



KR0100921

KAERI/AR-582/2000

원자력발전소 로봇 시스템의 신뢰도 및 안전성
분석 기술 현황

A Survey on Reliability and Safety Analysis Techniques of
Robot Systems in Nuclear Power Plants

한국원자력연구소

제 출 문

한국원자력연구소장 귀하

본 보고서를 2000 연도 “원전안전등급기기 성능개선 기술개발에 관한 연구” 과제의 기술현황분석보고서로 제출합니다.

2000. 12. .

부서명 : 종합안전평가팀

주 저 자 : 엄홍섭

공 저 자 : 김재희

이재철

최유락

문순성

요 약 문

I. 제 목

원자력발전소 로봇 시스템의 신뢰도 및 안전성 분석 기술 현황

II. 목적 및 필요성

로봇 시스템은 원자력분야를 비롯해서 모든 산업분야에서 널리 사용되고 있다. 이처럼 로봇이 많이 사용됨에 따라 이로 인한 사고도 많아지게 되자 최근에는 로봇에 관련된 안전성과 신뢰도에 대한 필요성이 대두되었다. 로봇이 많이 사용되고 있는 선진국의 각 기관들(미국의 ANS, 일본의 JISHA, EC) 그리고 여러 국제 표준기구(ISO, IEC)에서는 로봇의 안전성과 신뢰도에 관련된 표준 및 법령 체계를 구축해 가고 있다. 그러나 로봇 시스템의 신뢰도 및 안전성 분석 기법 분야는 그동안 로봇 산업 분야에서 주류가 아니었기 때문에 설계나 제작 분야에 비해 뒤떨어져 있었고 근래에 이르러서야 관심 분야로 대두되고 있다. 따라서 현재 로봇 시스템의 신뢰도 및 안전성 분석에 사용되고 있는 기법들은 다른 분야에서 입증된 여러가지 분석 기법을 도입하여 적용하는 상태이다. 현재 수행중인 “원전 안전등급 기기 성능개선 기술개발” 과제에서 개발중인 원자로 검사 장비에는 로봇 서브시스템이 포함되어 있는데 전체 장비의 품질 및 안전성과 신뢰도 확보를 위해 이들 분석 기법의 필요성이 대두되었다. 특히 원자력 분야에서 사용되는 로봇은 매우 높은 신뢰도와 안전성을 요구하며 또 일반적인 신뢰도평가에 더하여 원자력발전소라는 특수한 환경 예들 들면 원격조종(teleopeation)이나 방사선 내구성 문제(radiation tolerance)가 고려되어야 한다. 이를 위해 기존의 각종 안전성과 신뢰도 분석 기법들 그리고 실제 적용 사례들을 조사 분석 하여 그 결과를 본 장비의 품질 보증 및 인허가 과정 등에서 활용하고자 본 기술 현황을 조사 분석 하였다.

III. 내용 및 범위

1. 각 산업분야에서 많이 사용되고 그 실용성이 입증된 각종 신뢰도 및 안전성 분석 기법들을 조사 하였다. 신뢰도와 안전성 분석과 관련하여 로봇 산업분야에서 고유로 사용되는 기법은 아직까지는 없으며 사례 조사분석에서 나타난

바와 같이 로봇 분야에서 사용되는 대부분의 분석 기법은 타 분야에서 사용해 오던 것을 도입하여 사용하고 있다. 이들 기법들은 이론적으로나 실용적으로 타 산업 분야에서 어느정도 검증된 방법들이긴 하나 로봇 시스템과 같이 그 구성 부품과 기능이 복잡한 시스템의 분석에는 아직 미비한 것으로 알려지고 있다. 특히 디지털 부분과 소프트웨어 부분에 이들 기법들을 적용하는 것은 아직 초기 단계에 있다고 할 수 있다.

2. 신뢰도 및 안전성 분석에는 대상 시스템에 대한 깊은 이해가 필요하다. 로봇 시스템은 여타 시스템과는 다른 여러 특징을 가지고 있는데 로봇 시스템의 신뢰도 및 안전성 분석에는 이들 특성을 충분히 고려해야 한다. 로봇 시스템을 구성하는 기계 부분, 전자 부분, 시스템 전체의 특징과 고장 모드 그리고 이들이 신뢰도와 안전성 분석에 미치는 영향을 조사 분석 하였다.

3. 로봇 시스템이 원자력 환경에서 사용될 경우에 신뢰도와 안전성 분석시 고려해야 내용에 대해 조사 분석 하였다. 일반 산업 환경과는 구별되는 방사선에 의한 부품과 기기의 고장이나 원격운전환경 등과 같이 원자력 분야라는 특수한 환경이 신뢰도와 안전성 분석에 영향을 미치는데 이들에 대하여 조사 분석 하였다.

4. 선진 각국에서 수행된 로봇 시스템의 신뢰도와 안전성 분석 사례를 수집 분석하였다. 주로 원자력분야에 사용된 로봇 시스템들(Remote Reconnaissance Vehicle-RRV, INGRID, ROBUG III 등)에 대하여 조사하였으며 각 로봇시스템의 개요, 특성, 신뢰도 및 안전성 분석 기법, 분석상의 특이점에 대하여 분석하였다.

IV. 연구개발 결과

시스템의 신뢰도와 안전성 분석에 관련된 기존의 여러 가지 기법들을 조사하고 실제로 로봇의 안전성과 신뢰도 분석에 적용된 사례들을 분석하였으며 이들 조사된 기법들 중에서 로봇 시스템의 신뢰도와 안전성 분석에 가장 적합한 기법들을 선정하였다. 그리고 로봇 시스템이 가지는 특성들과 신뢰도 분석 시 원자력발전소라는 특수한 환경에서 생기는 사항들을 도출하였다. 조사된 신뢰도와 안전성 분석 기법들의 한계점으로는 이들 방법들이 그 동안 여러 산업과 기술분

야에서 널리 사용되어 왔고 그 실용성이 입증된 방법들이지만 최근의 로봇 시스템에는 거의 반드시 포함되어 있는 전자부분과 소프트웨어 부분, 즉 디지털 시스템 부분의 안전성과 신뢰도 분석에는 그 효용성과 정확성을 보장하지 못하고 있고, 특히 정량적 분석에는 거의 적용하지 못하고 있는 것이 현재의 기술 수준이다. 이 디지털 시스템의 신뢰도와 안전성 분석기술 분야의 연구는 원자력 분야를 포함해서 군수, 화학, 운수 산업 등 여러 분야에서 현재 활발히 진행중이며 Advanced Markov 모델, Bayesian Belief Nets과 같은 새로운 기법들이 각 분야에서 적용 시도되고 있다. 앞으로의 계획은 이들 조사 분석된 내용을 본 과제에서 개발중인 원자로 검사 장비의 로봇 서브시스템에 활용하여 본 장비의 품질 및 성능 향상에 기여하고 또 검사장비의 인허가 등의 과정에 사용할 계획이다.

SUMMARY

I. Project Title

A Survey on Reliability and Safety Analysis Techniques of Robot Systems in Nuclear Power Plants

II. Objective and Importance of the Project

Recently, robot systems have been introduced into various industries. Over the years there have been many robot-related accidents and increasing attention is being given to both reliability and safety of robot systems nowadays. Many organizations such as ANS in USA, JISHA in Japan and International Organizations including ISO and IEC are establishing standards and regulations for robot safety and reliability. But the analysis of safety and reliability of robot systems has not been main stream in robot industry so it had less concern than the design and manufacturing field. Thus techniques and models for robot safety and reliability were mostly from other industry fields. For the purpose of safety and reliability analysis of robot system which is the subsystem of reactor inspection system we are developing now, state of the art techniques related to safety and reliability analysis of systems are surveyed. Especially for robot systems in nuclear power plant environment ultra high level of reliability and safety are required and also requires special considerations related to the working environments such as teleoperation and radiation tolerance. Thus these topics were also surveyed.

III. Scope and Contents of Project

1. This report describes the current status of reliability and safety analysis techniques which have been used widely in many industry fields and which have been approved in practical applications. There were no inherent techniques or models for the safety and reliability analysis of

robot fields. Though all of these techniques approved in real fields they are still insufficient for the complicated system such as robot systems which are composed of electronic parts, mechanical parts, and software. Particularly the application of these techniques to digital and software parts of robot systems is immature at this times.

2. It is necessary to understand target system for the analysis of the system. Robot system has many characteristics differentiated from other systems and these characteristics are essential for the reliability and safety analysis of robot systems. All features and failure modes of mechanical parts, electronic part, and overall system were studied and the effect of these to the analysis was surveyed.

3. Working environments of robot systems must be considered in the analysis of robot systems. In nuclear applications of robot systems radiation degradation effect of components or teleoperation environment must be included in the analysis.

4. The case studies of safety and reliability analysis of robot systems developed in other countries were collected and studied. They were mainly robot systems developed for nuclear applications. System description, characteristics, analysis techniques, and the specialties of the analysis for each case were surveyed.

IV. Result of Project

The current status of the reliability and safety analysis was surveyed for the purpose of overall quality improvement of the reactor inspection system which is under development in our current project. The results of this survey are: (1) Reviewed various safety and reliability analysis techniques and models of systems: Reviewed reliability and safety analysis techniques were generally accepted techniques in many industries including nuclear industry. And we selected a few techniques which are suitable for our robot system. (2) Studied the characteristics of robot systems which are distinguished from other systems and which are important to the analysis of our robot system and reactor inspection system. (3) Studied

nuclear environmental factors which affect the reliability and safety analysis of robot system. (4) Collected and analyzed the case studies of robot reliability and safety analysis which were performed in foreign countries.

Reviewed techniques were proven in many industries but they still has limitations in real application, especially for the complex systems as robot systems. For the advanced and complex robot systems which are composed of electric parts, mechanical parts, and software parts the effectiveness and the exactness of these techniques were not validated until now, and quantitative assessment of robot systems using these techniques is just started. The research for safety and reliability analysis of digital systems including software are carrying out by many industries including nuclear field, military field, chemical field, and transportation field and new techniques such as advanced Markov model or Bayesian Belief Nets are introduced and applied to various applications.

The results of this survey will be applied to the improvement of reliability and safety of our robot system and also will be used for the formal qualification and certification of our reactor inspection system.

**PLEASE BE AWARE THAT
ALL OF THE MISSING PAGES IN THIS DOCUMENT
WERE ORIGINALLY BLANK**

목 차

제 1 장 서론	11
제 2 장 로봇 시스템 분석 기법	13
제 1 절 안전성 분석 기법	13
1. Checklists	14
2. Hazard Analysis	15
3. MORT Analysis	16
4. Fault Tree Analysis(FTA)	17
5. Failure Mode and Effect Analysis(FMEA)	19
6. Event Tree Analysis(ETA)	20
7. Hazard and Operability Analysis(HAZOP)	21
8. Cause-Consequence Analysis(CCA)	22
제 2 절 신뢰도 분석 기법	23
1. FMEA	23
2. FTA	23
3. Reliability Block Diagram(RBD)	25
4. 복합기술	26
5. Markov 모델	27
6. 모의 기법	28
제 3 장 로봇 시스템의 특성	30
제 1 절 고장의 특징과 메카니즘	30
제 2 절 안전성과 신뢰도 향상 방안	32
1. 안전성 문제 해결 방안	32
2. 설계 및 제작상의 요구사항	33

제 4 장 원자력 환경	35
제 1 절 개요	35
제 2 절 방사능에 영향을 받는 로봇 구성품	35
1. Drive mechanisms	36
2. 일반적 센서	37
3. 거리 센서	38
4. Force 센서	39
5. 관찰 시스템	39
6. Audio feedback 시스템	39
7. 통신 시스템	40
8. Electrical cables and connectors	40
9. 신호 전달 전자기기	41
제 3 절 부품 고장에 미치는 방사능 영향 모델링	42
제 5 장 외국의 로봇 시스템 신뢰도 및 안전성 분석 사례 ..	45
제 1 절 개요	45
제 2 절 사례	45
1. Remote Reconnaissance Vehicle(RRV)	45
2. Remote Work Vehicle(RWV)	47
3. Weigh and Leak Check System(WALS)	48
4. INGRID	49
5. ROBUG III	54
6. Gripper	56
7. Waste Retrieval Manipulator	59
제 6 장 결론	62
제 7 장 참고문헌	67

표 목차

표-1. FMEA 테이블 양식	19
표-2. Guidewords for HAZOP	22
표-3. RBD의 Connection 및 신뢰도 계산	26
표-4. Limit of usability for subsystems	42
표-5. Scenario decomposition with elementary task specification	51
표-6. Equipment requirements for elementary tasks: Teleoperator mode ..	51
표-7. Failure rates for equipment categories	52
표-8. Top event: Failure of Inspection, Cutting and Welding of Pipe ..	53
표-9. Top event: Failure of Inspection, Cutting and Welding of Pipe- Relative radiation	54
표-10. Top event: Failure of ROBUG communication system	56
표-11. Cutset lists of Top event: Failure of normal gripper function ..	58

그림 목차

그림-1. Fault Tree logic symbol	18
그림-2. FTA 절차도	19
그림-3. Simple radiation degradation function	43
그림-4. Piece-wise linear radiation degradation function	44

제 1 장 서론

그동안 로봇 산업 분야에서는 설계 및 제작 그리고 응용 기술에 중점을 두어 왔지만 로봇이 많이 사용됨에 따라 이로 인한 사고도 많아지게 되자 최근에는 로봇에 관련된 안전성과 신뢰도에 대한 필요성이 대두되었고 이에 대한 연구 및 현장 적용이 활발하게 진행되고 있다[1]. 그리고 이러한 산업 현장의 추세에 맞추어 로봇이 많이 사용되고 있는 선진국의 로봇 관련 각 기관들(미국의 ANS, 일본의 JISHA, EC)과 각종 국제 표준기구(ISO, IEC)에서는 로봇의 안전성과 신뢰도에 관련된 표준 및 법령 체계를 구축해 가고 있다[1][23].

한편 신뢰도와 안전성 분석 기법 분야에서는 이 분야가 그동안 로봇 산업분야에서 주류가 아니었기 때문에 설계나 제작 분야에 비해 뒤떨어져 있었으며 근래에서야 관심 분야로 대두되고 있는 실정이다. 따라서 현재 사용되고 있는 신뢰도와 안전성 분석 기술은 다른 분야에서 입증된 여러 가지 분석기술을 도입하여 적용하는 상태이다. 본 과제로 개발중인 원자로 검사 장비에는 로봇 서브시스템이 포함되어 있는데 전체 장비의 품질 및 안전성과 신뢰도 확보를 위해 이 로봇 서브시스템의 신뢰도와 안전성분석 기법에 대한 필요성이 요구되었다. 특히 원자력 분야에서 사용되는 로봇은 매우 높은 신뢰도와 안전성을 요구하며 또 일반적인 신뢰도평가에 더하여 원자력발전소라는 특수한 운전 환경, 예를 들면 방사선에 의한 부품이나 기기의 열화와 고장 문제 그리고 원격운전 환경 등이 고려되어야 한다. 이를 위해 기존의 각종 신뢰도와 안전성 분석 기법들 그리고 실제 적용 사례들을 조사 분석 하여 그 결과를 본 장비의 신뢰도와 안전성 향상에 활용하고 또 장비의 개발 완료 후 품질 보증 및 인허가 과정 등에서 활용하고자 본 기술 현황을 조사 분석 하였다.

본 보고서의 구성은 제 2장에서는 로봇 산업분야를 비롯하여 여타 산업 분야에서 널리 사용되고 있는 여러 가지 신뢰도와 안전성 분석 기법들에 대한 내용을 기술하였고 제 3장에서는 로봇 시스템이 타 시스템이나 장비들과 구별되는 로봇 시스템 고유의 특성에 대해 기술하였다. 그리고 제 4장에서는 신뢰도와 안전성 분석이 고려되어야 할 원자력발전소의 특수한 환경 요인들에 대해 기술하였고 제 5장에서는 선진 각국에서 수행된 로봇 시스템이 신뢰도 및 안전성 분석 사례를 수집 분석하였다. 그리고 제 6장 결론에서는 위의 각 조사 분석된 항목

에 대한 요약 및 결론과 로봇 시스템의 신뢰도 및 안전성 연구분야의 앞으로의
경향에 대하여 기술하였다.

