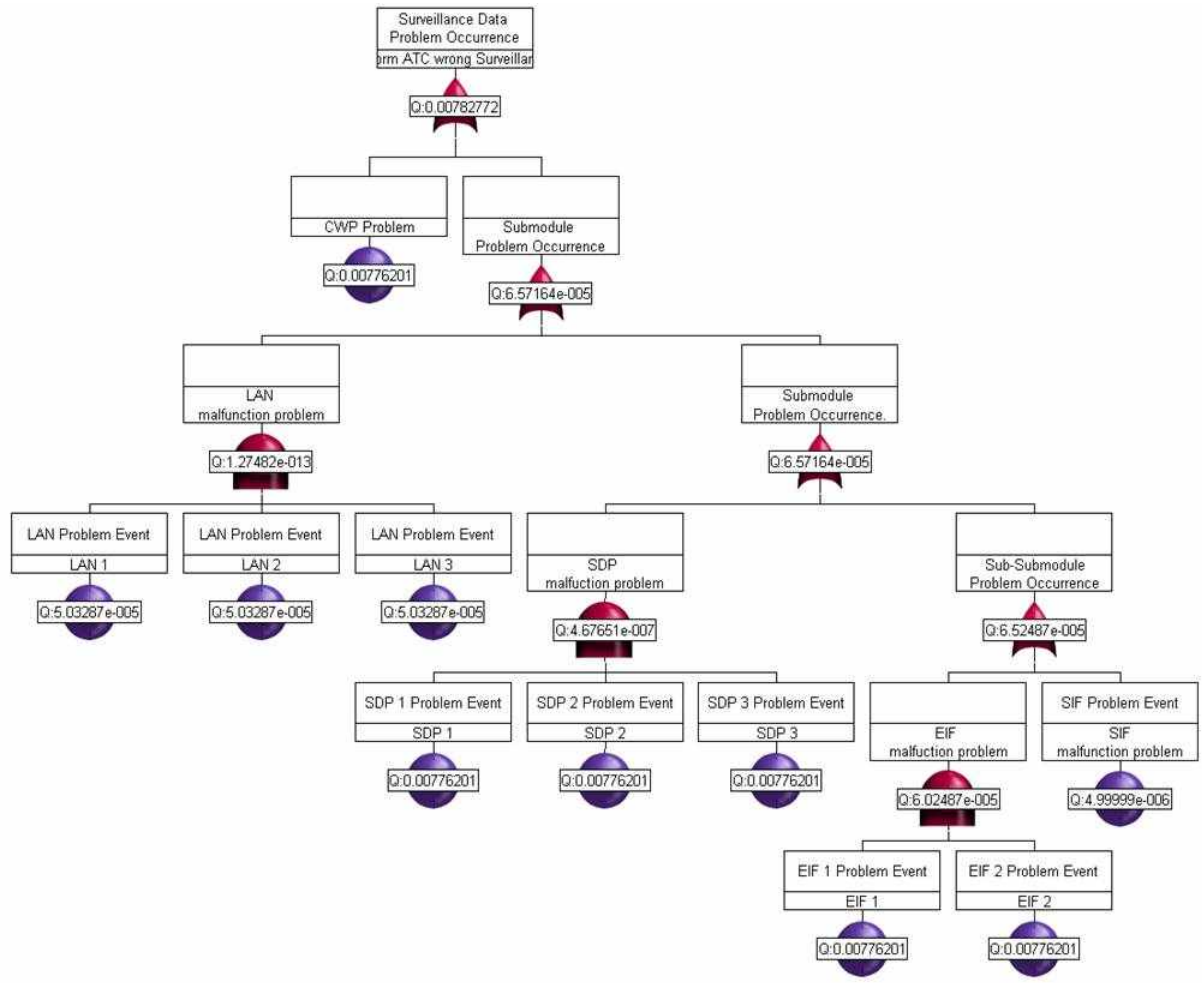

그림 4. 감시자료 처리시스템의 Fault Tree Analysis
figure 4. Fault Tree Analysis of SDP

른 시스템의 Reliability, Availability, Failure Rate, Total Downtime등을 알 수 있다. 모델을 개발하고 실험을 수행한 결과 값은 다음과 같다. 감시자료 처리시스템의 RBD의 경우 1000시간 사용기준으로 Reliability 0.992088, Availability 0.988000, Failure Rate 7.945083, Total Downtime 3.960884의 결과 값을 확인 하였다.

