컴퓨터기반 철도신호제어시스템의 안전성 확보에 관한 연구

論 文
53B-11-1

A Study on Safety for Computer Based Railway Signaling Control System

辛 德 浩† · 李 鍾 宇*
(Ducko SHIN · Jongwoo LEE)

Abstract - Computer system is widely used for controlling systems such as nuclear power plant, train speed control and air plane control. The failure of computerized controlling system can be arrived to catastrophic accident, so the safety ensuring of computerized controlling system is very important. This paper shows how to improve and ensure the safety of computerized systems. In this paper, we show how to identify, analyze hazards of the computerized system and to demonstrate risk of the system. Finally, we show how to adopt safety techniques for improving safety of the target system.

Key Words : Safety, Hazard, HAZOP, Risk, Computer Safety, Fail Safe

1. 서 론

안전성기술은 주로 자연재해방지를 목적으로 한 것이었지만, 산업혁명 이후 동력이 기계화됨에 따라, 인간-기계 시스템의 안전성이 새로운 문제로 대두되었다. 이 경우 안전성이란 인간의 과실 또는 기계 고장으로 인하여 인간이 위해를 입거나 혹은 장치가 파손되는 상태가 발생하지 않는 것이라고 할 수 있다[1].

IEC 61508에서는 안전에 관련된 컴퓨터기반 시스템에 대해서 시스템의 구성, 설계, 제조 및 운용의 전 단계를 통해 각 관리 면에서 안전성을 확보하기 위한, 시스템 안전성 프로그램계획 SSPP(System Safety Program Plan)를 작성하고, 시스템 라이프사이클의 모든 단계를 통해 안전성활동을 수행하도록 명시하여 제조자에게 의무화 하고있다. SSPP의 목표는 ①시스템의 목표에 적합한 안전성설계의 실시, ②위험원(hazard)의 식별, 제거 또는 허용레벨 이하로의 감소 ③새로운 재료 및 제조기술의 채용에 따른 위험의 최소화 ④과거 안전성에 관련된 데이터의 분석과 적절한 활용 등을 보증하는 것으로 되어있다[2].

현대사회는 컴퓨터를 많은 분야서 제어를 목적으로 활용하고 있으며, 특히 항공기, 원자력발전, 철도차량의 속도제어 등에 적용하고 있다. 위와 같은 응용분야에서의 컴퓨터고장은 사고를 유발할 수 있다. 예를 들면 항공기에서의 제어컴퓨터의 고장은 항공기의 손실을 초래할 수 있으며, 원자력발전에서의 제어실패는 노심의 용융과 방사선 누출로 이어질 수 있고, 철도신호에서는 열차의 충·추돌을 야기할 수 있다[3].

본 논문에서는 컴퓨터 자체의 안전성을 확보하는 방법보다는 컴퓨터를 이용한 시스템에서 컴퓨터 자체고장으로 인한 사고의 발생으로부터 어떻게 안전성을 확보하는 가에 초점을 맞추고 있다. 이제까지의 안전성의 확보는 컴퓨터의 신뢰성이 확보되면 안전성이 확보되는 것으로 간주되어 왔으나, 신뢰성의 확보는 안전성 향상에 기여 하지만, 신뢰성이 낮다고 해서 안전성이 낮은 것은 아니며 신뢰성이 낮아도 안전성이 높은 경우도 존재함을 알게 되었다.[1]

본 논문에서는 컴퓨터를 이용한 제어시스템에서의 안전성을 확보하기 위한 방법과 안전성을 확보하기 위한 목표인 시스템 안전요구사항 설정의 핵심이 되는 위험원정의 및 위험원으로 인한 사고의 정량적 평가를 통해 안전성목표를 할당하는 체계수립에 초점을 맞추었으며, 이렇게 수립된 목표달성을 위한 안전성 평가방법 그리고 이론적인 안전성 확보방법을 제시한다.