제 2 장 신뢰도 및 안전성 분석 기법

현재까지 문헌상에 나타난 신뢰도 및 안전성 평가 기법들은 30여 가지가 넘는다. 이들을 사용할 때 중요한 점은 대상 프로젝트에 가장 적합한 모델과 기법들을 선택하는 일이다. 각 기법들은 서로다른 적용 범위와 검증성을 가지고 있고 그래서 개발 제품의 생명주기 전체에 걸쳐 수개의 기법이 필요할 수도 있다. 아래에 기술된 기법들은 어느 한 기법이 다른 기법에 비해 절대적으로 우수한 것은 없다. 어떠한 종류의 기법도 모든 프로젝트나 모든 목표를 만족시키는 것은 아직까지는 없기 때문이다. 또 하나의 중요한 점은 이들 기법들이 아직까지는 충분한 검증을 거쳤다고 볼 수 없기 때문에 그 분석 결과를 사용할 경우 주의를 기울여야 한다는 점이다. 이는 이들 기법들이 소용없다는 것이 아니고 다만 조심스럽고 적절하게 그리고 전문가의 판단과 경험을 바탕으로 사용되어야 한다는 것을 뜻한다. 이들 기법들을 여러 가지로 분류가 될 수 있다. 여기에서는 안전성 분석에 사용되는 것과 신뢰도 분석에 사용되는 것으로 나누어 기술한다. 두 용도에 모두 사용되는 기법들은 한 곳에만 내용을 기술하고 다른 곳에서는 용도상의 차이에 대해서 기술하였다.

제 1 절 시스템의 안전성 분석 기법

시스템 분석의 일부로서 시스템 안전성 분석은 설계 및 제작 단계에서 일찍부터 사용되어 왔다. 분석의 목표는 시스템에 의한 사고가 발생하기 전에 위험 요소를 미리 파악하여 설계 및 제작 단계에서 이들 요소를 제거하프로서 보다 안전한 시스템을 개발하는 것이다. Clemens에 의하면 시스템의 안전성 분석과 관련된 기법은 30여가지가 넘으며 다음과 같은 것들이 있다[2].

- (1) Management Oversight and Risk Tree(MORT) Analysis
- (2) Interface Analysis
- (3) High potential method
- (4) Fault Tree Analysis(FTA)
- (5) Failure Mode and Effect Analysis(FMEA)
- (6) Event Tree Analysis(ETA)
- (7) Critical incident technique,

- (8) Change analysis,
- (9) Audits,
- (10) Criticality Analysis
- (11) Job safety analysis,
- (12) Flow analysis,
- (13) Sneak circuit analysis,
- (14) Systematic inspections
- (15) Single point failure analysis
- (16) Prototype
- (17) Subsystem Hazard Analysis
- (18) Technique of human error rate prediction
- (19) System hazard analysis,
- (20) Random number simulation analysis
- (21) Industrial hygiene methods
- (22) Generic preliminary hazard analysis
- (23) Naked man method
- (24) Procedure analysis
- (25) Networks login analysis,
- (26) Preliminary hazard analysis
- (27) Worst case condition technique
- (28) Operating and support hazard analysis
- (29) Energy analysis
- (30) Contingency analysis
- (31) Scenario technique

이들 안전성 분석 기법 중에서 효용성과 실용성 측면에서 인정을 받아 각 산업분야에서 사용되고 있는 주요한 기법들을 다음에 요약하였다.

1. Checklists

안전성에 관련된 항목 체크 리스트를 이용하는 방법이다. 특별히 안전성 분석 기법이나 모델로 분류되는 방법은 아니지만 가장 기초적이며 그 적용의 간단함 때문에 대부분의 분석 방법에서 명시적으로나 암시적으로 내포되어 있고 또 단

독으로도 많이 사용된다. 각 체크 항목들은 과거의 실패 사례나 경험에서 얻어진 교훈 그리고 각종 절차나 표준들을 이용하여 작성되며 많은 다른 기법들이 이 체크리스트의 형태를 그 내부에 포함하고 있다. 잘 알려져 있는 시스템의 설계나 제작 그리고 기술이 급속히 변하지 않는 경우에 가장 적합하게 사용될 수 있으며 체크리스트의 내용이 적절하게 갱신된다면 그 조직의 고유한 분석 절차의 하나로서 자리잡을 수 있다. 제품의 생명주기의 각 단계에서 모두 사용될 수 있고 생명주기의 한 단계에서 다음단계로 넘어가는 시점에서 매우 유용하다. 이 기법은 설계자와 검토자에게 모두 사용하기 쉽고 유용한 도구이지만 단점으로는 리스트에 포함되지 않은 사항에 대해서는 간과하기 쉽다는 점과 완벽하게 하기 위해서는 수많은 질문 항목이 있어야 하고 또 그 질문 항목 개수는 점점 증가한다는 것이다. 그리고 리스트에 있는 항목을 모두 만족시키면 그 시스템은 안전하고 신뢰성이 있다는 거짓 믿음을 갖기 쉬운 점과 리스트 상의 각 항목에 관련된 특수한 상황을 제대로 이해하지 못하고 적용하면 오히려 더 위험한 결과를 초래할 수도 있다는 점이다.

2. Hazard Indices

이 기법은 화재, 폭발, 또는 화학적 물질로 인해 발생하는 재난으로부터 발생할 수 있는 잠재적 손실을 측정하는 것으로 프로세스 산업에서 주로 사용되며 Dow Chemical Company Fire and Explosion Index Hazard Classification Guide (간략하게 Dow Index)가 그 대표적인 예다. 처음에는 보험과 화재 방지 방법의 선택을 지원하기 위해 개발되었지만 일반적인 위해도 규명이나 잘 알려진 위험의 위해도 수준을 평가하거나 기존 공장을 감사할 때도 효용성이 있다. 이 기법은 주어진 설계상에서 위해도의 잠재성을 정량적으로 제공한다. 설계와 장비가 표준화되고 변경이 별로 없는 프로세스 산업에서는 매우 유용한 기법이지만 새로운 설계가 필요한 시스템이나 기술이 급속도로 변하는 경우에는 효용성이 별로 없다. 또 Index들은 단지 제한된 위해도 관련 항목들만을 포함하고 있고 또 이들에 대해서도 위해도 수준만을 결정해준다. 따라서 위험을 제거하거나 축소화하기 위해 반드시 필요한 특정 원인들에 대해서는 고려하지 않는 기법이다. 이런 이유로 이 기법은 단독으로는 완전한 도구가 되지 못하고 다른 기법들을 보완하는 형태로 주로 사용된다.

3. Management Oversight and Risk Traa(MORT) analysis

US. Nuclear Regulatory Agency의 Johnson에 의해 1970년대에 개발되었으며 원래는 로직 다이어그램(fault tree)에 근거한 사고(accident) 모델인데 안전성 분석에도 사용된다. MORT는 사고 조사용으로 작성된 체크 리스트 형태로 사고에 포함된 모든 요인들이 로직 게이트(and/or)로 연결되어 있다. 98개의 일반적인 문제들에 대한 1500여개의 기본 사건들이나 요인들이 MORT 수목(tree)에 포함되어 있다. 모든 사고에 의한 손실은 예상하지 않은 에너지의 전이에 의해 발생하며 이의 원인은 장벽이나 제어의 결함으로 보고 있다. 손실은 두가지 원인으로 부터 발생하는데 그것은 (i) specific job oversight and omissions (ii) the management system that controls the job 이다. 이 모델은 특히 사고에 있어서 변화의 역할을 증시하는데 그들은 다음과 같다.

- o nonroutine operations mode, such as trials and tests(Chernobyl 경우)
- o maintenance and inspection(TMI 경우)
- o changeover or repair(Flixborough 경우)
- o starting or stopping, special jobs, troubleshooting, incipient problems

사고들은 일반적으로 연속된 에러나 변화처럼 원인이 되는 요인들을 가지고 있기 때문에 MORT는 사고순서를 개별적인 사건으로 분해해 주는 방법을 제공하며 그러한 요인들로는 다음과 같은 것들이 있다[3].

- o technical informaton system
- o design and planning
- o maintenance
- o inspection
- o immediate supervision and high-level management
- o barriers
- o unwanted energy flow
- o policy
- o management system

MORT는 체크리스트를 기본으로 하고 있기 때문에 체크리스트 방법이 가진 장점과 단점을 그대로 가지고 있다. 이 방법의 특기할 만한 장점은 조직이나 정보 시스템 관리 절차 기업의 원칙이나 목표와 관련된 요인들을 고려하였다는 점이지만 그 사용상의 복잡성 때문에 많이 사용되지는 않는다.

4. Fault Tree Analysis(FTA)

항공, 전자, 원자력산업 분야 등에서 널리 사용되는 방법이다. 1961년 Bell 연구소에서 H.A. Watson에 의해 개발되었는데 Minuteman Launch Control System의 평가가 그 목적이었다. 그 후 Bell 연구소에서 통신장비에 사용중이던 Boolean Logic 방법이 FTA에 채용되었고 보잉사에서 그 전체적 분석 절차를 개발하였다. FTA의 주 목적은 위험 사건을 찾아내는 것이 아니고 그 위험의 원인을 분석하는 것이다. 따라서 수목(tree)의 최상위사건(top event)은 미리 알려져 있어야 하며 이는 종종 다른 분석 기법을 이용하여 수행된다. FTA는 일반적으로 다음과 같이 4단계로 나누어 수행된다.

- 시스템 정의
- Fault Tree 구성
- 정성적 분석
- 정량적 분석

(1) 시스템의 정의

FTA에서 가장 중요하고 어려운 단계로 최상위 사건, 초기조건, 기존 사건들 그리고 허용불가 사건들을 결정한다. 최상위 사건의 결정은 매우 중요한데 시스템 분석에 필요한 모든 최상위 사건이 나오지 않으면 그 그분석 결과는 결함을 가지게 되기 때문이다.

(2) Fault Tree 구성

시스템이 정의가 되면 다음 단계는 수목을 구성하게 되는데 여기서는 먼저 시스템의 상태와 정점 사건(top event)을 설정하게 된다. 그리고 이 정점 사건의 원인이 되는 사건들을 찾아내어 logic symbol을 이용하여 연결해 내려간다. FTA에 사용되는 logic symbol은 그림-1과 같다.

(3) 정성적 분석

Fault tree가 만들어진 다음 수행되는 정성적 분석의 목적은 정점 사건을 야기시키고 더 이상 수를 줄일 수 없는 minimal cut sets이라고 불리우는 기본사건들을 찾아내는 것이다. Cut set은 Cut set 내의 어느 한 사건이라도 일어나지 않으면 정점 사건이 일어나지 않은 것으로 정의된다. Minimal cut set은 시스템의 취약점에 대한 정보를 제공한다.

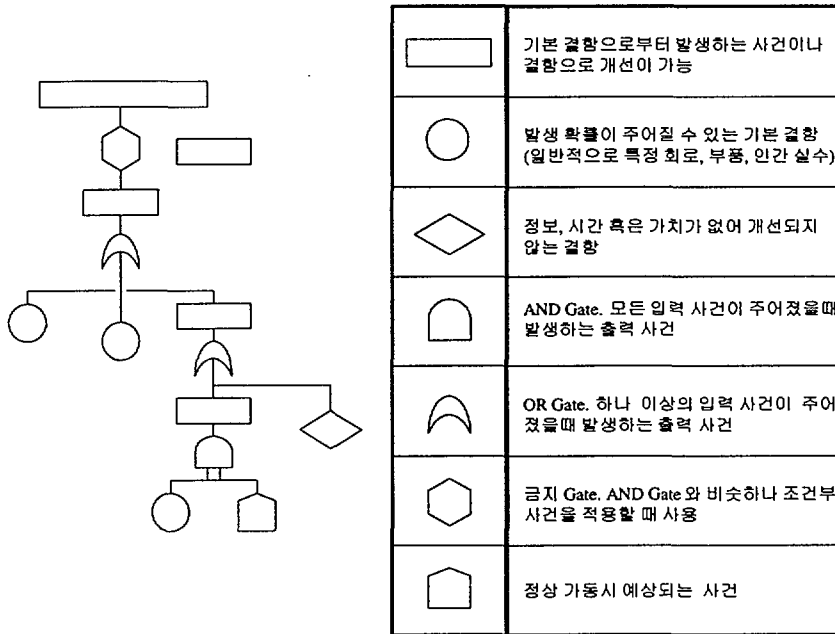


그림 1 고장 수목

(4) 정량적 분석

정량적 분석은 minimal cut set을 이용하여 기본사건이 일어날 확률로부터 정점 사건이 일어날 확률을 구하는 것이다. FTA의 일반적인 정량적 분석 절차는 그림 2와 같다. 정점 사건이 일어날 확률은 통계적으로 독립적인 모든 cut sets 확률의 합이다. Fault tree의 정량적 분석을 수행 할 때 자주 일어나는 오류는 빈도(frequencies)와 확률(probabilities)을 곱하게 되는 경우라고 알려져 있다.

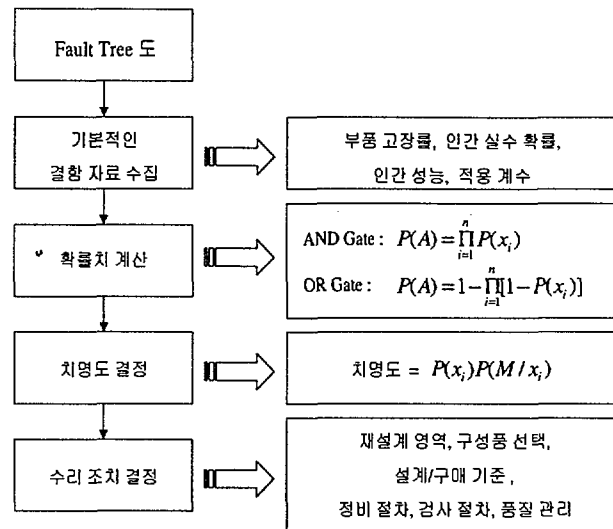


그림 2 FTA 절차

5. Failure Mode and Effect Analysys(FMEA)

이 기법은 기기의 신뢰도를 예측할 목적으로 개발 되었으며 위해나 위험보다는 기능의 성공적 수행에 강조를 두고 있다. 따라서 대상 기기나 시스템이 정해진 시간동안 고장 없이 성공적으로 운전될 전체적인 확률을 구하는 것이 이 기법의 목표이다. 분석의 첫 단계는 시스템을 구성하고 있는 모든 부품을 나열하고 가능한 운전상태에 따른 고장 모드를 열거하는 것이다. 그리고 각 고장모드별로 시스템의 다른 부품에 미치는 영향과 전체 시스템에 미치는 영향을 밝혀낸다. 마지막으로 각 고장모드별 결과의 심각성과 확률을 계산한다. 각 부품의 고장율은 과거의 경험이나 제작자로부터 얻어지는 일반화된 고장율을 주로 사용하게 되는데 분석 대상 부품이 사용될 환경이 얻어진 고장을 데이터가 생성된 환경과 일치하거나 유사한 지 주의가 필요하다. 왜냐하면 신뢰도 데이터의 생성환경과 운전 환경이 많이 다를 경우 각 부품의 고장율은 현저히 달라지기 때문이다. 분석 결과는 테이블 형태로 작성되는데 일반적 양식은 다음 표-1과 같다.

표-1 FMEA 테이블 양식 예

Component	Failure probability	Failure mode	Percent failures by moce	Effect

FMEA는 단독 부품이나 단독 고장에 대한 분석에 유효하며 분석의 완전성을 기할수 있다는 장점이 있는 반면 그 만큼 시간과 비용을 많이 요구한다. 따라서 모든 부품이 표준화되어 있고 고장 모드가 미리 알려져 있는 경우에 적합하다.

FMEA가 주로 적용되는 단계는 상세 설계가 완료되고 모든 하드웨어 부품이 결정된 후의 단계이다.