3-3-2 비행자료 처리시스템 Reliability Block Diagram

그림 1의 Prototype ATM에서 비행자료 처리시스템의 동작은 비행자료 터미널의 데이터가 비행자료 처리시스템을 지나서 최종적으로 현시시스템으로 전달되는 과정으로 구성된다. 그 과정을 그림 3에 RBD로 모델을 설계하였다. 그림 3의 모델은 Flight Data Terminal과 New Flight Data Sensor, 이중 구조의 External Interface (EIF), TMR 구조의 Flight Data Processor (FDP), 근거리 통신망과 단일이 현시 시스템 (CWP)을 직렬 연결하여 구성하였다. 비행자료 처리시스템의 RBD는 앞서 제시한 서버 모듈과 근거리 통신망의 failure rate값을 적용한다. 즉 EIF, FDP, CWP는 서버 모듈의 failure rate인 7.792288FIT을 적용하였고, 근거리 통신망은 0.050330FIT을 적용하였다. Flight Data Terminal과 New Flight Data Sensor는 관련된 자료가 없는 관계로 임시 Failure rate 값을 각각 0.15FIT, 0.05FIT 적용 하였다. 분석 결과를 통해 시간에 따른 시스템의 Reliability, Availability, Failure Rate, Total Downtime등을 알 수 있다. 본 절에서 제시한 비행처리시스템의 RBD의 경우 1000시간 사용기준으로 Reliability 0.991979, Availability 0.994000, Failure Rate 8.113721, Total Downtime 4.005637의 결과 값을 확인 할 수 있다.

3-4 Fault Tree Analysis

3-4-1 감시자료 처리시스템 Fault Tree Analysis

감시자료 처리시스템 (SDP) 의 고장형태를 분석하기 위해 FTA를 설계하였으며, 이는 그림 4에 도식되어 있다. FTA의 Top Event는 ATC가 관제를 수행할 때 오류가 발생할 수 있는 상황을 고려하여 ATM시스템에서 CWP로 잘못된 감시 정보가 전달되는 이벤트를 결정하였으며, 이 이벤트를 기준으로 FTA 분석을 수행하였다. 그림1의 prototype ATM 블록도를 기반으로, 앞서 설명한 FTA분석절차에 따라 고장 수목을 설계하였다.

그림 1의 시스템을 분석하면 잘못된 감시정보가 ATC에게 전달 될 경우, 현시 시스템 자체의 문제 또는 현시 시스템으로 전달된 데이터의 문제를 예상 할 수 있다. 따라서 Top event는 현시 시스템의 문제와 잘못된 데이터의 전달 사건을 OR 게이트로 연결하였다. 현시 시스템의 실패는 앞서 제시한 서버모듈의 failure rate 값인 7.792288을 적용한다. 잘못된 데이터의 전달 사건은 다음의 2가지 경우로 나누어 생각 할 수 있다. 첫 번째는 데이터 경로상의 문제, 또는 SDP에서 잘못된 연산을 수행한 경우 이다. 따라서 잘못된 데이터의 전달 사건은 OR 게이트로 표현한다. 데이터 경로상의 문제는 근거리 통신망의 failure rate인 0.050330을 적용한다. 단 근거리 통신망의 경우 TMR 구조로 되어 있으므로, 3개의 근거리 통신망이 모두 failure가 된다. 따라서 3개의 근거리 통신망 failure event을 AND 게이트로 연결하여 표현한다. SDP 잘못된 연산결과의 경우 자체적인 처리 시스템의 문제 또는 외부로부터 잘못된 입력 값을 받을 경우로 나누어 생각 할 수 있다.

두 번째는 경우는 SDP 자체적인 처리 시스템의 문제의 경우 서버 모듈의 failure rate을 적용하며, 근거리 통신망과 동일한 TMR 구조를 가지고 있으므로, 3개의 이벤트를 AND 게이트로 연결한다. 외부로부터 잘못된 입력 값을 받을 경우 역시 2가지 경우로 나누어 생각 할 수 있다. 즉 감시 센서의 문제로 잘못된 입력 값이 생성되는 경우와, EIF의 문제로 인해 잘못된 값이 전달되는 경우 이다. 감시 센서의 문제는 인위적인 failure rate인 0.15값을 적용하였다. EIF의 경우 서버 모듈의 failure rate을 적용하였으며, 이중화되어 있어 2개의 이벤트를 AND게이트로 연결하였다. 이와 같이 설계한 FTA의 결과 ATC가 잘못된 감시정보를 얻을 빈도는 1000시간 운용 시 7.852117로 산출 되었다.