2. 사고 및 안전성 확보방법

2.1 안전성 확보기술

안전성을 확보하기 위해서 그림1과 같이 사고원인이 발생하지 못하도록 각 단계에서 적절한 대책을 강구하여 사고의 발생을 억제한다. 예를 들어 사고원인이 발생하지 않도록 결함을 제거하며, 결함이 발생하였을 경우 위험원 상태로 도달하지 않도록 결함을 표시하고, 위험원이 사고로 이어지지 않도록 안전측 작동을 유도 및 사고가 발생하였을 경우 사고의 결과가 확대되지 않도록 하는 방법과 사고 후 처리 방법을 강구하는 것 모두가 안전성기술 확보라 할 수 있다[4].

† 교신저자, 正會員 : 광운대학교 제어계측공학과 박사과정
한국철도기술연구원 주임연구원
E-mail : ducko@krri.re.kr
* 正 會 員 : 한국철도기술연구원 책임연구원
接受日字 : 2003年 8月 3日
最終完了 : 2004年 9月 8日

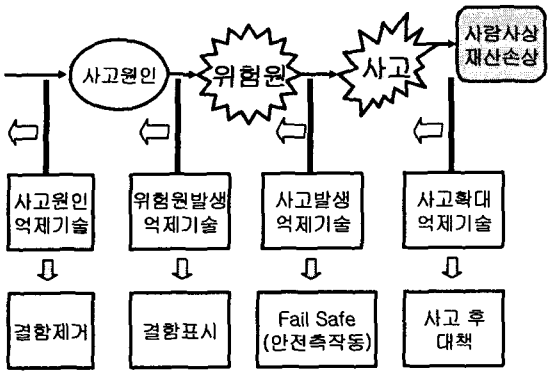

그림 1. 사고방지를 위한 안전성 적용기술
Fig 1. Countermeasure against accidents

2.2 사고발생순서

사고의 발생은 그림2에서 나타난 것과 같이 내·외부의 임의원인 발생으로 인하여 위험원(Hazard)으로 전이되고, 위험원은 다시 내·외부의 요인에 의해서 사고로 전이된다.

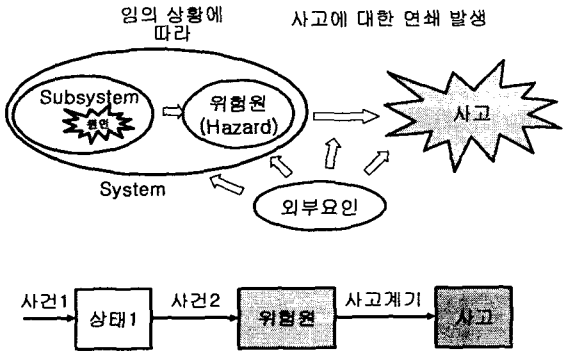

그림 2. 사고의 발생은 어떤 원인에 의해서 위험원으로 전이되고 다시 위험원은 사고로 전이된다.
Fig 2. Causes such as fault are transited to hazards and the hazard are transited to accidents

사고는 인간에 대해서는 부상, 불구가 혹은 생명을 잃게 하며, 사회적으로는 재산(의 기능)을 잃게 하는 것이다. 사고는 그림2와 같이 위험원을 발생시키는 원인과 사고를 발생시키는 위험원의 사고진전순서로 나타낼 수 있다. 사고가 발생하기 위해서 다양한 원인에 의해서 사고원인이 발생하고, 과도상태(위험원)로 전환되어 사고로 이어지게 된다. 따라서 발생된 사고에는 사고를 발생시키는 사고원인이 있다. 즉 사고가 발생되는 관계는 장치 혹은 시스템의 고장에 의해서, 위험원(Hazard) 상태로 전이되고, 다시 위험원에서 사고로 확대되어 진다.

2.3 위험원 규명 및 분석(Hazard Identification and Analysis)

2.3.1 위험원 규명

위험원의 규명은 안전성을 확보하는데 가장 기본적인 요소 중의 하나이다. 위험원이 없다면 그 위험원으로부터 기인되는 사고도 없다. 즉, 위험원 도출에 실패하면 그 위험원으로부터 기인되어 발생될 수 있는 사고를 방지할 수 없다.