6. Event Tree Analysis(ETA)

FTA가 시스템 고장의 정량화에 가장 많이 쓰이는 방법이지만 이 방법은 시스템이 복잡해 질 경우 고장 수목이 너무 복잡하게 만들어지기 때문에 사용하기가 어렵다. ETA는 WASH-1400의 확률론적 위험도 평가(probabilistic risk assessment, PSA)의 FTA를 수행하던 중 위와 같은 문제점을 해결하고자 경영, 경제 분야에서 당시 널리 사용되던 결정수목(decision tree) 기법을 채용하여 해결하고자 하는 문제를 FTA가 가능한 작은 단위로 분해하기 위해 만들어졌다. ETA는 주어진 초기 사건(initiating event)에 의해 생길 수 있는 모든 가능한 결과를 찾아내게 되는데 초기 사건들은 시스템의 고장이나 또는 시스템에 대한 외부의 사건이 될 수 있다. 사건 수목(event tree)은 초기 사건이 진행되는 방향으로 그려지게 되는데 각 단계별 진행은 다른 시스템이나 기기의 성공과 실패에 의해서 결정된다. 원자력발전소 보호 계통의 경우 어떤 초기 사건(예: 파이프 파열 등)이 발생하면 이와 관련한 보호 계통이 작동하게 되는데 이들 보호 계통을 구성하는 각 시스템들이 사건 수목의 heading이 되고 초기 사건의 진행은 이들 heading에 위치한 각 시스템의 성공 또는 실패에 의해 분기하는 형태로 작성된다. 분기는 두가지 경우가 되는데 (i) 보호계통이 성공적으로 동작하는 경우(upper branch), (ii) 보호 계통이 실패하는 경우(lower branch)이다. 수목이 완성되면 초기 사건부터 최종 결과까지 경로(path)들이 생기게 되고 이들 각 경로가 사고(accident)의 순서(sequence)가 된다. ETA는 다음과 같은 경우에 유용하다.

- 사고의 확률에 가장 큰 영향을 미치는 방어 시스템의 특성을 파악하여 그들의 고장 확률을 줄일 수 있는 조치를 취할 수 있게 한다.
- 다음 단계의 분석 작업이 되는 FTA의 정점 사건을 확인한다.
- 단일 초기 사건으로부터 야기될 여러 가지의 사고 시나리오를 표시한다.

반면 ETA는 시간 순서가 있는 시스템간의 상호작용이 많을 경우 극단적으로 복잡한 수목이 생긴다는 것과 초기 사건들 별로 수목이 그려지기 때문에 복잡한 초기사건의 영향이나 상호 작용에 대해 알기 어렵다는 점 등이다. 생명 주기상에서 ETA가 주로 사용되는 단계는 대부분의 설계가 끝난 다음이다.

7. Hazards and Operability Analysis(HAZOP)

HAZOP은 영국의 Imperial Chemical 회사에 의해 1960년대 초에 개발되었으며 화학공정 산업 분야에서는 새로운 시설을 설치할 경우 절반 이상이 이 기법을 사용하고 있다고 한다[31]. 이 기법은 이름에서 나타나듯 위험(hazard) 분석과 더불어 효율적인 운영에 대한 분석도 겸하고 있다. 이 기법은 정량적 분석 기법으로 설계상 의도 되었던 운전상태로부터 벗어나는 모든 상황과 이런 상황과 관련된 모든 위험을 찾아내는 것이 주 목적이다. 체크리스트와 같은 다른 기법들과는 달리 HAZOP은 새로운 설계상에서의 위험이나 예전에는 고려되지 않았던 위험도 찾아낼 수 있고 이 점이 다른 기법들과는 다른 가장 큰 특징이다. HAZOP의 분석 내용은 다음과 같다.

- o The design intention of the plant
- o The potential deviations from the design intention
- o The causes of these deviations from the design intention
- o The consequences of such deviations

이 분석 과정에서는 지침 단어(Guidewords)가 사용되는데 그 내용은 표-2와 같다.

표-2. Guidewords for HAZOP

지침 단어	의 미
NO, NOT, NONE	The intended result is not achieved, but nothing happens
MORE	More of any relevant physical property than there should be
LESS	Less of a relevant physical property than there should be
AS WELL AS	An activity occurs in addition to what was intended, or more components are present in the system than there should be
PART OF	Only some of the design intentions are achieved
REVERSE	The logical opposite of what was intended occurs
OTHER THAN	No part of the intended result is achieved, and something completely different happens

8. Cause-Consequence Analysis(CCA)

CCA는 1970년대에 Neilson에 의해 개발되었다[32]. 분석은 critical event라는 초기 사건으로부터 시작해서 그 사건의 원인을 찾아내고(top-down or backward search) 또 그로부터 발생할 수 있는 결과를 찾아낸다(forward search). Cause-sequence diagram은 사건들 간의 시간 종속성과 인과 관계를 보여준다.

Cause-sequence diagram에 사용되는 심볼들은 일반적으로 다음과 같다.

- o AND gate, OR gate, AND vertex, Mutually exclusive/exhaustive OR vertex,
- o Mutually exclusive OR vertex(used after time delays),
- o EITHER/OR vertex(decision box), Condition vertex, Basic condition,
- o Initiating event(maybe critical event), event,
- o Significant consequences, Condition, Fixed time delay, Variable time delay

CCA는 FTA에 비해 사건의 순서를 명시적으로 보여주기 때문에 CC (Cause-consequence) 다이어그램은 기동이나 정지 그리고 다른 순서 제어 시스템을 분석하는데 매우 유용하며 플랜트의 블록다이어그램이나 배선도로부터 체계적으로 다이어그램을 생성하는 기법이 있다. 또 CC 다이어그램은 ETA에 비해

time delays, alternative consequence paths, combination of events 등을 표현할 수 있는점에서 이점을 가지고 있으며 정량적 분석에도 사용할 수 있다. 단점으로는 각 초기 사건에 대해 별도의 다이어그램이 필요하며 분석 결과들은 분석 대상이 되는 원인에만 한정된다는 점이다.

제 2 절. 시스템의 신뢰도 분석 기법

1. Failure Mode and Effect Analysis(FMEA)

FMEA는 로봇 시스템의 안전성 분석에서 뿐만 아니라 신뢰도 분석에서도 사용이 가능하다. 이 기법은 로봇 구성품의 고장 모드를 체계적으로 분석하고 그들 고장의 효과가 전체 시스템의 기능 수행능력에 미치는 영향을 결정하는데 사용한다. 신뢰도 분석에 있어서 이 기법의 주요 장점은 고장의 근원에 대한 가설을 세우는 것이다. 그리고 그것에 의하여 fail-safe나 시스템 redundancy와 같은 기능을 포함하는 재 설계를 하여 고장의 확률이나 고장 결과의 치명도를 줄일 수 있다. 신뢰도 분석시의 단점으로는 단일 고장 (singularity-failure) 분석이라는 특성으로 인하여 둘 이상의 고장이 복합된 효과에 대하여는 평가가 적합하지 않다는 점이다.

2. Fault Tree Analysis(FTA)[29]

이 기법 역시 FMEA와 마찬가지로 로봇 시스템의 안전성과 신뢰도 분석 모두에 사용이 가능하며 가장 널리 쓰이고 있다. 설계, 공장 시험 혹은 실제 자료 분석 동안에 발견된 고장 유형을 분석하는데 적합하다. FTA 절차는 그림 2와 같이 기본적인 결함을 발견하여 이들의 원인과 결과를 밝혀내고 이들의 발생 확률을 결정하는 반복적인 기록 과정으로 특징 지워진다. 즉, 시스템 고장과 안전 위험을 일으키는 기본적인 결함이나 사건을 설명하는 고장 수목 논리도를 작성하고 확률값 계산을 위해 기본적인 결함 자료와 고장 확률 자료를 수집한다. 그런 다음에 기본적인 결함을 분석하고 고장 유형에 대한 확률을 결정, 치명도를 결정하는 것이다.

이러한 FTA 절차는 시스템의 생명주기 어느 단계에도 적용이 가능하나 다음의 경우에 가장 효과적이다.

- ① 기초적인 설계단계에서 설계정보와 실험실 혹은 기술적 시험 모델에

근거하여 적용할 경우

- ② 최종 설계자가 끝나고 대량생산이 이루어지기 전에 생산 설계와 초기 생산 모델을 근거하여 적용할 경우

첫 번째 경우는 고장 유형을 결정하고 다른 대안(일차적으로 설계분야에서)을 구성할 때 수행된다. 두 번째 경우는 신뢰도와 안전도 관점에서 시스템의 생성이 수용 가능한가를 보여주는 데 사용된다. 두 번째 분석으로부터 도출된 정정 조치나 척도는 제조에 따른 설계 구조의 관점에서 수행될 수 있는 관리나 체계적인 조치에 중점을 두고 있다.

장점: 고장수목으로 표현하면 시스템의 고장 프로세스와 고장 전파를 명확히 파악할 수 있다.

단점: 고장수목이 널리 사용되고 있지만 다중 구성의 시스템을 다루는데는 부족한 점이 있으며, 단점들을 열거하면 다음과 같다.

- 시간 표현 : 다단계 임무(multiphase mission)는 수행시 각 단계마다 서로 다른 기기구성을 요구한다. 그러나 고장수목을 가지고 나타내기가 쉽지 않다. 또한 다중 시스템에서 전환 시에 걸리는 시간과 같은 시간 간격을 표현 할 수 없다.
- 고장의 심각도 : 복잡한 시스템에서는 다중고장과 같이 고장유형도 복잡할 수 있다. 기기가 기능을 못하는 것과 기기는 영향이 적으나 인명이 위태로운 경우 등을 구분하기가 어렵다.
- 고장 순서 : 복잡한 다중 시스템에서는 고장의 영향을 파악하기 위해서는 고장 순서가 중요하다. 시스템의 대응이 고장 순서에 따라 달라지기 때문에 중요한 다중 시스템에서는 고장 발생 순서가 더욱 중요하다. 그러나 고장 수목은 이것을 나타낼 수가 없다.
- 고장 중복 : 동일한 형태의 고장이 다른 곳에서도 나타날 수가 있는데 이것을 구분하여야 예러가 발생되지 않는다.
- 고장 전파 : 다중 시스템에서 한 시스템에 고장이 발생되면 이 고장을 복구 또는 우회하기 위하여 시스템 구성이 동적으로 변경된다. 즉 동적 신뢰도 모델이 필요하나 고장 수목으로는 이를 표현할 수 없다.
- 복구 및 보수 : 다중시스템에서는 복구와 보수가 중요한 운전 상태이다. 그러나 고장수목으로는 이러한 프로세스를 표현할 수 없다.

3. Reliability Block Diagram(RBD)

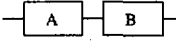
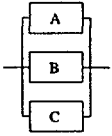
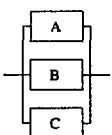
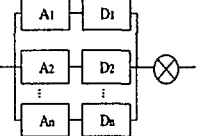
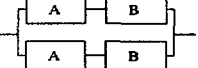
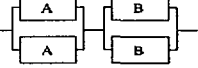
RBD는 시스템의 구성 부품별 성능 및 이들의 연결에 의거해 전체 시스템의 신뢰도를 계산하는 간단하고 효과적인 방법이다. 이 기법에서 시스템의 신뢰도 측정을 위한 첫 단계는 시스템의 고장모드를 찾아내고 모든 부품의 신뢰도 정보를 수집하는 것이다. 블록 다이어그램 상에서 성공 확률이나 고장율이 부여된 블록들은 시스템을 구성하는 각 부품을 나타낸다. 이들 블록들은 서로 연결되어 신뢰도 망을 구성하게 되는데 이것은 시스템 각 구성 부품의 신뢰도 의존도를 나타내는 것이다.

RBD 모델 기본 규칙은 다음과 같다.

- o Failure Independence Of Block Failures
- o Bimodal Device Status
- o System Operational If All Devices Operate
- o System Failure If All Devices Fail
- o A Device Failure Cannot Make a Failed System Operational
- o System Remains Operational After Any Device Repair
- o All Block Connecting Lines Have A Reliability Of 1
- o A Block Fails If Any Part Of the Block Fails

RBD의 신뢰도 망들은 시스템이 어떻게 구성되느냐에 따라 여러 가지로 구성되는데 각 구성 형태에 따른 연결 및 신뢰도 계산은 다음 표-3와 같다

표-3. RBD의 연결형태 및 신뢰도 계산

연결 형태	다이아그램	신뢰도 계산
Series		$\prod_{i=1}^n R_i$
simple parallel redundancy		$1 - \prod_{i=1}^n (1 - R_i)$
m of n parallel redundancy		$\sum_{i=m}^n \frac{n!}{i!(n-i)!} R_i^i (1 - R_i)^{n-i}$
standby redundancy		$e^{-\lambda_s t} [1 + \frac{\lambda}{\lambda_s} (1 - e^{-\lambda_s t})]$
parallel-serial redundancy		$2R_a R_b - R_a^2 R_b^2$
serial-parallel redundancy		$(2R_a - R_a^2)(2R_b - R_b^2)$

RBD의 가장 큰 장점은 이해와 적용이 쉽다는 점이고 단점으로는 부품이나 서브시스템의 열화 고장모드를 모델링하기에 부적합하다는 점이다.

4. 복합 모델(Combinational Models)

시스템의 신뢰도 계산을 하는데 있어서 두 개 이상의 기법을 사용하는 방법은 널리 사용되어 왔고 대부분의 시스템 분석에서 표준 기법으로 채용되고 있다 [27]. 가장 많이 사용되는 것은 FTA와 RBD를 사용하는 방법이다. 하지만 이러한 방법에도 제약점이 있는데 그 내용은 다음과 같다[30].

- o It is difficult, if not impossible to allow for various types of dependencies such as repair, near coincident faults, transient and intermittent faults and standby systems with spares

- o The nature of the combinational approach requires that all combinations of events for the entire time period must be included. For complex systems, this results in complicated models.
- o A fault tree is constructed to predict the probability of a single failure condition. If a robot has many failure conditions, separate fault trees must be constructed for each one of them.

5. Markov Models

Markov 확률 모형은 두 확률변수의 함수로써, 시스템의 상태(state)를 나타내는 확률변수 X 와 관측시간을 나타내는 확률변수 t 의 함수이다. 여기서 X 와 t 가 각각 이산적(discrete)인가 연속적(continuous)인가에 따라 Markov 모형을 4가지로 분류할 수 있으며 그 중에서 상태가 이산적이고 관측 시간이 연속적인 모형은 신뢰도 공학에서 중요한 의미를 가진다. 상태와 관측시간의 개념을 설명하기 위해서 4칸으로 나누어진 나무상자의 경우에, 이 나무상자의 4칸 중의 하나에 탁구공을 넣어 상자의 밑바닥을 치면 공이 위로 튀어 올랐다가 4칸 중에 하나에 다시 떨어진다. (문제를 간단히 하기 위해 공이 상자밖으로 떨어질 가능성은 없다고 가정한다). 나무상자의 4칸을 상태(state)라 하고 상자의 밑을 친 직후 탁구공이 튀어 올랐다가 다시 어떤 칸으로 떨어지는 시각을 관측시간이라고 하자. 만약 상자 밑을 주기적으로, 예를 들어 5초에 한번씩 친다면 상태도 이산적이고 시간도 이산적이므로 이런 모형을 Markov 사슬(chain) 모형이라고 한다. 만약 상자 밑을 치는 시각이 주기적이 아니라면 관측시간은 연속변수(continuous variable)이고 이런 모형을 Markov 과정(process)이라고 한다. 만약 상자의 칸을 없애고 상자의 길이(l)에 따라 $x=0$ 부터 $x=l$ 까지의 척도를 가지고 공이 떨어진 위치를 측정한다면 $x=0 \sim l$ 의 연속적인 상태를 생각할 수 있게 되며 관측 시간이 이산적인가 연속적인가에 따라 연속상태 변수를 갖는 모형도 두 종류로 분류할 수 있을 것이다.

Markov 모형은 어떤 상태 i 에서 다른 상태 j 로의 천이(transition) 확률의 집합 P_{ij} 로 정의된다. 위의 이산 상태의 예에서 상자의 칸의 크기를 모두 같게 해 준다면 천이 확률은 모두 같을 것이고 좀더 일반적으로 칸들의 크기를 모두 다르게 한다면 천이 확률도 각각 달라질 것이다. Markov 모형의 중요한 특성 중 하나는 천이 확률 P_{ij} 가 상태 i 와 j 에만 달려 있어서 과거의 상태와는 전혀 관계가 없다는 것이다(independent).