3-4-2 비행자료처리시스템 Fault Tree Analysis

비행자료 처리 시스템 (FDP)의 고장형태를 분석하기 위해 FTA을 설계 하였으며, 그림 5에 도시하였

다. FTA의 Top Event는 ATC가 관제를 수행할 때 오류가 발생할 수 있는 상황을 고려하여 ATM시스템에서 CWP로 잘못된 비행처리 정보가 전달되는 이벤트를 결정하였으며, 이 이벤트를 기준으로 FTA 분석을 수행하였다. 그림1의 ATM 구조 블록도를 기반으로, 앞서 설명한 FTA분석절차에 따라 FDP 고장 수목을 디자인 하였다. 잘못된 비행처리정보가 ATC에게 전달 될 경우, 현시 시스템 자체의 문제 또는 현시 시스템으로 전달된 데이터의 문제를 예상 할 수 있다. 따라서 Top event는 현시 시스템의 문제와 잘못된 데이터의 전달 사건을 OR 게이트로 조합하였다. 현시 시스템의 실패는 앞서 제시한 서버모듈의 failure rate 값인 7.792288을 적용하였다. 잘못된 비행 자료의 전달 사건은 2가지 경우로 나누어 생각 할 수 있다. 첫 번째는 전송되는 데이터 경로상의 문제, 또는 FDP에서 잘못된 연산을 수행한 경우 이다. 따라서 잘못된 데이터의 전달 사건은 OR 게이트로 표현한다. 데이터 경로상의 문제는 근거리 통신망의 failure rate인 0.050330을 적용한다. 단 근거리 통신망의 경우 TMR 구조로 되어 있으므로, 3개의 근거리 통신망이 모두 failure 가 되야 한다. 따라서 3개의 근거리 통신망 failure event을 AND 게이트로 연결해서 표현한다. FDP의 잘못된 연산결과의 경우 자체적인 처리 시스템의 문제 또는 외부로부터 잘못된 입력 값을 받을 경우로 나누어 생각 할 수 있다.

두 번째 경우는 FDP 자체적인 처리 시스템의 문제를 고려할 수 있다. 이 경우 서버 모듈의 failure rate을 적용하면 되는데 서버가 TMR 구조를 가지고 있으므로, 3개의 이벤트를 AND 게이트로 연결한다. 외부로부터 잘못된 입력 값을 받을 경우 3가지 경우로 나누어 생각 할 수 있다. 즉 비행자료 터미널 또는 비행자료 센서의 문제로 잘못된 입력 값이 생성되는 경우