위험원의 특성에서 어떤 위험원들은 사고와 유사하고, 어떤 것은 근본 원인에 가까워서, 그림3에서 나타낸 것처럼 시스템에 따라서 위험원의 위치가 달라진다. 예를 들어서 컴퓨터를 사용한 열차제어 시스템에서 "한 구역에 동시에 두 대의 열차가 있다면" 이것은 사고에 상당히 근접해 있는 것이다. 반면에 "열차 운영자간의 인터페이스(상호접촉)의 부적절한 관리"는 사고의 근본 원인에 해당한다. 이러한 문제는 원인과 사고 사이의 많은 단계에서 무수히 존재하는 변수에 의해 발생한다. 주요 손실 사고는 원인에서 사고까지의 많은 단계와 관련되며, 반면에 적은 손실은 단계가 매우 적기 때문이다.

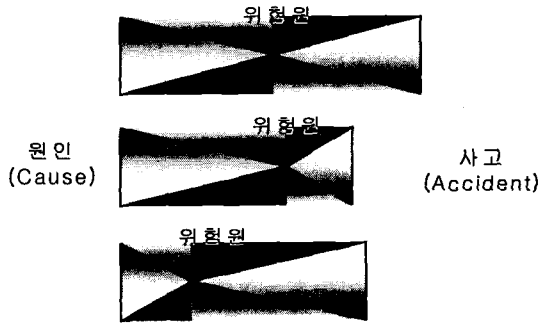

그림 3. 사고원인, 위험원 및 사고관계간의 다양한 연결관계
Fig 3. Multiple interconnection between causes, hazard and accidents

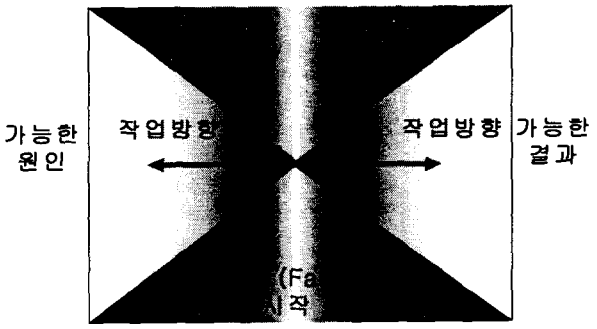

그림 4. HAZOP : 원인에서 결과로 진행하는 작업
Fig 4. HAZOP : working from the fault both forwards to possible consequences and backwards to possible causes

매우 위험도가 높은 위험원(예, 동시에 한 구역에 두 대의 열차가 존재) 하위에 해당하는 수많은 하위 위험원들을 추가시킬 수 있다.

위험원을 규명하는 방법에는 여러 가지 방법이 있다. 대표적인 방법들로는 "그렇다면 무엇이 나타나는가", 상호작용의 특별한 면을 가지고 관찰하는 "상호 매트릭스 방법", 시스템

부품간의 상호작용을 관찰하는 "부분분석", 무엇과 어떻게를 연관하여 "검사항목"을 제정하는 방법, 시스템의 기능고장과 고장의 영향을 분석하는 "FMEA" 방법 및 부품과 부품간의 상호작용을 조사하고, 설계영역에서 벗어나는 요소를 조사하며, 원인과 결과의 연관관계를 조사하는 "HAZOP : Hazard and Operability"이 있다[5][6].

위험원을 광범위하게 정의하는 것은 위험도(위험) 모형에서 실질적인 사고 결과의 손실을 가져올 수 있으며 모형화 과정에 상당히 주의하지 않으면 정확성과 이해부족의 결과를 가져온다. 특히 컴퓨터를 이용한 시스템에 대해서 부적절한 입력과 출력으로 인한 위험원은 매우 포괄적으로 정의된다.

2.3.2 HZOP(Hazard and Operability)

위험원 도출의 한가지 방법인 HAZOP은 설계목적으로부터의 결함(Fault)으로부터 시작하며, 가능한 원인을 찾기 위해 역방향으로 작업을 수행하여 결과를 알기 위해 순방향으로 작업을 진행한다.