Markov 과정은 연립 미분 방정식과 초기조건으로 나타나게 된다. 단지 최종 상태만이 확률을 결정한다는 Markov 과정의 기본 가정 때문에 항상 연립 1계 미방(first-order differential equation)을 얻게 된다. 연립 미방에서 계수들을 추이 행렬(transition matrix)로 만들어 명시할 수 있다. Row는 과정이 시간 t 에 있을 상태를 나타내고 column은 과정이 시간 $t+dt$ 에 추이할 상태를 나타내며 전자를 초기상태(initial state), 후자를 최종상태(final state)라 한다. 여기서 P_{ij} 는 시간 간격 dt 사이에 시스템이 초기상태 i 에서 최종상태 j 로 추이할 확률을 나타낸다. 이렇게 정의된 미분 방정식을 풀어내므로써 시스템이 각 상태에 존재할 확률을 구하게 된다.

일반적으로 Markov 모델을 모사하기 위해서 시스템 상태를 나타내는 마디(node)와 추이 확률을 나타내는 지선(branch)로 이루어진 Markov graph를 사용하는 경우가 많다.

6. Simulation Technique(Monte-Carlo)

Monte-Carlo 모의실험은 시스템을 구성하는 부품의 고장에 의거 분산된 시간 상에서 각 부품의 고장을 모의함으로서 신뢰도를 계산하는데 사용될 수 있다. 아이템 고장과 수리 분산(repair distribution)으로부터 무작위 표본을 추출하게 되는데 이는 매우 많은 양의 무작위 숫자를 필요로 한다. 고장이나 수리 또는 동작과 같은 매 사건이 각 시간 단위마다 표본추출 되어야하기 때문에 어느정도 크기의 시스템이 되면 이의 모의 실험은 매우 많은 시간의 컴퓨팅 시간을 요하게 된다. 이 기법은 다른 방법으로는 신뢰도를 계산 할 수 없거나 다른 기법을 사용할 경우 가정을 단순화 해야하는데 이러한 가정의 단순화가 허용되지 않는 경우에 주로 사용된다. 이 기법의 단점으로는 계산에 필요한 비용이 높다는 점과 약간의 변화만 있어도 전체 모의를 다시 해야한다는 점이다.

지금까지 살펴 본 기존의 신뢰도 및 안전성 분석 기법들 중에서 각 기법의 장 단점을 고려하고 또 그 분석 결과의 효용성과 적용의 용이성 그리고 비용 측면에서 평가하여 보면 다음과 같은 기법들이 가장 적합하여 로봇 시스템의 안전성 및 신뢰도 분석에 널리 사용되고 있다[4].

- 1) 로봇의 안전성 분석 기법
 - o Fault Tree Analysis(FTA)

- o Failure Mode and Effect Analysis(FMEA)

2) 로봇의 신뢰도 분석 기법

- o Failure Mode and Effects Analysis(FMEA)

- o Fault Tree Analysis(FTA)

- o Reliability Block Diagram(RDB)

- o Combinational models(FTA와 RDB 등)

- o Markov models

- o Simulation Technique(Monte-Carlo 등)

한편 위의 방법들은 그 동안 여러 산업과 기술분야에서 널리 사용되어 왔고 그 실용성이 입증된 방법들이지만, 이들 방법들조차 최근의 로봇 시스템에는 거의 반드시 포함되어 있는 전자부분과 소프트웨어 부분, 즉 디지털 시스템 부분의 안전성과 신뢰도 분석에는 그 효용성과 정확성을 보장하지 못하고 있고, 특히 소프트웨어를 포함하는 정량적 분석에는 거의 적용하기 어려운 것이 현재의 기술 수준이다. 이 디지털 시스템의 신뢰도와 안전성 분석기술 분야의 연구는 원자력 분야를 포함해서 군수, 화학, 운수 산업 등 여러 분야에서 현재 활발히 진행중이며 Advanced Markov 모델, Bayesian Belief Ntes과 같은 새로운 기법들이 각 분야에서 연구되고 있고 시험적으로 적용되고 있다.

제 3 장 로봇 시스템의 특성

제 1 절 고장의 특징과 메카니즘

기존의 여러 가지 신뢰도 및 안전성 분석 기법들 중에서 로봇의 신뢰도와 안전성 분석에 적합한 기법들을 선정하기 위해서는 로봇 시스템의 특성 및 고장 메카니즘을 고려해야 한다. 로봇 시스템의 신뢰도 및 안전성 분석시 다른 시스템과 차별되는 특징을 살펴보면 다음과 같다[1].

- 로봇은 다른 장비에 비해 보다 많은 자유도와 넓은 작업 범위를 가진다.
- 로봇의 동작은 하드웨어와 소프트웨어의 상호 작용이 다른 기기에 비해 상대적으로 높고 그 영향이 큰데 이것은 로봇 시스템의 고장 확률을 높인다.
- 로봇의 설계 제작 기술은 빠른 속도로 발전하고 있지만 신뢰도 분석기술은 로봇의 설계 분야에서 주된 개념으로 정착하지 못하고 있기 때문에 로봇의 설계 제작과 신뢰도 구현에는 괴리가 있는 상태이다.
- 로봇이 적용되는 분야는 다른 장비가 사용되는 분야에 비해 서로 다른 형태의 다양한 에너지원(source)이 존재한다 - kinetic, chemical, thermal, electrical, laser, X-ray 등.

또한 로봇 시스템은 매우 다양한 기능을 수행하고 또 여러 형태의 복잡한 구성품으로 만들어져 있으며 그 구조 또한 매우 복잡하다. 대부분의 로봇은 기계적인 부분, 수압을 사용하는 부분, 공기압을 사용하는 부분, 전자 부분 그리고 제어 소프트웨어 부분들을 포함하고 있고 이들 다양한 부분들은 다양한 형태의 고장 원인과 메커니즘을 만들어낸다. 일반적으로 로봇 시스템의 고장 범주는 다음과 같이 나타낼 수 있다.

- 구조적 이상으로 인한 고장
- 기술적 이상으로 인한 고장
- 행위적 이상으로 인한 고장

구조적 고장은 온도나 압력 등의 변화에 영향을 받기 쉬운 재질로부터 주로 발생하고, 기술적 고장은 구성 부품의 랜덤 고장이나 하드웨어의 설계 결함 그

리고 소프트웨어의 결함에서 주로 기인한다. 그리고 행위적 고장은 운전이나 유지보수 중에 일어나는 인적 오류로부터 발생한다. 따라서 로봇의 신뢰도 분석은 체계적인 방법을 통하여 위에서 기술한 여러 고장 가능성과 관련된 잠재적인 설계상의 취약점을 밝혀내야 하는데 여기에는 로봇이 잘못될 수 있는 모든 경우와 각 고장 모드의 원인, 각 고장 모드가 로봇 시스템의 신뢰도에 미치는 영향 그리고 각 고장 모드의 발생 가능 확률을 고려해야 한다.

실례로 일본 로봇 산업계에서 발표된 로봇의 사고 원인들과 전체 사고에서 각 각이 차지하는 비율을 보면 다음과 같다[17].

- o incorrect action by the robot during manual operation (16.6%)
- o incorrect movement of peripheral equipment during teaching or testing(16.6%)
- o erroneous movement of the robot during teaching or testing(16.6%)
- o incorrect movement during checking, regulation, and repair(16.6%)
- o sudden entry of the human to the robot area(11.2%)
- o incorrect movement of peripheral equipment during normal operations(5.6%)
- o erroneous movement of robot during normal operations(5.6%)
- o others (11.2%)

한편 General Motors Corporation에서 보고된 로봇 사고의 원인은 다음과 같다.

- o The presence of an authorized person in the robot operating enclosure
- o The robot operating enclosure may simply be defined as the utmost operating boundaries of the robot, including any attachments to the robot or its arm
- o Workers were not vigilant to adjacent robots.
- o People with authorization ignorant of the robot program's ramifications

로봇 시스템의 부정확한 동작이나 고장으로 인해 원자력 발전소에 생길 수 있

는 피해는 여러 가지 요인에 의하는데 중요한 것들은 발전소 환경, 로봇의 형태 (stationary or mobile), 작업대상 기기/시설에 가해지는 로봇의 힘 등으로 이로 인한 위험 범주들을 다음과 같다[19][21].

- o Fire
- o Flooding
- o Release of poison or radioactive material
- o Electrical harm
- o Loss of plant control
- o Damage to plant structure

또한 General Motors에서 발견한 예방 가능한 로봇 사고의 특성들은 다음과 같다.

- o no effort was spent to plan the task
- o there was no anticipation of the injury
- o there was no development of specific safeguard methods
- o the injured workers himself took initiatives to rectify the situation

제 2 절 안전성/신뢰도 향상 방안

제 1 절에서 살펴본 바와 같이 로봇 시스템의 고장과 사고의 원인은 매우 복잡하고 다양하다. 따라서 이와같은 로봇 시스템의 안전성과 신뢰도를 향상시키기 위해서는 다음과 같은 사항이 요구된다.

1. 안전성 문제 해결 방안

로봇 시스템의 안전성 문제를 해결하기 위해서는 다음과 같은 사항이 고려되어야 한다[1][25].

- o 로봇의 신뢰도를 향상시킨다.
- o 기계적 부분과 하드웨어 부분의 설계를 개선한다.
- o 로봇의 유지보수와 운전 그리고 시험에 관련된 요원들에 대하여 적절한

안전 교육을 제공한다.

- 로봇의 상태에 대한 효과적인 지각적 감지 능력 개발한다.
- 모든 로봇 동작 단계에 안전 소프트웨어 제어를 포함시킨다.
- 인간/로봇 워크스테이션 배치에 적절한 인간 공학적 요인을 고려한다.
- 로봇 시스템의 설계 단계에서 적절한 인간 공학적 요소를 고려한다.

2. 설계 및 제작상의 요구사항

로봇 시스템은 기계적 부분과 제어 부분이 함께하는 매우 복잡한 시스템이다. 따라서 로봇의 신뢰도와 안전성 분석시에는 기계적 부분, 제어 부분, 그리고 시스템 전체에 대하여 고려되어야 한다. 신뢰도와 안전성 분석에는 시스템의 요구사항이 그 기본이 되는데 각 부분별 그리고 전체 시스템에서의 요구사항을 보면 다음과 같다[18][24].

가. 기계적 부분에 대한 요구사항

- 작업 대상 물체나 시설로의 로봇 경로는 명시되어야 하고 이 경우 매니퓰레이터의 동작 범위가 고려되어야 한다. 그리고 매니퓰레이터의 동작 범위와 경로는 반드시 제한 되어야 하며 동적이거나 정적인 힘에 의해 매니퓰레이터가 작업 범위를 벗어나는 것을 방지하는 구조적 요소가 반드시 설계어야 한다.
- 매니퓰레이터 드라이브 기능은 정해진 특정 작업을 하기에 충분한 힘을 제공할 수 있을 정도가 되어야 하지만 로봇의 제어나 기계적 부분의 고장으로 인해 작업 대상 기기를 파손할 정도로 강하지 않게 해야 한다.
- 여러 가지 형태의 작업 대상 기기나 설비에 대하여 각각에 맞는 전용 매니퓰레이터를 개발해야 하며 다목적(all-purpose) 매니퓰레이터의 사용은 실증이 되어야 한다.

나. 제어 부분에 대한 요구사항

- 제어 시스템은 프로그램 기반의 제어와 원격 수동 제어 둘다 가능해야 한다. 그리고 각 프로그램 주기의 초기화는 오퍼레이터에 의해서 수행 되어야 한다.
- 작업 대상 시설/장비나 로봇 자체의 rigging 고장을 방지하기 위해 그리고 제어 시스템의 고장 방지를 위해 그 상태가 감시 가능한 적합한

인터록을 제공해야 한다.

- 어떤 한 모드의 운전을 위해 제공된 인터록은 다른 모드의 운전을 방지해야 하고 한 모드에서 다른 모드로의 임의적 변경이 허용되어서는 안 된다.
- 제어 시스템은 자체 진단기능을 가지고 있어야 한다. 설계상의 어떤 기능이 제대로 수행되지 않을 가능성이 보이면 로봇 시스템의 동작을 멈추게 하는 신호가 자동적으로 발생되어야 하며 해당되는 메시지가 오퍼레이터에게 전해져야 한다.
- 제어 시스템은 다음과 같은 정보를 오퍼레이터에게 제공하여야 한다.
 - 운전 모드
 - 매니퓰레이터의 동작 준비 상태
 - 인터록 운전
 - 고장 경보
- 제어 시스템은 운전원의 명령에 의해 동작하는 비상정지 장치를 가지고 있어야 한다. 그리고 비상정지 장치가 동작하면 로봇은 그 동작을 멈추어야 한다. 또한 반복된 로봇의 초기화는 오퍼레이터 명령에 의해서만 가능하도록 해야 한다. 또하나의 중요한 점은 로봇의 정지로 인해 작업 대상 장비/시설이 위험한 상태로 가는 것을 간과하지 말아야 하는 점이다. 비상정지 기능의 구현에는 이 경우를 예상한 우선순위가 정해져야 한다.

다. 종합 및 일반적 요구사항

- 로봇은 원자력발전소에서 일어날 가능성이 있는 외부적 상황(예: 지진)을 고려하여 설계 및 제작하여야 한다. 그런 외부적 상황이 일어날 경우 로봇 시스템이 원자력발전소의 장비/시설의 고장 원인이 되거나 또는 비상상태로 가게하는 원인이 되어서는 안된다.
- Electromagnetic interference나 방사선 영향을 고려해야 한다. (예: 제어 부분의 전자기기나 부품들)
- 로봇의 설계 및 제작 재질들은 방사능 오염(decontamination)이 가능하도록 해야한다.
- 고 방사능에 의한 로봇 시스템의 고장을 고려해야 한다.

제 4 장 원자력 환경

제 1 절. 개요

원자력 산업에서는 초기부터 원격제어 매니퓰레이터가 사용되어 왔다. 그리고 최근에는 더욱 진보된 형태의 로봇을 사용한 원격 작업들이 수행되고 있는데 로봇의 기계적인 장치인 매니퓰레이터 부분은 그 속성상 방사선에 내구력이 있는 것으로 알려져 있어 별 문제가 없지만 진보된 로봇에는 대부분 포함되어 있는 선센서 드라이버 그리고 전자회로등은 방사선에 매우 민감하여 원자력분야 특히 방사선 구역에서 작업을 수행하는 로봇의 신뢰성을 확보하기 위해서는 이 부분에 대하여 설계 및 제작상의 주의가 요구된다[8]. 그리고 원자력분야에서 사용되는 로봇 시스템은 대부분 원격 제어라는 특징이 있다[22]. 일반 산업용 로봇 시스템 특히 대량생산 공정에 사용되는 로봇 시스템의 경우에는 신뢰도 및 안전성 분석의 주안점은 작업자를 위험에서 보호하는 것과 로봇 기술의 유용성을 최대화하는데 있고 따라서 로봇이 다루는 대상(상품이나 기기 등)에 대해서는 큰 비중을 두지 않는다. 반면 원자로 검사에 사용되는 로봇은 원격으로 조종되고 동작되며 그 로봇이 다루는 기기가 매우 중요하고 고가이므로 신뢰도 및 안전성 분석의 주안점은 로봇 동작의 안전성과 정확성에 큰 비중을 두게 된다. 즉 검사 대상 기기인 원자로의 잠재적인 손상 가능성과 그 결과가 가장 중요한 요인이 된다. 다음 제 2절과 제 3절에서는 로봇이 운전되는 원자력 환경의 특수성 중에서 타 산업 분야와 가장 구별되는 방사선과 신뢰도 분석에 대해 기술하였다.

제 2 절. 방사능에 의해 영향을 받는 로봇 구성부품

과거의 단순한 기능을 수행하던 로봇 시스템과는 달리 고도의 기능을 가진 현대의 로봇 시스템은 매우 다양한 부품들로 복잡하게 구성되어 있다. 이러한 최근의 로봇 시스템을 구성하는 부품들은 다음의 세가지 범주로 구분하여 볼 수 있다[9][28].