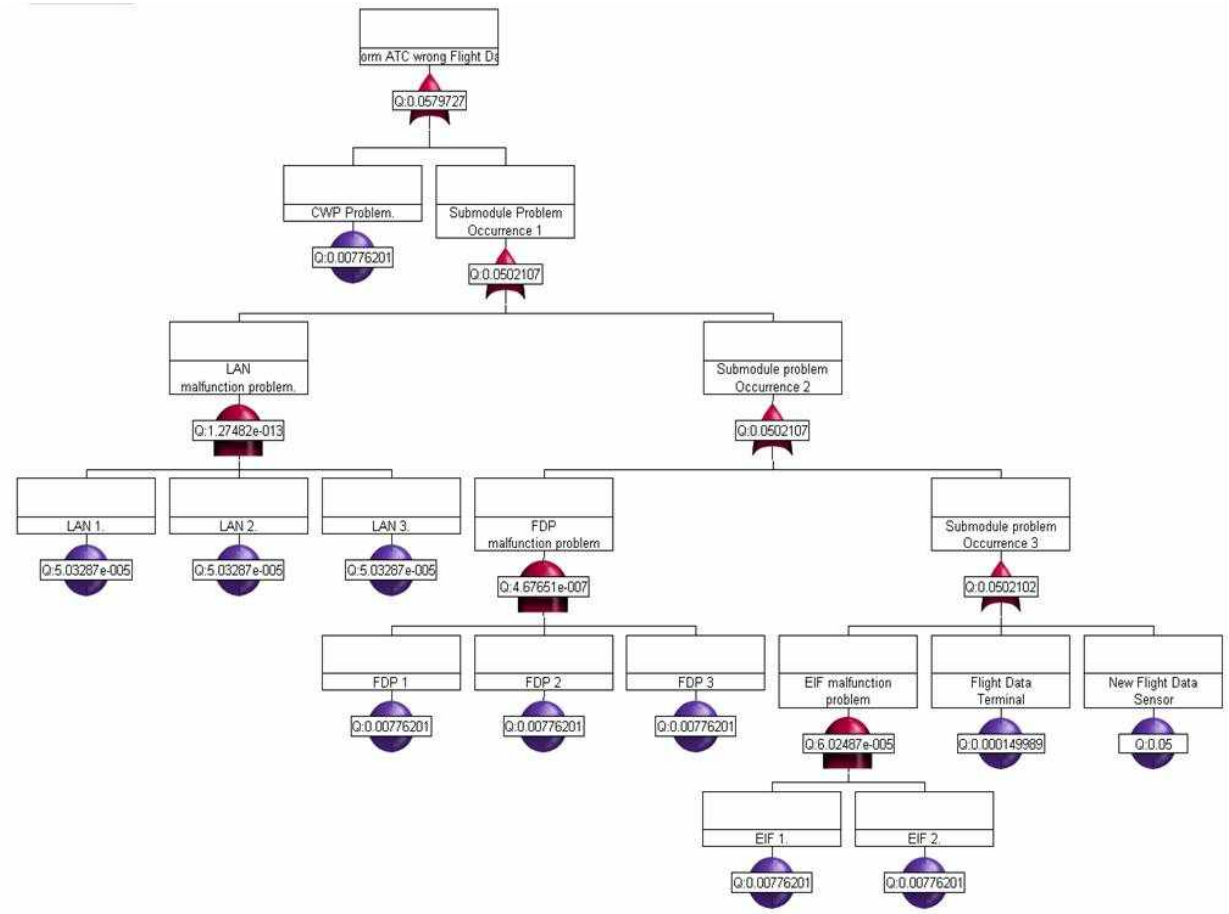

그림 5. 비행자료 처리시스템의 Fault Tree Analysis
figure 5. Fault Tree Analysis of FDP

와, EIF의 문제로 인해 잘못된 값이 전달되는 경우이다. 비행자료 터미널의 문제와, 비행자료 센서는 인위적인 failure rate인 0.15, 0.05을 각각 적용하였다. EIF의 경우 서버 모듈의 failure rate을 적용하였으며, 이중화되어 있어 2개의 이벤트를 AND게이트로 연결하였다. 이와 같이 설계한 FTA의 결과 ATC가 잘못된 비행처리 자료를 얻을 빈도는 1000시간 운용 시 8.003208로 산출 되었다.

Ⅳ. 결 론

Prototype ATM시스템을 RBD와 FTA를 사용하여 신뢰도를 평가하였다. 감시자료 처리시스템의 경우 1000시간 운용 시 Reliability 0.992088, Availability 0.988000, Failure Rate 7.945083, Total Downtime 3.960884이고 ATC가 잘못된 감시 정보를 얻을 빈도는 1000시간 운용 시 7.852117이다. 비행자료 처리시스템의 경우 1000시간 사용기준으로 Reliability 0.991979, Availability 0.994000, Failure Rate 8.113721, Total Downtime 4.005637이며 ATC가 잘못된 비행처리 자료를 얻을 빈도는 1000시간 운용 시 8.003208로 산출 되었다. 이와 같이 ATM시스템의 신뢰도를 정량화 및 일반화하여 ATM시스템의 신뢰도를 평가 및 검증 하였고 고신뢰성을 요구하는 ATM시스템의 설계에 신뢰성 평가지표로 사용 할 수 있다.

참 고 문 헌

[1] 김원경, 신뢰도공학의 이론과 실제, 교우사, 2005
[2] ICAO, http://www.icao.int/icao/en/anb/atm
[3] Aurora Air Traffic Management System http://www.adacel.co.uk/press/whitepapers/Aurora_White_Paper_07.pdf
[4] US MIL-HDBK- 217, "Reliability Prediction of Electronic Equipment ", *version F*, DOD, USA, 1991
[5] Bellcore technical Ref. TR-TSY- 000332, "Reliability prediction procedure for electronic equipment" issue 6, 1997
[6] British Telecom, "Handbook of reliability data for component s used in telecommunications systems ", Issue 4, 1987
[7] Siemens AG, SN29500, "Reliability and quality specifications failure rates of components ", *Siemens Technical Liaison and Standardization,* 1986
[8] NTT, "Standard Reliability Tables for semi conductor devices ", *Nippon Telegraph and Telephone Public Corporation* , 1982
[9] Italtel, “Italtel Reliability Prediction Handbook ", *Italtel corporate quality department* , Milano, 1993
[10] Centre National d 'Etudes des Telecommunications, "Recue il de Donnees de Fiabilite du CNET", *(National Centre for Telecommunications Studies, 'Compilation of CNET's reliability data').* 1983 edition

김 병 영 (金炳暎)

2008년 2월 : 한국항공대학교 항공전자 및 전자공학과(공학사)
2008년 3월 ~현재 : 한국항공대학교 항공전자 및 전자공학과 석사과정
관심분야 : 컴퓨터 시스템 설계

이 동 우 (李東雨)

2006년 2월 : 한세대학교 정보통신학과 졸업(공학사)
2008년 2월 : 한국항공대학교 항공전자 및 전자공학 석사 졸업
2008년 2월~현재 : 한국항공대학교 항공전자 및 전자공학 박사과정
관심분야 : 컴퓨터 시스템

나 종 화 (羅宗和)

1985년 2월 : 서강대 전자공학과 졸업.
1988년 : Wayne State University 석사.
1995년 : University of Arizona 박사.
2005년~현재 항공대학교 전자공학과 부교수.
관심분야: 컴퓨터 시스템.