하지만 현실적으로는 어느 방법도 위험원을 완벽하게 규명할 수 없으며, 위에서 제시된 방법을 조합하여 사용하는 것이 최상의 방법이다. HAZOP과 FMEA는 서로 다른 측면에서 위험원을 규명하는 상호보완적인 방법이다. 또한 FTA (Fault Tree Analysis)와 ETA(Event Tree Analysis)는 규명된 위험원을 분석하는데 서로 상호보완적인 관계를 갖는다.

2.3.3 위험원 분석

위험원 분석은 위험원의 발생원인을 규명하는 것으로 위험원 분석에 자주 사용되는 방법중 FTA(Fault Tree Analysis)가 있다. FTA는 부품고장으로부터 서브시스템의 조합, 하위단계의 사건 및 각각의 원인측면에서 최상위 위험원을 분석하는 방법이다[7]. 그림5는 위험원을 발생시키는 시스템의 위험원 원인분석에 대한 개념도이며, 그림6은 FTA 방법 실시 예이다.

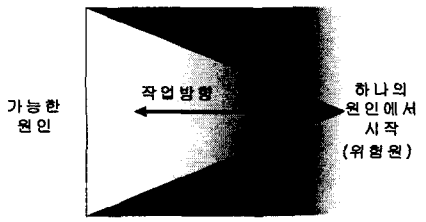

그림 5. FTA : 원인에서 결과로 진행하는 작업
Fig 5. FTA : working back from consequence to causes

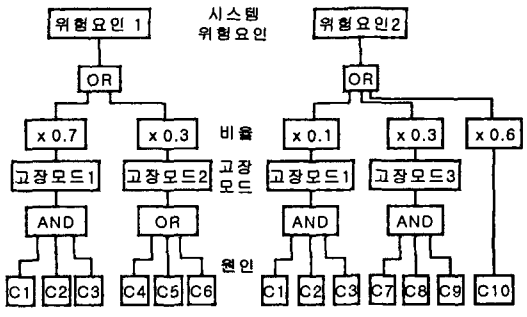

그림 6. FTA를 이용한 위험원도출 및 확률할당
Fig 6. Hazard identification and probability allocation using FTA

위험원의 원인이 되는 다양한 종류의 고장은 위험원에 연결되어 있으며, 고장모드에 따라서 발생확률을 할당한다. 그림5에서 예로든 FTA 방법은 시스템에 따라서는 대단히 복잡하고, 부분적으로 논리를 따르고 있을 뿐 전체적인 구조가 보이지 않는 경우도 있다. 따라서 복잡한 시스템의 해석을 행하기에 적합하다[7].

2.3.4 위험원의 결과

위험원에 의해 기인된 사고의 결과를 분석함에 있어서는 FMEA(Fault Mode Effect Analysis)를 사용한다. FMEA는 일반적으로 고장(Failure)모드와 그 영향으로 생각되지만, 실제로는 결함(Fault)모드와 그 결함의 영향을 검토해야 한다. 따라서 FMEA는 결함형태가 시스템에 미치는 영향을 추론하는 방법으로 그림7과 같은 개념도를 갖는다.

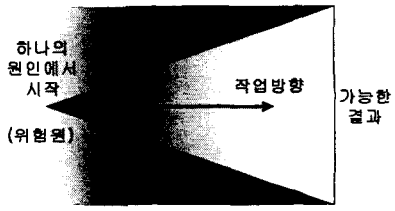

그림 7. FMEA : 원인에서 결과로 진행하는 작업
Fig 7. FMEA : Working forward from cause to possible consequence

그림 7에서 하나의 원인은 하나 혹은 다단계의 과정을 거쳐 사고로 이어지게 된다. 그림8은 철도신호시스템에서 접근구간의 조기해정을 위험원으로 가정하여 위험원이 사고결과까지 진행되는 사고 시나리오를 예로 든 것이다. 이 시나리오에서는 위험원이 다양한 서브 위험원으로 진행될 수 있으며 궁극적으로는 사고로 이어질 수 있음을 보인다. 사고 시나리오의 분석방법으로 가장 많이 사용하는 FMEA, FMECA 및 ETA가 있다.[5][7][8]