○ 드라이버

electrical actuators with bearings, gear boxes,
position feedback devices

- o sensors

- distance and force sensors, viewing systems, microphones

- o cables and other communication devices

- line driver, multiplexing circuits, analog to digital converters,
radio links, preamplifiers for sensors

이들 부품에 대한 방사선 내구성은 그들이 위치와 사용빈도에 의해 결정되고 전체 시스템의 신뢰도가 방사선에 의해 받는 영향은 다음의 세가지 항목을 고려해야 한다.

- o 전체 시스템의 신뢰도에 얼마나 치명적인 영향을 미치는가

- o 부품 열화는 어떤 형태로 나타나는가

- (sudden failure or progressive failure)

- o 해당 부품의 방사선 내구도는 어느정도인가

일반적으로 현대의 로봇을 구성하고 있는 각 서브 시스템에 영향을 미치는 방사선 열화 내용을 보면 다음과 같다.

1. Drive mechanisms

방사선에 의해서 전기 모터의 성능이 저하되거나 고장이 나는 메카니즘은 다음과 같은 것들이 있다

<직접적 영향에 의한 것>

- o loss of insulation in the motor coils or in the connection wires
- o embrittlement of the connections
- o hardening of the lubricant in the bearings and gear boxes
- o degradation of the commutation electronics

<간접적 영향에 의한 것>

- o gamma heating causing too high an internal temperature
- o halogen release from polymeric materials and lubricants inside the motor leading to the corrosion of critical parts

모터는 매니퓰레이터의 가장 중요한 구성품이므로 이의 고장은 joint의 고장으로 연결되고 따라서 전체 로봇 시스템의 동작 고장을 유발한다. 그래서 fail-safe 브레이크와 기어상자의 풀기 기능은 시스템에 반드시 필요한 안전 기능으로 간주되고 있다. 이 부분에 대한 고 신뢰도 보장을 위해서는 다음과 같은 설계, 제작상의 요구가 필요하다.

- o use of radiation hardened motors
- o use of radiation hardened cables for coils and leads
- o use of radiation hardened lubricants in the bearings
(or grease free bearings)
- o careful design of the connections to remove any source of fatigue
- o no electronics should be located at the motor level

프로토 타입 시스템에 대해 실험을 한 결과 수십 Megagray 피폭량까지 안전하게 동작할 수 있다는 결과가 나와있다.(ref-Rohrbacher, Radiation and temperature hardened components for in-vessel handling equipment, 18th Symp. Fusion Tech. 1994) 그리고 고장 양상은 어느 순간에 기능을 상실하는 돌발 형태가 대부분이었고 주 원인은 고온에 의한 열화후 연결 상태가 나빠지는 것으로 나타났다. 한편 점진적인 lubricant 열화와 급작스런 엔코딩 결함들은 시스템의 비 정상적 동작으로 나타나게 된다.

2. 일반적 센서들

센서 시스템은 고 기능을 갖춘 컴퓨터 제어시스템에서 핵심적이고 중요한 역할을 담당하고 있고 특히 원격제어의 경우 오퍼레이터와 제어 시스템에 필수 불가결한 요소이다. 이들 센서 시스템이 사용되는 용도는 장애물의 발견, 목표 대상물 탐지, 접촉 상태 측정등 시스템의 기본 기능을 위한 것과 장비의 충돌 방지와 같은 안전 기능을 위한 것이 대부분이다. 최근의 진보된 로봇 시스템에는 smart sensor라고 불리우는 자체에 신호처리 기능을 가진 센서 시스템이 많다. 이들은 그 기능과 크기 등에서 장점이 많지만 견고하며 passive한 형태의 트랜스듀서가 적합한 원자력 분야의 적용에는 문제점이 많아 그 적용에는 주의가 요구된다.

3. 거리 센서(Distance sensors)

거리 측정을 위해서 사용되는 트랜스듀서의 대표적인 것은 다음의 세 종류이다[10].

(1) electromagnetic for short distances

와전류 측정에 기반을 둔 센서의 경우 적절하게 설계된다면 20MGy 까지 사용될 수 있다. 미세한 decalibration만이 필요하고 갑작스런 센서 시스템의 고장은 주로 연결상태의 결함에서 발견된다. 짧은 거리의 측정에 사용되며 safety limit 스위치로도 사용된다. capacitive 효과를 사용한 센서는 주로 충돌 회피용으로 사용된다. 이 센서 타입의 방사선 내구성을 높이는 연구가 진행되고 있기는 하지만 아직까지는 방사선 환경에서 동작하는 기판이나 전단 전자기기에서의 사용은 제한되어 있다.

(2) ultrasonic for large distance and wide angular coverage

장거리 측정용으로 매니퓰레이터를 원하는 위치에 가져가는 경우 등에 사용된다. 주된 장점은 각도와 거리에 있어서 넓은 범위를 가지는 점으로 장애물과 목표 물체의 탐지에 적합하다. 1% 이내의 오차로 정확도를 가지고 있으나 공기나 온도와 같은 환경 요인들을 잘 고려해야 한다. capacitive membrane 형태 (angular coverage 30 deg.)와 piezoelectric crystal 형태 (angular coverage 10 deg.)의 두가지 설계 형태의 트랜스듀서가 원자력분야에서 주로 사용된다. 두 형태 모두 10 MGy까지의 감마선 피폭량에 견딜수 있다. 가장 큰 장점은 방사선에 대한 내구성이다.

(3) optical systems for accurate angular resolution

정확한 각도 측정이 가능하지만 대상 물체의 표면상태에 대해 매우 민감하고 주요 활용분야 중 하나는 근접 충돌 방지용이다. 방사선 환경에서 사용될 경우 이 센서를 구성하는 light emitter와 receiver가 방사선에 의해 열화되는 정도가 매우 높으므로 전체적 성능 저하가 생긴다. 내 방사선용으로 만들어진 제품의 경우에도 방사선 열화 효과를 완전히 없앨수는 없고 단지 그 열화 속도를 감소시키는 정도이다.

4. Force sensors

force 센서는 매니퓰레이터의 팔에 장치되어 힘의 강약을 조절하는 부분에 정확한 신호를 제공하거나, force control 또는 매니퓰레이터나 도구에 과한 부담이 걸리는 것을 방지하는데 사용된다. 모든 이 형태의 센서는 변형을 측정하는 방법을 사용하는데 방사선에 대한 내구도가 강해서 원자로 운전 중에 원자로 내부에서 사용된 경우도 있다. 내방사선 타입의 strain gauge, load cells, 6축 force/torque 센서의 경우를 실험한 결과 1MGy까지 decalibration 효과없이 잘 동작하는 것으로 나타났다.

5. Viewing systems

원거리 관찰은 원격 조종에서는 필수적인 사항이지만 카메라와 같이 이 기능을 담당하는 장비는 방사선에 매우 취약하다. 방사선에 민감한 부분들은 다음과 같다.

- o optical elements: lenses
- o drive mechanism: pan/tilt, focus, zoom
- o image sensors: tube, CCD
- o image transport system: prisms, periscope, optical fibre bundle or cables
- o front end equipments: scan circuit, power supply

카메라는 일반적으로 방사선이 약한 부분에 위치하는데 이런 경우 상용 CCD를 사용해도 무방하다. 반면 어떤 경우는 카메라가 매니퓰레이터의 끝에 부착되어 매우 많은 양의 방사선에 노출되는 경우도 있다. 이런 용도를 위해 방사선에 내구성이 있는 특수한 카메라도 일부 회사에서 제작하고 있지만 이들 조차 10-100 Gy가 한계이다. 또한 이들 내방사선 카메라들 조차도 방사선에 계속 노출되어 있으면 화질이 저하된다. 이와 관련된 신뢰도 문제는 운전원이 이렇게 방사선에 의해 저하된 화질을 통해 작업하면서 비정상적인 사건들을 간과하는 것으로 이에 대한 주의가 필요하다.

6. Audio feedback

로봇의 원격 운전에는 있어서 audio feedback은 매우 중요한 역할을 하고 있다

고 보고되었다. (Horne, Advanced teleoperator development at CERN, BNES Conference on Remote Techniques for Nuclear Plants, 1993)

CERN에서 MANTIS라는 시스템을 이용해 작업을 한 경험에 의하면 force reflexing 없이 audio feedback 기능만을 가지고 매우 복잡한 작업을 수행할 수 있었다고 한다. audio feedback을 위해서는 마이크로폰이 주로 사용된다. 이 마이크로폰을 이용해서 로봇이 작업하는 장소의 주위 소리나 또는 매니퓰레이터 접단부분이 대상 물체와 접촉하는 소리를 들을 수 있다. 마이크로폰은 capacitive/piezoelectric 센서의 일종으로 초음파 센서의 제작과 비슷하게 만들어진다. 상용 마이크로폰에 대한 내 방사선 데이터는 현재까지는 문헌상에 나타나바가 없지만 매우 높은 피폭수준까지 무난히 사용 가능할 것으로 보여진다.

7. Communication systems

원격 조종되는 장비에서 신뢰성과 관련하여 가장 치명적인 부분 중 하나가 control station과 on-board 부품간의 연결이라는 것이 그 동안의 경험으로부터 알려져 있다. 이는 전기나 공기압에 의한 서비스 부분과 신호 선 모두에게 해당된다. 전체 로봇 시스템의 신뢰도에 중대한 영향을 주는 다음과 같은 것을 생각할 수 있다.

- 많은 케이블을 가지고 있는 이동 시스템의 관리상 어려움
- 케이블에 따른 많은 connector가 존재하고 이들 중 일부는 방수와 같은 특수한 상황을 처리해야 함
- multiplexing이나 무선을 이용한 해결 방법은 전자회로의 내 방사능 문제를 야기 시킴
- 트랜스듀서와 신호처리 장비간의 원거리는 신호/잡음 비를 높이고 이는 다시 A/D 변환, 조화된 line driver, front-end preamplification과 같은 문제를 야기시킴
- 케이블에 의해 시스템에 추가적으로 기계적 스트레스가 생김

8. Electrical cables and connectors

원자력발전소 환경하의 케이블 수명에 대한 경험은 많이 축적되어 있다[11]. 그런데 현재 사용중인 대부분의 케이블은 polymeric insulation 기반으로 되어 있고 이들 케이블은 저 방사선 구역에 주로 설치되어 있다. 원자로 근처나 내부

에 사용되는 케이블은 주로 mineral insulation 형태이며 최근에는 방사선에 대해 내구성성이 높은 polymeric insulation 타입의 제품도 나오고 있다. 방사선 환경에서 나타날 수 있는 케이블과 커넥터의 신뢰성 관련 사항을 보면 다음과 같다.

- 매니퓰레이터의 작업수행 부분에 부착된 센서나 actuators 에 연결된 케이블의 경우 방사선 피폭량이 많고 또 bending stress가 높다.
- PVC나 PE와 같은 polymeric insulation 형태의 케이블은 방사선에 매우 취약하여 낮은 레벨의 피폭에도 그 전기적, 기계적 속성이 저하된다.
- 방사선에 대해 저항력이 높은 Radox(polyolefin), PEEK(polyetherketone), Kapton(polyimide) 재질은 유연성이 적은 단단한 타입이기 때문에 커넥터에 상당한 부담을 준다.
- polymeric 재질의 케이블은 방사선에 의해 halogen 가스 누출과 같은 화학적 문제를 야기시킬 수도 있다.
- 경험에 의하면 전기 소켓은 고장을 일으킬 정도로 부식될 수도 있다.
- PEEK 타입의 커넥터는 10MGy 및 섭씨 120도 환경에서 전기적 기계적 특성을 잃지 않고 정상적으로 작동되는 것이 알려졌다.

한편, 위와같은 방사선에 의한 영향 말고도 케이블과 커넥터의 신뢰성에 중대한 영향을 주는 것은 적절하게 마운트하는 것과 과도한 부담과 진동으로부터 방지하는 일이다.

9. 신호전송 전자기기(Electronics for signal communications)

전자 기기는 일반적으로 방사선 구역 밖에 위치하는 것이 일반적이지만 현대의 원격 조종 고기능 로봇 시스템의 경우 이들 전자 기기가 방사능이 존재하는 장소에서 동작중인 매니퓰레이터 내부에 위치하는 경우도 많다. 매니퓰레이터 내부의 on-board 신호처리, front-end preamplification, A/D 변환, 광통신의 경우 on-board optoelectronics, mobile 로봇의 경우 마이크로 프로세서와 메모리를 포함하는 각종 통신용 전자기기 등이 이에 해당한다. 이런 기기를 방사선에 의한 열화로부터 방지하기 위해서는 다음과 같은 방법이 주로 사용된다.

- 각 기기들의 기능적 특성을 파악하여 방사선에 영향을 적게 받도록 특수한

설계를 한다. 이 방법에 의해 설계된 전자기판을 이용한 디지털 스위치 운전이 6MGy에서도 가능한 것으로 나타났다[12].

- 각 부품의 제조과정에서 내방사선 기능은 주로 insulation 기법을 사용하여 이루어진다. 우주에서의 사용을 주 목적으로 개발된 내 방사선 CMOS는 1 - 10 kGy까지 사용 가능한 것으로 나타났다[13].
- 10kGy을 초과하는 경우는 SOI(Silicon on Insulation)과 GaAs(gallium arsenide)가 유력하다. 최근의 실험 결과는 위의 두가지 방법에 의해 만들어진 제품은 1MGy까지 사용 가능한 것으로 나타났다[14][15].

위와 같은 방법에 더하여 전자기기의 신뢰성과 관련되어 가장 중요한 점은 열화 행동의 정확한 이해와 그에 적합한 방지 대책이다.

위에서 언급한 서브 시스템들의 방사선 환경에서의 사용 한계 예는 다음 표-4와 같다[8].

표-4. Limit of usability for subsystems

Sub-system	Limit(MGy)
Drive mechanisms	10
Distance sensors	20
Force sensors	1
Viewing systems	1
Audio feedback	1
Electrical cables and connectors	10
Electronics for signal communications	1

제 3 절 부품 고장에 미치는 방사선 영향 모델링

사용시 방사능 환경에 위치하게 되는 부품의 신뢰도 데이터는 방사능에 의한 영향을 고려하지 않고 계산된 신뢰도 데이터와 다르게 취급되어야 한다. 일반적으로 방사선 열화 요인 (radiation degradation factor) Δ 는 다음과 같이 정의된다[16].

$$\Delta = \begin{cases} (P_0 - P_t)/(P_0 - P_f) & \text{for } P_0 \geq P_t < P_f \text{ or } P_0 \leq P_t < P_f \\ 0 & \text{for } P_0 > P_t > P_f \text{ or } P_0 < P_t < P_f \\ 1 & \text{for } P_0 > P_t > P_f \text{ or } P_0 < P_t < P_f \end{cases}$$

where,

P_0 = value of a characteristic parameter(e.g., the modulus of elasticity of a polymer) before exposure

P_t = value of the characteristic parameter after a total radiation dose D_t

P_f = value of the characteristic parameter at failure

파라미터 값은 해당 부품이나 서브 시스템의 radiation degradation function 으로부터 추정되는데 radiation degradation function은 부품의 특정 재질이나 형태상 특성이 방사선 피폭량이 증가함에 따라 어떻게 변화하는가를 나타낸다. radiation degradation function은 일반적으로 두가지 형태가 있다. 부품의 신뢰도 데이터 상에서 P_f 만 가능할 경우는 단순 형태인 그림-3과 같은 함수가 사용 되고 P_t 의 값이 구해질 경우에는 그림-4와 같은 piece-wise linear radiation degradation function이 사용될수 있다.