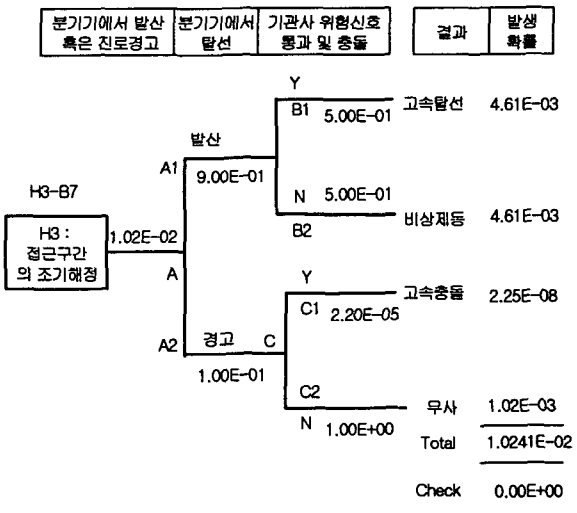

그림 8. 전자연동장치에서의 위험분석의 실제의 범례로서 사고전개사양
Fig 8. Accident scenario using real example for risk analysis to solid state interlocking system

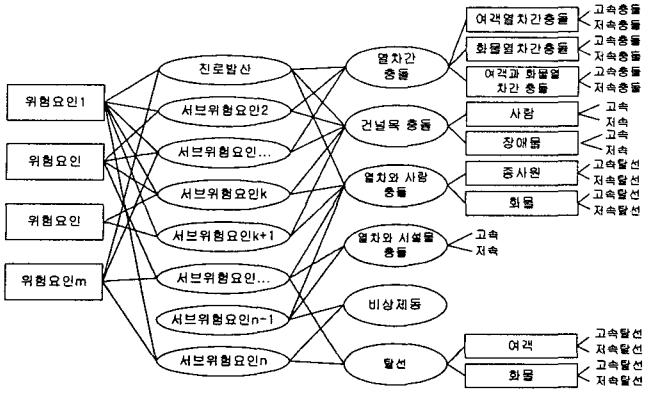

그림 9. 위험원 → 하부위험원 → 사고결과로 이어지는 그래프 형식의 사고추론 맵의 구성

Fig 9. Accidents inference diagram with a sequence : Hazard → sub hazard → consequence

그림 9는 위험원에서부터 사고까지의 다양한 경로에 따라 사고결과의 크기가 다양하게 나타날 수 있음을 보인다. 따라서 안전성확보를 위해서는 관련된 위험원에 대한 손실분석이 선행되어야 한다.

2.4 손실의 분석

철도분야에서 손실분석은 승객, 승무원, 철도원 및 공중을 대상으로 하여 추정한다. 사람의 손실분석은 사망, 장애, 부상 등으로 나누어지며, 사망은 인원수로 정의되고 장애는 치료 후 평생동안 장애를 가지고가는 경우를 의미한다.

위험도(Risk)는 특정한 위험원에 대해서 피해가 발생하는 빈도와 그 피해크기를 나타내는 지표이며, 다음과 같은 정의에 의해 정량적으로 표시된다.

- 위험도(Risk)=(발생확률) × (사고의 결과)

위험도는 정량화된 값에 따라 우선권이 설정되어 제어대책의 적용에 사용되며, 정량적으로 정의하는 것이 적합하지 않은 경우는, 발생빈도에 따라 표1과 같은 레벨로 결정한다. 발생확률과 결과의 상호개연성은 정성 및 정량적 값으로 분류될 수 있다.

예를 들어서 확률은 다음과 같이 정성 및 정량적인 값으로 분류할 수 있다.

표 1. 발생빈도의 정성적 및 정량적 분류

Table 1. Qualitative and quantitative classification for accident frequency

정성적	정량적	설명
• 자주 (Frequent)	$f > 10^{-1}$	빈번하게 발생되는 것
• 종종 (Probable)	$10^{-1} > f > 10^{-2}$	시스템 라이프타임동안 여러 회 발생되는 것
• 가끔 (Occasional)	$10^{-2} > f > 10^{-3}$	시스템 라이프타임동안에 가끔 발생할 수 있는 것
• 거의 (Remote)	$10^{-3} > f > 10^{-4}$	시스템 라이프타임동안에 가끔 발생할 가능성이 있는 것
• 없음 (Improbable)	$f < 10^{-6}$	발생할 가능성이 전혀 없는 것

10^{-4}은 평균 1년에 1회

사고의 결과는 표2와 같이 정성 및 정량적인 항목으로 분류할 수 있다.

표 2. 사고크기의 정성 및 정량적 분석

Table 2. Qualitative and quantitative analysis for accident seriousness

정성적 분석	정량적 분석	비고
• 치명 (Catastrophic)	손실비용 > 2×10^{6} USD	생명의 위험, 시스템 손실 : 다수의 사망 혹은 다수의 심각한 부상
• 심각 (Critical)	10^{6} > 손실비용 > 10^{5} USD	심각한 상처, 병, 큰 시스템 손상 : 1인 사망, 1인의 심각한 부상
• 상당 (Marginal)	10^{5} > 손실비용 > 10^{4} USD	가벼운 부상 혹은 병, 작은 시스템 손상 : 손상을 일으킬 수 있는 가능성의 내포
• 무시 (Negligible)	손실비용 < 10^{4} USD	가벼운 부상·병, 시스템 손상에 이르지 않는 것

USD = U.S. Dollar

이러한 발생활률과 발생된 사고 크기에 대한 정성 및 정량적 분석을 종합하여 표3과 같이 위험원 매트릭스를 얻을 수 있다.

표 3. 정량적인 위험도 예

Table 3. An example of quantitative risks

발생빈도	사건결과			
	치명적	심각	상당	무시가능
100~999 / 10000 년인원	1	3	7	13
10~99 / 10000 년인원	2	5	9	16
1.0~9.9 / 10000 년인원	4	6	11	18
0.10~0.99/10000 년인원	8	10	14	19
0.010~0.099/10000년인원	12	15	17	20

표 3에서 사건결과에 숫자는 위험의 순서를 나타내며, 미육군규격(System Safety Program Requirement)에서 유래한 것이다. 이 숫자는 위험평가 코드로 알려져 있으며, 각 항목에 대한 중요도와 제어의 필요성을 나타낸다.

① 위험평가코드 1~5 : 수용불가-위험도를 반드시 감소시켜야함

② 위험평가코드 6~9 : 부적정-모든 가능한 제어수단을 사용해야하며, 잠재위험도에 대한 문서화된 허용 방안을 가지고 있어야 한다.

③ 위험평가코드 10~17 : 조건부허용 - 잠재위험도에 대한 문서화된 허용 안을 가지고 승인됨

④ 위험평가코드 18~20 : 허용가능

3. 안전성확보영역

안전한가 아닌가를 결정하는 크기는 주관적, 상대적으로 정의된다. 이것을 결정하기 위한 방식으로서, ALARP(As Low As Reasonably Practicable) : "실제 적용할 수 있을 정도로 위험이 작음"모델이 있다. ALARP 모델은 그림10에서 나타내는 것처럼 작은 위험도라면 허용 가능, 큰 위험도는 허용불가, 그 중간이라면, 편익과의 균형을 생각하여 설정한다라는 모델이다. 역삼각형은 시스템에서 고려해야 하는 위험도가 높은 위치(그림10의 위쪽)에 있어서, 위험도를 정의된 위험도기준 이하로 감소시키기 위해서 소요되는 비용도 증가하게(그림10의 위쪽에서의, 삼각형의 가로방향의 증가) 된다

일반적으로 안전은 숫자로는 표시할 수 없는 것이라고 되어 있으며, 어느 정도의 레벨 이하라는 표현은 허용할 수 있다고 해도, 비용측면을 고려하여, 비용과의 균형으로 안전을 생각한다라는 것은 일반적이지 않다. 이것은 안전을 희생해서 비용을 삭감하는 경향을 엄하게 제한하기 위한 것으로서, ALARP 모델에서도 안전과 비용과의 관계를 고려하여 각 영역에서 다음과 같은 기준을 정의할 수 있다.