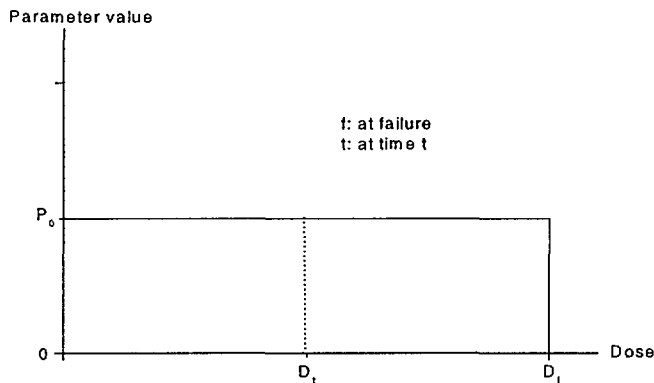


그림-3. Simple radiation degradation function

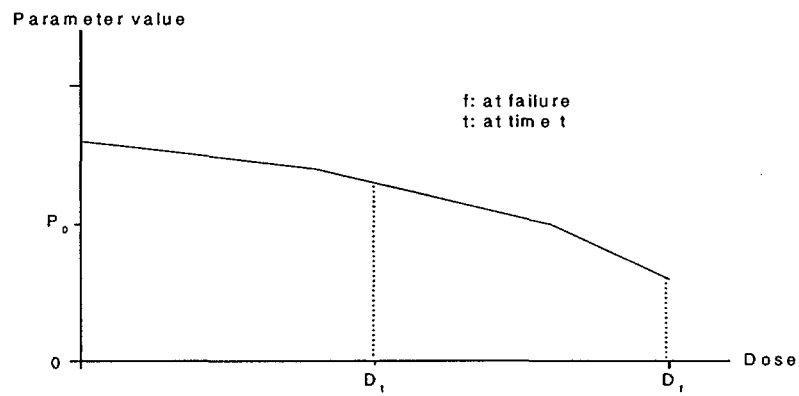


그림-4. Piece-wise linear radiation degradation function

제 5 장 외국의 로봇시스템 신뢰도/안전성 분석사례

제 1 절 개요

원자력 분야에 사용된 로봇들은 대부분 방사성 물질의 취급과 원자력발전소의 감시 및 운전에 사용되었다. 본 장에서는 그들 중 대표적인 로봇 시스템들에 대하여 시스템의 개요와 사용된 신뢰도 및 안전성 분석 기법 그리고 분석상의 특징을 중심으로 요약하였다. 조사된 대상 시스템은 다음과 같다.

- o Remote Reconnaissance Vehicle(RRV)
- o Remote Work Vehicle(RWV)
- o Weigh and Leak Check System(WALS)
- o INGRID
- o ROBUG III
- o Gripper
- o Waste Retrieval Manipulator

제 2 절 사례

1. Remote Reconnaissance Vehicle(RRV) [5]

가. 시스템 개요

Carnegie Mellon 대학에서 개발하여 미국의 원자력발전소 TMI-2의 Clean up project에 투입되었다. 원자로 건물에서 사용되어야 하기 때문에 방수 및 방사능 오염 방지에 대한 설계가 되었고 6개의 모터로 구동되는 바퀴를 가지고 있다. 주요 임무는 video/radiation survey, sampling of concrete walls, sludge deposit washdown of structures 이다.

나. 신뢰도 분석 기법

FTA와 FMEA가 사용되었다. 정점 사건으로 “RRV irretrievable”이 정의 되었고 이것은 그 원인이 되는 다음의 세 개의 서브 카테고리 고장으로 구성되었다.

- o Loss of hoisting capability for retrieval from the Reactor Building(RB) basement
- o Loss of drive force
- o Loss of systems required for operator remote guidance

이들 서브 카테고리는 다시 더 세부 사건들로 쪼갰는데 “Loss of drive force”의 경우를 보면 각 부품의 고장, 오일 공급 고장, 연결 고장 등과 같은 수준까지 나누어졌다. FMEA는 bottom up 방식으로 수행되었는데 RRV의 기본 구성부품 고장을 가정하고 RRV의 회수 불능에 영향을 미치는 효과를 분석하였다.

다. 특징

분석 결과를 근거로 하여 신뢰도 개선 전략이 개발되었다. 이 전략은 redundancy, diversity, 그리고 assurance의 세가지 전제를 포함하고 있고 이 전제를 사용하여 다수의 설계 개선 권고안이 작성되었다. 세 개의 권고안은

“Highly recommended”, “Recommended”, “Marginally recommended”로 나누어졌는데 그 분류 기준은 다음과 같다.

(1) Highly recommended

설계의 변경이 상대적으로 용이하며 신뢰도 개선에 있어서 그 효과가 현저한 항목

(2) Recommended

신뢰도 개선에 효과가 현저하나 설계의 변경에 많은 시간과 비용이 요구되는 항목

(3) Marginally recommended

설계의 변경에 많은 시간과 비용이 요구되나 신뢰도 개선 효과는 미미한 항목

RRV의 경우 “highly recommended” 항목만이 실제로 구현 되었으며 그 주요 내용은 다음과 같다.

- o 전체 시스템에 큰 영향을 주는 부품 리스트를 기초로하여 pre-mission check list를 개발하고 구현할 것.
- Pre-mission check list에는

- . structural integrity of upper boom support columns and light assembly,
 - . leak tightness of electronics enclosure and O-rings seals,
 - . connectors to each camera and light, hydraulic pumps and filters,
 - . wheel bolts, tether cable, idle roller for tether cable and capstan,
 - . hydraulic hoses and fittings,
 - . hydraulic fluid level,
 - . boom hose track assembly,
 - . boom tip assembly,
 - . camera and light functions,
 - . reservoir nitrogen pressure,
 - . on-board sensors,
 - . telemetry diagnostics on console monitor가 포함되어 있다.
- o Implement a procedural constraints that requires retrieval of the RRV upon recognition of a failure of one of the identified redundant components
 - o Practice returning to the hoist location without the tether retrieval capability
 - o conduct an environmental test of the RRV by storage in and appropriate environment and inspect selected components

2. Remote Work Vehicle(RWV)[5]

가. 시스템 개요

RRV와 마찬가지로 미국의 원자력발전소 TMI-2에서 사용되어 졌으며 Carnegie Mellon 대학에서 제작되었다. RRV보다 더욱 진보된 형태의 로봇으로 원자로 건물 내부의 장비나 설비 철거 및 파괴와 같이 RRV 수행 임무보다 더 실질적인 임무 수행을 목적으로 설계되었고 원격 조종과 전자 수압방식이며 무게는 5톤이 넘는다. 정밀 움직임은 4개의 바퀴에 의해 조종되었고 모듈화 및 오염 방지가 설계에 반영되었다.

나. 신뢰도 분석 기법

시간과 자원의 제약 때문에 FTA만 수행되었다. RRV보다 훨씬 복잡하고 큰 로봇이었기 때문에 두 개의 정점사건의 정의 되었는데 “RWV irretrievable”과 “RWV fails to complete mission”이다. “RWV irretrievable”은 RWV를 원자로 건물 베이스먼트에서 지상 레벨로 회수하지 못하는 것이고 “RWV fails to complete mission”은 RWV가 고장이나 수선없이 정해진 시간동안 정해진 특정 임무를 완수하는데 실패하는 것으로 정의되었다. 정점 사건 “RWV irretrievable”에 대한 수목 구성은 RRV와 유사하고 “RWV fails to complete mission”은 :

- . Loss of steering capability,
- . loss of propulsion capability,
- . loss of hydraulic power source,
- . RMS telemetry systems fails,
- . tether management system fails,
- . loss of boom control,
- . loss of stiffleg control,
- . loss of video system,
- . master control arm fails,
- . slave control arm fails,
- . loss of graphics display로 구성되었다.

다. 특징

분석 결과에 의거 RRV와 마찬가지로 3가지 등급의 권고 사항을 도출하였고 그 중 “Highly recommended”, “Recommended” 사항을 구현하였다. RRV의 “Highly recommended”에 포함된 사항을 대부분 그대로 포함하였으며 이 외에 filter bypass line의 단일 고장으로부터 오는 영향을 최소화 하기 위해 hydraulic 시스템의 구성이 재설계 되었다.

3. WALs(Weigh and Leak Check System)[6][20]

가. 시스템 개요

WALS는 그 당시 수작업으로 진행되던 미국 Department of Energy(DOE) Pantex

시설의 무기에 사용된 원자력 물질의 처리과정을 자동화하기 위한 로봇 시스템으로 Sandia National Lab.에서 개발되었다. 시스템은 track-mounted Fanuc Model S-700 로봇과 수대의 워크스테이션으로 구성되었는데 한 워크스테이션은 원자력 물질이 부착된 고정물체의 조립 및 해체를 담당하고 다른 두 개의 워크스테이션은 무게와 누설 체크를 감시하는 기능을 담당한다. 그리고 또 다른 워크스테이션은 수동 검사를 위해 사용되었다.

나. 안전성 분석 기법

미국 원자력발전소 내의 모든 설비는 그 안전성이 증명되어야 하고 WALs의 경우 그 요구사항은 DOE Order 5480.23를 기준으로 했다. DOE Order 5480.23에 의하면 안전성 분석은 정량적 분석이 요구되었으나, 예외적으로 원자로 시설이 아니고 그 위험도가 현저히 낮은 경우에는 정성적 안전성평가를 인정하고 있었기 때문에 WALs는 FMEA를 기반으로 하는 평가를 수행했다.

다. 특징

시스템의 안전성 분석에 있어서 로봇의 동적 특성을 고려한 방법론을 개발하여 적용했다. 기존의 안전성 평가 기법들은 정적 상태를 모델링하기 때문에 로봇과 같이 동적 특성이 강한 시스템에 그대로 적용할 경우 대부분 문제가 프로젝트에서 허용한 자원을 초과하는 한계점이 있다. WALs의 안전성 분석에서는 이 문제점을 해결하기 위해 로봇의 전체 과정을 관리가능한 로직의 스텝으로 세분한 다음 각 스텝에 대하여 독립적으로 FMEA를 적용하여 분석을 수행하였다. 그리고 안전성 분석 결과를 설계에 반영하여 재설계하는 방식으로 시스템의 명세와 위험도 레벨이 모두 당초 계획된 수준을 만족할 때까지 반복하여 수행하였다. 그리고 분석에 사용된 고장 데이터는 로봇 제작자로부터 입수했으며 이 데이터는 테스트 프로그램에 의해서 생성된 것이 아니고 WALs와 비슷한 환경에서 사용된 로봇에 대한 서비스 콜에 기준하여 작성된 것을 사용했다.

4. INGRID(Intelligent Nuclear Gantry Robot Integrated Demonstrator)

[7]

가. 시스템 개요

EC가 수행하는 Teleman Phase II 프로그램의 5개 프로젝트 중 하나에서 만들

어졌으며 원자력 산업에서 사용할 진보된 원격조종 로봇 기술을 실현하는 것이 주 목적이며 British Nuclear Fuel Sellafield 사이트에 설치되었다. 재처리 공장이나 고 방사능이 존재하는 지역에서 사용될 수 있도록 설계되었고 7축의 개조된 Puma robot이다. 개발된 시스템의 주요 내용은 로봇의 임무를 계획하고 자동으로 수행하는 원격 조종 워크스테이션을 구현하는 것이다. 수행해야 할 수개의 시나리오를 정의하고 이들 연속된 사건들에 대해 방사능 영향을 고려한 신뢰도 분석을 수행하였다.

나. 신뢰도 분석 기법

신뢰도 모델은 4개의 시나리오와 하나의 사건으로 구성되었고 그 내용은 다음과 같다.

- o Inspection, Cutting and Welding of Pipe
- o Dismantling of the constant volume feeder
- o Decontamination of calciner surface and tray
- o Removal of heavy components
- o Loss of robot(event)

이들 시나리오와 사건들은 연속된 task들을 포함하고 있다. 검토와 분석이 용이한 모델을 만들기 위해 이 task들은 다시 연속된 elementary task들로 분해되고 모듈화 되었다. 그리고 elementary task들은 관련된 센서 시스템과 도구들 그리고 다른 정보들과 결합되어 시나리오 task들을 정의하도록 만들어졌다. 시나리오 분해 예는 표-5와 같다.

표-5. Scenario decomposition with elementary task specification

Scenario task description	Elementary task no.	Additional features		
		sensor type no.	Tool type no.	Other no.
Position nut runner	3.1	3		
Operate nut runner	3.3	10	16	
Stop nut runner	3.5	5		
Remove nut runner	3.1	10		
Change tool	1.2	1-+22	17	

다음 단계는 각 elementary task에 포함될 장비들을 확인하는 과정인데 여기에는 소프트웨어와 오퍼레이터를 포함한다. 텔레오퍼레이터 모드인 예는 표-6과 같다. 최종적인 모델의 구축은 각 elementary task들에 대해 정점사건(top event)을 정의한 다음 이의 원인이 되는 각 사건들로 고장수목(fault tree)를 구성하는 것으로 이루어진다.

표-6. Equipment requirements for elementary tasks. Teleoperator mode

Equipment/Personnel		Elementary task				
Text	Model top event no.	3.1 Manual tool positioning	3.2 Jib operation	3.3 Tool task	3.4 Move robot away	3.5 Stop tool operation
RHWS, TOM	5002	X	X	X	X	X
RS, HTC	5010	X	-	X	X	X
GS	5011	-	X	-	X	-
Joint ctr.	5054	X	-	X	X	X
NEATER	5058	X	-	X	X	X
robot operator	various	X	X	X	X	X

INGRID 고장수목은 모두 212개의 기본 사건들과 143개의 gate로 구성되었다. 한편 정량적 분석을 위해 필요한 신뢰도 데이터는 다음과 같이 구해졌다.

- (1) 표준화된 부품 또는 표준화된 부품과 유사한 부품

- o IEEE STd 500-1984, IEEE Guide to collection and presentation of electrical, electronic, sensing component and mechanical equipment reliability data for nuclear power generating stations, IEEE
- o Handbood of reliability data for electronic components, RDF 93, CNET, 1993
- o Smith, D.J., Reliability, Maintainability and Risk Practical Methods for Engineers, Oxford, 1993
- o FARADIP.THREE, Failure Rate Data in perspective, Failure rates, Failure Modes and Failure Mode and Effent package, Technis, UK, 1994
- o Guidelines for Process Equipment Reliability Data with Data tables, Center for Chemical Process Safety of the Americal Institute of Chemical Engineers, 1989

(2) 프로토타입 부품

부품의 신뢰도 데이터를 구하기 힘들어서 전문가의 판단에 의거하여 추정하였다. 예를 들면, 많은 부품을 포함하고 있는 전자장비의 고장율은 부품의 개수와 각 부품의 평균 고장율에 의거하여 구한다음 각 범주별 고장율을 표-7에서 보는 것처럼 적용하였다.

표-7. Failure rates for equipment categrois

Category No.	No. of components	Average no. of comp.	Failure rate(h ⁻¹)
1	1 - 10	5	4*10 ⁻⁷
2	11 - 50	30	2*10 ⁻⁶
3	51 - 300	175	1* 10 ⁻⁵
4	301 - 1000	650	5*10 ⁻⁵

다. 특징

전통적인 신뢰도 분석 방법과 마찬가지로 발생 확률에 의거 cut set이 작성되고 정점 사건의 전체 확률이 계산되었다. 그러나 신뢰도분석에 사용된 각 부품 데이터에 불확실성이 많았기 때문에 정점 사건의 전체확률에 대해서는 큰 비중이 두어지지 않았다. 대신 cut set 리스트들은 시스템의 고장에 중대한 영향을

미치는 요인들을 확인하고 설계 개선을 주안점을 찾는데 사용되었다. “Failure of Inspection, Cutting and Welding of Pipe”의 cut set list 예는 표-8과 같다.

표-8. Top event: Failure of Inspection, Cutting and Welding of Pipe

Cut Set(Basic event)	Probability of occurrence
Operator error in the operation: tool task	0.1
Operator error in the operation: Tools into rack	0.1
Operator error in teleoperator mode by jib operation	0.1
Gripper unit failure	$0.3 * 10^{-02}$
Gantry subsystem controller software failure	$0.5 * 10^{-03}$
HTC software failure	$0.5 * 10^{-03}$
Semi autonomous Controller software failure	$0.5 * 10^{-03}$
Sensor support unit software failure	$0.5 * 10^{-03}$
Sensor support system failure	$0.5 * 10^{-03}$
Auxiliary hoist drum cable or hook failure	$0.5 * 10^{-03}$

이 표에서 나타난 것처럼 operator error가 전체 시스템 고장에 미치는 영향이 매우 크게 나타났다. INGRID 분석 팀은 이 operator error의 신뢰도 수치가 어느정도 과대하게 추정되었다고 인정하고 있지만 그것을 고려하더라도 다른 요인들에 비하면 이 시스템의 신뢰도에 가장 큰 영향을 미친다고 평가하고 있다. 그리고 소프트웨어의 고장에 대해서는 이 표에 나타난 수치에 불확실성이 매우 많다고 인정하고 있다. 방사선에 의한 신뢰도 영향 평가에 있어서는 시스템의 운전시간인 2000시간 동안의 누적 피폭량을 최저 예상치와 최대 예상치로 나누고 또 피폭 지역을 6개의 구역으로 나누어 각 경우별로 분석하였다. 분석 결과는 표-9와 같다.

표-9. Top event: Failure of Inspection, Cutting and Welding of pipe

Cut set(basic event)	Relative radiation	
	Low dose case	High dose case
Force torque sensor unit failure	0.18	1.00
Force sensor unit failure	0.18	1.00
1 of 8 optical fibre heads failure	0.17	1.00
1 of 4 electronic modules failure	0.00	0.00

그리고 분석 결과에 따른 설계 권고 사항은 다음과 같다.

(1) Cut set list중에서 방사능에 의한 열화 영향이 조금이라도 있는 부분에 대해서는 설계시 특별한 주의를 기울여야 한다.

(2) 방사선에 의한 피해를 줄이는 방법으로 다음의 세가지가 가능하다.

(가) make the equipment tolerant

Semiconductor electronics와 같이 방사능에 강한 버전의 부품이 있는 경우 사용한다. 하지만 이들 내 방사성 부품은 값이 비싸다는 단점이 있다.

(나) reduce doses

방사선 구역에 들어갈 때 오염 제거를 하거나 또는 방사선 구역에서 보다 그 영향이 적은 장소를 준비해 장비를 그곳에 위치하게 하는 방법이다.

(다) replace the equipment in time before it fails

장비의 상태 감시나 dose monitoring을 통해서 적절한 시점에 장비를 교체하는 방법이다.

5. ROBUG III [8]

가. 시스템 개요

영국 Portsmouth 대학과 PORTECH에 의해 개발되었으며 발에 흡착판이 부착되어 있어서 벽을 오르거나 천장을 타고 다닐 수 있게 설계되었다. 방사능 구역, 제한 구역, 접근이 어려운 구역에서 감시, 정비, 수리 임무를 수행하는 기능을 가지고 있다.

나. 신뢰도 분석 기법

ROBUG III은 8개의 다리를 제어하고 복잡한 기능을 수행해야 하기 때문에 방사선에 취약한 전자부품과 기타 부품들이 많이 사용되었고 따라서 신뢰도 분석은 방사선에 의한 고장과 방사선에 의해 시스템이 고장날 때 까지의 예상 시간의 추정에 초점이 두어졌다. ROBUG의 작업 시간은 100 시간이고 감마선 누적 피폭량은 1000 Gy/h로 설정되었다. 그리고 정점 사건으로는 다음의 4가지 경우가 선정되었다.

- o Failure of more than 3 legs
(max. 2 legs on the same side of the robot)
- o Loss of communication with the robot
- o Navigation failure
- o Foot adhesion failure

위의 정점 사건의 구성은 시스템이 본래 의도된 기능을 제대로 수행하는 것 뿐 아니라 로봇을 방사선 지역에서 잃게 되는 위험을 검사하는데에도 초점이 두어졌다. 이 두가지는 서로 밀접하게 관련되어 있어서 설계된 기능대로 시스템이 적절하게 동작될 경우에는 로봇의 상실 위험도 줄어든다. ROBUG III의 고장수목에는 643개의 기본사건과 270여개의 게이트가 사용되었다.

나. 특징

INGRID 시스템의 분석 결과와 마찬가지로 cut set listing이 작성되었다. 그리고 완전하지는 않지만 INGRID 시스템 보다는 더 확신된 값을 가진 정점 사건의 확률값이 계산되었다. 표-10은 “Failure of ROBUG communication with the robot” 정점 사건에 대한 cut set list이다.

표-10. Top event : Failure of ROBUG communication system

Cut Set (basic event)	Prpbability
graphic workstation software failure	2.50E-04
graphic workstation hardware failure	2.50E-04
control computer software failure	2.50E-04
control computer hardware failure	2.50E-04
communication cable failure	1.40E-05
umbilical supply cable failure	1.16E-05
back plane supply cable failure	7.60E-06
rectifier-stabilizer failure	6.20E-06
graphic workstation communication failure	2.60E-06
control computer communication card failure	2.60E-06
back plane pcb failure	4.00E-07
U8 chip LM393 failure	1.60E-07
Total probability	0.1049E-02

제어 소프트웨어의 신뢰도는 소프트웨어의 신뢰도 분석 기술이 미비한 관계로 해당 소프트웨어가 설치되어 운영되는 하드웨어와 동일한 값이 사용되었다.

6. The Gripper[7]

가. 시스템 개요

Advanced gripper라는 명칭의 이 시스템은 로봇 시스템의 일부를 구성하는 서브 시스템으로 네델란드의 Delft 대학에서 개발되었다. 이 시스템은 회전하는 손가락들과 screwdriver 등을 조작할 수 있는 “active palm”으로 구성되어 있다. 손가락들과 active palm은 전자모터와 수압으로 구동된다. 이런 기능을 가진 서브 시스템은 많은 로봇 시스템에 포함되어 있으며 또 방사능 구역에서 작업할 경우 이 부분이 방사능이 가장 강한 부분에 위치하기 때문에 신뢰도 분석은 전통적 신뢰도 분석보다는 radiation tolerance 부분에 치중되었다.

나. 신뢰도 분석 기법

Gripper를 구성하고 있는 부품과 hydraulic, electronic 시스템 그리고 제어 시스템 일부가 분석 대상이 되었고 소프트웨어와 오퍼레이터 고장은 제외되었

다. 이 gripper는 전체 커다란 로봇의 일부분이기 때문에 “Loss of equipment in radiation area”는 고려하지 않아도 되었고 주어진 임무 즉 정확한 위치로 이동해서 처리할 대상을 적절한 압력으로 잡는 것과 같은 기능적 측면이 분석되었다. 이를 위해 Fault Tree Analysis가 사용되었고 189개의 기본 사건과 83개의 gate로 고장수목이 구성되었다.

다. 특징

Gripper를 구성하는 부품의 대부분이 프로토타입 제품이었기 때문에 신뢰도 계산에 필요한 데이터를 구하는 것이 불가능했고 따라서 대부분의 데이터는 전문가의 판단에 의거하여 작성되었다. 운전시간은 8시간, 장비는 “not-repairable”로 설정되었다. 정점 사건 “Failure of normal gripper function”의 cut set list의 일부는 표-11과 같다

표-11. Cut set list of top event: Failure of normal gripper function

Cut Set	Probability
Actuator unit finger 1 link 2 motion failure	4.80E-04
Actuator unit finger 1 link 1 motion failure	4.80E-04
Pancake rotation motor, finger 1 failure	4.80E-04
Rotation gear, finger 1 failure	3.20E-04
Sensor controller unit failure	2.80E-04
Wire for force sensor finger 1 failure	1.60E-04
Pancake rotation motor finger 1 failure	1.60E-04
Force sensor finger 1 failure	1.44E-04
Pump motor finger 1 link 1 failure	1.20E-04
Gear, pump motor finger 1 link 1 failure	8.00E-05
Mechanics, finger 1 link 1 failure	8.00E-05
Rotation mechanism, finger 1 failure	5.60E-05
Pressure sensor finger 1, link 1 failure	4.80E-05
O-rings before canal 1.1, finger 1 link 1 failure	2.24E-05
O-rings of actuator finger 1, link 1 failure	2.24E-05
Current sensor finger 1, link 2 failure	8.00E-06
Hydraulic pump finger 1, link 1 failure	8.00E-06
Rotation position sensors finger 1 failure	6.40E-06
Hydraulic hose, finger 1 link 1 failure	4.80E-06
Actuator unit finger 1 link 1 pressure failure	2.24E-06
O-rings finger 1 link 1 sliding failure	8.00E-07
Pump position sensor with finger 1, etc	2.56E-08
Motor axis position sensor with finger 1, etc	2.56E-08
Total probability	1.22E-02

방사선 효과의 계산에 있어서는 운전시간 2000 시간에 해당하는 피폭량 200 kGy와 운전시간 10,000 시간에 해당하는 피폭량 1MGy의 경우에 대해 수행하였다. 결과 방사선에 가장 민감한 영향을 받는 부분은 hydraulic hose와 O-ring들로 나타났지만 이들조차 완전히 동작 불능상태로 될 가능성은 적게 나타났다. 따라서 gripper 시스템은 정해진 조건의 환경에서는 충분한 내 방사선 상태를 유지할 수 있다고 결론지어졌다.

7. WRM(Waste Retrieval Manipulator) [26]

가. 시스템 개요

미국 Hanford 원자력 사이트에 있는 폐기물 탱크의 오염 제거를 위해 제작된 로봇시스템으로 manipulator arm-based retrieval 시스템의 일종이다. 기계적인 구성은 지상에 telescoping mast가 있고 지하에 매설된 폐기물 탱크 속으로 로봇 manipulator가 들어가게 되어있다. 그리고 manipulator의 끝에 폐기물질을 처리하는 End effector가 부착되어 있다. 제어 구조는 수개의 처리 유닛이 연결되어 구성되었는데 대표적 유닛은 다음과 같다.

- o Input device(operator interface)
- o Supervisory Computer(planning functions)
- o Subsystem controller
- o Individual Joint Controller
- o Low-level Actuator Drivers
- o Analog to Digital Converters

그리고 arm의 kinematics는 다음과 같다.

- o first joint motion - vertically down into the tank
- o rotation about the vertical axis
(rotate the arm in the tank to all directions around the tank)
- o the following joints are all in the same plane
(perpendicular to the ground)

나. 신뢰도 분석 기법

정성적 Fault Tree 분석이 수행되었고 다음의 2개 시나리오에 대해 집중적 분석이 이루어졌다.

- (1) The failure scenario of a collision with a vertical riser within the tank
- (2) The failure scenario of the inability to remove the manipulator from

the underground storage tank

또 고장 수목을 구성하는데 설정된 가정들은 다음과 같다.

- (1) The position of any risers are presumed to be reasonably accurately known
- (2) The operator is assumed to have access to a monitor with camera feed from inside the tank
- (3) The actuators are assumed to be hydraulic, driven by hydroelectric valves.
- (4) Arm/mast collision scenario is caused primarily by motion of one joint, by rotation about a horizontal axis

다. 특징

분석 결과를 설계의 개선에 사용하는데 중점을 두었다. 분석 결과 발견된 설계상의 취약점과 권고 개선사항은 다음과 같다.

- (1) redundant sensors
처음의 설계에는 센서가 하나 뿐이었으나 redundant sensor를 추가하여 로봇이 정해진 코스에서 현격하게 벗어나는 것을 방지할 수 있게 하였다.
- (2) sensor fault detection
Redundant sensor를 활용하기 위한 부분으로 잘못된 센서를 가려내고 정상 신호만을 joint controller로 보내주기 위한 것이다.
- (3) kinematic redundancy
Manipulator arm mechanism 고장에 대한 fault tolerance를 제공하기 위해 joint failure 레벨에 kinematic reconfiguration 기능이 추가되었다.
- (4) Emergency stop
로봇 arm의 동작을 오퍼레이터가 수동으로 멈추게 하는 기능이다. 로봇 팔이 장애물과 충돌하는 것을 방지하기 위해 추가되었다.
- (5) Reflex control module
소프트웨어 모듈로서 전체 제어 시스템 체계 내에서 잘못된 명령이 발생

되었는지를 검사하고 충돌이 예상되는 경우 비상 정지를 수행하는 기능을 가지고 있다.

(6) Hardware limiters

Actuator driver 기판의 하드웨어 리미트 스위치로서 특정 범위를 벗어나는 joint 동작을 방지하는 기능이다.

(7) Model-based preview

오퍼레이터가 로봇에게 실제 작업 명령을 내리기 전에 미리 계획된 동작을 검토할 수 있게 하는 기능이다. 카메라 등을 활용하여 알려지지 않은 장애물 등 작업 환경의 모델을 업데이트 할 수 있게 한다.

(8) Heartbeat monitor

각 프로세서의 상태를 주기적으로 감시하는 모듈이다. 시스템 내의 각 프로세서가 정해진 실시간 일정에 따라 정확하게 동작하고 있는지를 감시하는 기능을 수행하며 과도한 작업일정이나 비정상적 시스템 정지로 프로세서가 응답을 하지 않게 되는 경우 이를 감지하여 잘못된 데이터가 시스템 전체로 퍼져 나가는 것을 방지한다.

(9) Communication network redundancy

매니퓰레이터 제어와 감시를 수행하는 모든 주요 프로세서간에 통신용 이중 버스 및 케이블 설치가 권고되었다. communication network이 고장날 경우 back-up 용이다.

(10) Fail-safe brakes

Dual redundant power hardware unit으로 구성된 fail-safe 브레이크이다. power-on release 방식이기 때문에 전원이 고장나면 자동으로 브레이크가 걸리게 되도록 설계되었다. 이 브레이크는 수동 비상 정지나 자동 emergency shutdown(ESD) 신호(로봇 제어기, watchdog computer, reflex control에서 나오는 신호)로서 동작된다.

위의 모든 분석 및 권고사항은 정성적 분석에 의한 것이다. 시스템의 정량적 분석은 로봇에 관한 신뢰할만한 고장률 또는 신뢰도 데이터가 없는 관계로 수행되지 않았다.

제 6 장 결 론

시스템의 신뢰도와 안전성 분석에 관련된 기존의 여러 가지 기법들을 조사하고 실제로 로봇의 안전성과 신뢰도 분석에 적용된 사례들을 분석하였으며 이들 조사된 기법들 중에서 로봇 시스템의 신뢰도와 안전성 분석에 가장 적합한 기법들을 선정하였다. 그리고 로봇 시스템이 가지는 특성들과 원자력발전소라는 특수한 환경에서 생기는 사항들을 도출하였다. 수행된 로봇 시스템의 신뢰도와 안전성 분석 기술 현황을 요약해 보면 다음과 같다.

1. 일반적 신뢰도 및 안전성 분석 기법과 원전 로봇 시스템 분석

현재까지 문헌상에 나타난 신뢰도 및 안전성 평가 기법들은 30여 가지가 넘는다(MORT analysis, interface analysis, high potential method, fault tree analysis, FMEA, event tree analysis, critical incident technique, change analysis, audits, job safety analysis, flow analysis, sneak circuit analysis, single point failure analysis hazard analysis, networks login analysis, energy analysis 등). 그러나 이들 기법들 중에서 실제 각 산업계에 사용되는 기법들은 많지가 않고 또 각 분야별 특수성에 맞추어 몇가지 방법들만이 사용되고 있다. 이들 기법들 중에서 로봇의 신뢰도와 안전성 분석에 적합한 기법들을 선정하기 위해서는 로봇 시스템의 특성 및 고장 메카니즘을 고려해야 한다. 로봇 시스템의 신뢰도 및 안전성 분석시 다른 시스템과 차별되는 특징을 살펴보면 다음과 같다.

- 보다 많은 자유도와 넓은 작업 범위
- 하드웨어와 소프트웨어의 높은 상호 작용
- 로봇 분야에서 설계, 제작기술과 신뢰도 분석기술의 괴리
- 로봇 적용 환경에 존재하는 양한 에너지원(source)

또한 원자력분야에서 사용되는 로봇의 경우에는 추가로 고려되어야 할 사항들이 있는데 이것은 원자력이라는 특수한 환경에 기인하는 것으로 다음과 같은 것들이 있다.

(1) 원격 제어 및 운전

일반 산업용 로봇 시스템 특히 대량생산 공정에 사용되는 로봇 시스템의 경우에는 신뢰도 및 안전성 분석의 주안점은 작업자를 위험에서 보호하는 것과 로봇 기술의 유용성을 최대한 발휘하는데 있고 따라서 로봇이 다루는 대상-상품, 기기 등-에 대해서는 큰 비중을 두지 않는다. 반면 원자로 검사에 사용되는 로봇은 원격으로 조종되고 동작되며 그 로봇이 다루는 기기가 매우 중요하고 고가이므로 신뢰도 및 안전성 분석의 주안점은 로봇 동작의 안전성과 정확성에 큰 비중을 두게 된다. 즉 검사 대상 기기인 원자로의 잠재적인 손상 가능성과 그 결과가 가장 중요한 요인이 된다.

(2) 방사능 효과

원자로 검사 로봇뿐만 아니라 원자력 분야에서 사용되는 모든 로봇을 설계할 경우 다른 분야와 차별되는 중요한 요인으로 방사능 영향이 있다. 방사능은 로봇 시스템의 신뢰도에 두 가지 측면에서 영향을 미치는데 구성 부품에 직접적으로 손상을 주는 것과 방사능 영향으로 인해 부품의 고장 확률이 높아지기 때문에 기존의 부품 신뢰도 데이터를 그대로 사용하지 못하게 되는 것이다. 최근의 로봇 시스템은 다양한 기능을 수행하며 그 성능이 높아짐에 따라 디지털 시스템이 사용되는 것이 필연적이다. 디지털 시스템을 구성하는 부품은 종래의 아날로 그 부품들에 비해 방사선에 취약한 경우가 많다고 알려져 있다.

기존의 신뢰도 및 안전성 분석 기법들 중에서 위에서 기술된 여러 가지 사항들을 고려하고 또 그 분석 결과의 효용성과 적용의 용이성 그리고 비용 측면에서 평가하여 보면 다음과 같은 기법들이 가장 적합하다.

- 로봇의 안전성 분석 기법
 - Fault Tree Analysis(FTA)
 - Failure Mode and Effect Analysis(FMEA)
- 로봇의 신뢰도 분석 기법
 - Failure Mode and Effects Analysis(FMEA)
 - Fault Tree Analysis(FTA)
 - Reliability Block Diagram(RDB)
 - Combinational models(FTA와 RDB등)
 - Markov models

- Simulation Technique(Monte-Carlo)

위의 방법들은 그 동안 여러 산업과 기술분야에서 널리 사용되어 왔고 그 실용성이 입증된 방법들이다. 그러나 이들 방법들조차 최근의 로봇 시스템에는 거의 반드시 포함되어 있는 전자부분과 소프트웨어 부분, 즉 디지털 시스템 부분의 안전성과 신뢰도 분석에는 그 효용성과 정확성을 보장하지 못하고 있고, 특히 정량적 분석에는 거의 적용하기 어려운 것이 현재의 수준이다. 이 디지털 시스템의 신뢰도와 안전성 분석기술 분야의 연구는 원자력 분야를 포함해서 군수, 화학, 운수 산업 등 여러 분야에서 현재 활발히 진행중이며 Advanced Markoc 모델, Bayesian Belief Ntes과 같은 새로운 기법들이 각 분야에서 적용 시도되고 있다.

2. 로봇의 신뢰도 및 안전성 분석 사례

원자력 분야에 사용된 로봇들은 대부분 방사성 물질의 취급과 원자력발전소의 감시 및 운전에 사용되었는데 그들 중 대표적인 로봇 시스템의 신뢰도 및 안전성 분석 사례는 다음과 같다.

(1) Remote Reconnaissance Vehicle(RRV)

- 사용된 장소 : 원자력발전소(TMI-II)
- 임무 : video/radiation survey, sampling of concrete walls, sludge deposit washdown of structures
- 신뢰도 및 안전성 분석 기법 : FTA, FMEA
- 특징 : 분석 결과에 의거 "Highly recommended", "Recommended", "Marginally recommended"의 세가지 권고 사항을 도출하였고 그 중 "Highly recommended"에 해당하는 사항들을 구현하였음.

(2) Remote Work Vehicle(RWV)

- 사용된 장소 : 원자력발전소(TMI-II)
- 임무 : RRV의 기능에 더하여 dismantling 및 demolition task in RB basement
- 신뢰도 및 안전성 분석 기법 : FTA
- 특징 : 분석 결과에 의거 RRV와 마찬가지로 3가지 등급의 권고 사항을 도출하였고 그중 "Highly recommended", "Recommended" 사항을

구현하였음.

(3) WALS

- 사용된 장소 : 군사용 핵 물질 저장소
- 임무 : check the nuclear material used in weapons for damage, leaks, weight
- 신뢰도 및 안전성 분석 기법 : FMEA
- 특징 : 시스템의 안전성 분석에 초점을 두었으며 분석 결과를 설계에 반영하여 재설계하는 방식으로 안전성 목표치를 달성하였음.

(4) INGRID

- 사용된 장소 : 원자력발전소
- 임무 : task planning, autonomous execution of various task by remote handling
- 신뢰도 및 안전성 분석 기법 : FTA
- 특징 : 일반적인 신뢰도 분석에 더하여 radiation degradation 영향에 대한 분석 항목이 추가 되었음.

(5) ROBUGIII

- 사용된 장소 : 원자력발전소
- 임무 : 사람의 접근이 어렵거나 위험한 지역에서 검사, 유비보수, 정비 업무를 수행
- 신뢰도 및 안전성 분석 기법 : FTA
- 특징 : radiation degradation에 대한 분석이 수행되었고 제어 소프트웨어의 신뢰도는 소프트웨어의 신뢰도 분석 기술이 미비한 관계로 해당 소프트웨어가 설치되어 운영되는 하드웨어와 동일한 값을 사용.

6) The Gripper

- 사용된 장소 : 원자력발전소
- 임무 : 로봇 시스템의 한 구성부분으로 인간의 손과 같은 기능을 수행
- 신뢰도 및 안전성 분석 기법 : FTA
- 특징 : 가장 방사선이 강한 곳에 위치하게 되는 부분이므로 전통적인 신뢰도 항목보다는 주로 radiation tolerance 부분에 중점을 두고 분석 되었음.

7) Waste Clean-up Manipulator

- 사용된 장소 : Nuclear Site(high-level radioactive waste storage)
- 임무 : remove, treat, dispose the wastes stored in tanks
- 신뢰도 및 안전성 분석 기법 : FTA
- 특징 : 시스템의 설계 단계에서 신뢰도 분석 기법을 적용하여 제품의 신뢰성과 안전성 개선에 활용.

위의 분석 사례에서 나타난 것처럼 원전 로봇 시스템의 신뢰도와 안전성 분석은 해당 로봇 시스템의 특성에 대한 이해와 방사선에 의한 부품 열화와 같은 원자력환경이라는 특수성의 고려에 중점을 두고 있고 분석 기법은 대부분 Fault Tree Analysis와 FMEA를 사용하고 있다. 또 로봇 시스템의 신뢰도와 안전성에 관련된 가장 중요한 요인중의 하나인 제어 소프트웨어의 분석에 대해서는 아직까지 관련 기술 수준이 미비한 관계로 적절한 분석이 수행되지 못한 것으로 나타났다. 이 소프트웨어의 신뢰도와 안전성 분석 분야는 현대의 산업 기술에서 소프트웨어가 차지하는 비중이 커짐에 따라 비단 로봇 산업분야 뿐아니라 원자력 분야와 군수, 항공 분야 등 각 분야에서 현재 활발히 진행되고 있다.

앞으로의 계획은 본 보고서에서 수행된 조사 분석 내용을 기본으로 하여 본 과제에서 개발중인 원자로 검사 장비의 로봇 서브시스템에 대한 신뢰도와 안전성 분석을 수행하여 동 원자로 검사장비의 품질 및 성능 향상에 기여하고 또 추후 검사장비의 인허가 등의 과정에 활용할 계획이다.

제 7 장 참고 문헌

1. B.S. Dhillon, Robot Reliability and Safety. Springer-Verlag, 1991
2. P.E. Clemens, "Compendium of Hazard Identification and Evaluation Techniques for System Safety Application" Hazard Prevention 2, No.2, 1982
3. Fred A. Manuele, Accident investigation and analysis, Readings in Accident Investigation: Examples of the Scope, Depth, and Source, 1984
4. B.S. Dhillon, "Safety and reliability assessment techniques in robotics" Robotica, Vol. 15, 1997
5. W.W. Weaver, "Techniques applied to improve robotic reliability", Safety aspects of nuclear power plant automation and robotics, IAEA, 1992.
6. Christopher B. Atcitty, "Safety Assessment of a robotic system handling nuclear material", Sandia National Lab. 1996
7. Kurt Lauridsen, Assessment of the reliability of robotic systems for use in radiation environments, Reliability Engineering and Systems Safety 53, 1996
8. Richard Sharp, Radiation tolerance of components and materials in nuclear robot applications", Reliability Engineering and System Safety 53, 1996
9. Rohrbacher, Radiation and temperature hardened components for in-vessel handling equipment, 18th Symp. Fusion Tech. 1994)
10. Noppe, Strain gauges in a nuclear environment, Materials and Design 14, 1993
11. Burnay, S.G., Cable life management in nuclear power plant, IAEA Specialist Meeting on Technology for lifetime management of Nuclear Power Plant, 1994
12. Leszkow, P. Radiation tolerant techniques of multiplexing analogue signals in a nuclear environment. First European Symposium on the Radiations and their Effects on Components and Systems, 1991)
13. Holmes-Siedle A. Handbook of radiation effects, Oxford University Press, 1993

14. Simoen, E., DC and low frequency characteristics of gamma irradiated gate-all-around silicon-on-insulator MOS transistors. Solid State Elect., 38, 1995
15. Hiemstra, D., Dose rate dependent 1/f noise performance of a GaAs operational amplifier. 32nd Int. Nuclear and Space Radiation Effects Conference, 1995
16. Lauridsen, Assessment of the reliability of robotic systems for use in radiation environments, RESS 53, 1996)
17. N. Sugimoto, Safety engineering on industrial robots and their draft standard safety requirements, Proceedings of the 7th International Symposium on Industrial robots, 1977
18. A.B. Pobedondostsev, The use of robots for enhancing the operational safety of nuclear power plant. USSR
19. P. Jezequel, Robots for the safety of nuclear power plant-prospects and reality. EdF, France
20. David G. Roninson, Safety assessment of high consequence robotics system. Sandia National Lab, 1996
21. Palle Christensen, Robots and Plant Safety, Risco National Lab. Denmark, 1996
22. M. Becquet, Reliability improvement of robotics systems: analysis, design and real time supervision. Institute for systems engineering and informations, EC
23. S.P. Gaskill, Safety issues in modern applications of robots. Reliability Engineering and Systems Safey 53. 1996
24. Deirdre L. Fault tolerance versus performance metrics for robot systems. Reliability Engineering and Systems Safey 53. 1996
25. I. Dassonville, Trust between man and machine in a teleoperation system. Reliability Engineering and Systems Safey 53. 1996
26. Ian D. Walker. Failure mode analysis for a hazardous waste clean-up manipulator. Reliability Engineering and Systems Safey 53. 1996

27. Koorrosh Khodabandehloo, Analysis of robot systems using fault and event trees: case studies, Reliability Engineering and Systems Safety 53, 1996
28. Coenen, The radiation resistance of force sensors used on telerobotic nuclear equipment, Proc. ANS 6th Topical Meeting on Robotics and Remote systems, 1995
29. 정환성 외, 디지털 계측기기의 확률론적 안전성 평가를 위한 하드웨어 신뢰도 예측 방법, KAERI/AR-571/2000, 2000.9.
30. Bazovsky, Reliability Analysis of Large System by Markov Techniques. Proc. Annual Reliability and Maintainability Symposium, 1993
31. Henry Ozog, Hazard Identification, analysis, and control. Hazard Prevention, 1985
32. Dan Neilson, Use of cause-consequence chart in practical systems analysis, In Theoretical and Applied Aspects of System Reliability and Safety Assessment, SIAM, 1075)

서 지 정 보 양 식					
수행기관보고서번호		위탁기관보고서번호		표준보고서번호	
KAERI/ - /					
제 목 / 부 제		원전 로봇시스템의 신뢰도 및 안전성 분석기술 현황			
연구책임자 및 부서명 (주저자)		엄홍섭 (종합안전평가팀)			
연 구 자 및 부 서 명		김재희 (종합안전평가팀), 이재철 (종합안전평가팀), 최유락 (종합안전평가팀), 문순성 (종합안전평가팀)			
출 판 지	대전	발행기관	KAERI	발행년	2000.12.
페 이 지	71 p.	도 표	있음(○), 없음()	크 기	21×29.7cm
참고사항					
비밀여부	공개(○), 대외비(), — 급비밀		보고서종류	기술현황분석보고서	
연구위탁기관				계약 번호	
초록 (15-20줄)		<p>본 과제로 개발중인 원자로 검사 장비의 품질을 향상시키고 신뢰도와 안전성을 확보하기 위해 원자력분야를 비롯한 여러 산업 분야에서 널리 사용되고 있는 시스템의 신뢰도와 안전성 분석 기법들을조사 분석 하였고 분석에 중대한 영향을 미치는 로봇 시스템의 특성, 로봇 시스템이 운전되는 원자력 환경 그리고 선진국에서 수행된 로봇 시스템의 신뢰도와 안전성 분석 사례를 수집 조사 하였다. 본 보고서의 주요 내용은:</p> <ol style="list-style-type: none"> 1. 기존의 신뢰도 및 안전성 분석 기법 조사 - 일반 산업 분야에서 인정되고 널리 사용되는 기법들을 조사하였고 그 중에서 본 과제로 개발중인 로봇 서브시스템의 분석에 적합한 기법들을 선정하였다. 선정된 기법들은 고장수목(Fault Tree Anlaysia), 고장모드 및 영향 분석법(Failure Mode and Effect Analysis), 신뢰도 블록 다이어그램(Reliability Block Diagram), Markov Model 그리고 모의 실험 기법 이다. 2. 신뢰도와 안전성 분석시 특별한 주의가 요구되는 로봇 시스템의 고장 및 사고 유형과 시스템 특성에 대한 조사 분석. 3. 로봇이 원자력 환경에서 운전될 경우 신뢰도 및 안전성 분석시 고려해야 할 요인 들인 원격 제어 및 방사선 효과에 의한 부품과 기기의 고장에 대한 조사 분석. 4. 선진 각국에서 수행된 원자력분야의 로봇 시스템에 대한 신뢰도 및 안전성 분석 사례 수집 및 분석. <p>본 보고서에서 조사된 내용과 그 분석 결과는 현재 개발 중인 원자로 검사 장비의 신뢰도와 안전성을 향상시키는데 사용될 예정이며 또한 추후에 공식적인 품질보증 및 인 허가 과정에서 필요하게 될 각종 데이터를 작성하는데 적용할 예정이다.</p>			
주제명키워드 (10단어내외)		로봇, 신뢰도, 안전성, 평가기법, 사례분석			

BIBLIOGRAPHIC INFORMATION SHEET					
Performing Org. Report No.		Sponsoring Org. Report No.		Standard Report No.	
KAERI/					
Title / Subtitle		A Survey on Reliability and Safety Analysis Techniques of Robot Systems in Nuclear Power Plants			
Project Manager and Department		H.S. Eom (Integrated Safety Assessment team)			
Researcher and Department		J.H. Kim (ISA team), J.C. Lee (ISA team), Y.R. Choi (ISA team), S.S. Moon (ISA team)			
Publication Place	Taejon	Publisher	KAERI	Publication Date	2000.12.
Page	71 p.	Ill. & Tab.	Yes(<input type="radio"/>), No (<input type="radio"/>)	Size	21 × 29.7cm
Note					
Classified	Open(<input type="radio"/>), Restricted(<input type="radio"/>), ___ Class Document		Report Type	Analysis Report	
Sponsoring Org.				Contract No.	
Abstract (15-20 Lines)		<p>The reliability and safety analysis techniques was surveyed for the purpose of overall quality improvement of reactor inspection system which is under development in our current project. The contents of this report are :</p> <ol style="list-style-type: none"> 1. Reliability and safety analysis techniques survey - Reviewed reliability and safety analysis techniques are generally accepted techniques in many industries including nuclear industry. And we selected a few techniques which are suitable for our robot system. They are falut tree analysis, failure mode and effect analysis, reliability block diagram, markov model, combinational method, and simulation method. 2. Survey on the characteristics of robot systems which are distinguished from other systems and which are important to the analysis. 3. Survey on the nuclear environmental factors which affect the reliability and safety analysis of robot system 4. Collection of the case studies of robot reliability and safety analysis which are performed in foreign countries. <p>The analysis results of this survey will be applied to the improvement of reliability and safety of our robot system and also will be used for the formal qualification and certification of our reactor inspection system.</p>			
Subject Keywords (About 10 words)		Robots, Reliability, Safety, Analysis technique, Case study			