따라서 안전성의 구분은 허용불가영역, 위험을 다스린 영역 및 위험이 존재하지 않는 영역의 3단계로 나누며, 안전이 확보되었다는 것은 허용되는 영역이나 제어가능단계(ALARP)로 위험도가 완화되었음을 의미한다.

안전의 정도는 비용과 편익과의 관계에 따라 변한다. 즉, 안전의 정의는 상대적이며 주관적이다. 그러므로, 안전평가는 사회적인 허용범위 혹은 사회적 위험도와의 관계에 따라 달라진다.

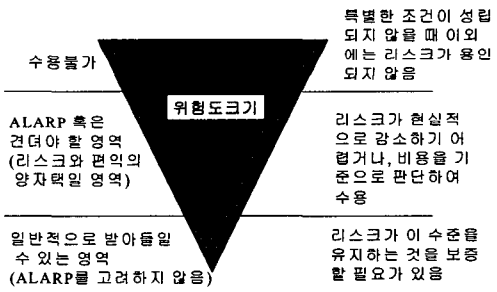

그림 10. ALARP 모델
Fig 10. ALARP Model

- 허용불가영역 : "대단히 특별한 조건이 성립했을 때 이외는, 이 위험도는 용인하지 않는다."
- ALARP영역 : "위험도가 제시된 수준 이상의 감소가 현실적으로 어렵거나 비용이 너무 소요된다고 판단되었을 때 받아들인다."
- 허용되는 영역 : "위험도가 일정 수준을 유지하는 것을 보증해 갈 필요가 있음"을 엄격히 적용한다.

4. 컴퓨터를 이용한 시스템에서의 안전성 확보방안

본 절에서는 위에서 제시한 그림11과 같은 안전성확보를 위한 체계를 바탕으로 실제 안전필수 분야에서 주어진 안전요구사항을 만족하기 위해 위험원을 완화시키는 예를 보였다.

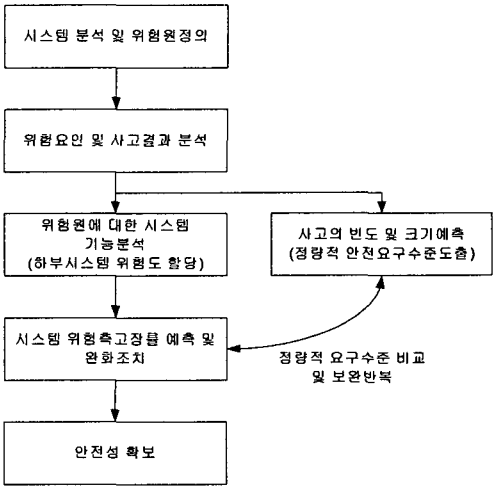

그림 11. 안전성확보를 위한 활동
Fig 11. Safety Insurance Activity

컴퓨터를 사용하는 시스템에서의 안전성 평가를 위한 예를 들면, 표4와 같이 현재 시중에서 생산되고 있는 워크스테이션의 평균고장(MTBF:Mean Time Between Failure)을 들 수 있다.[9]

표 4. 각기 다른 컴퓨터 제조자의 평균고장시간(MTBF)
Table 4. MTBF for different manufacture's computers

제조자	1 Node Workstation	1,000 Node MPP
DEC	35,872 시간	35 시간
HP	58,700 시간	58 시간
SUN	40601 시간	40 시간
NASA/IBM AP101S	20,000 시간	20 시간

표 5. 각 분야에서의 컴퓨터의 적용과 이상으로 인한 위험원과 피해결과
Table 5. Hazards and consequence from computer abnormality in different control systems

시스템	적용개소	컴퓨터적용 및 제어내용	안전한 상태	컴퓨터 위험원	시스템 위험원	위험사건 결과	피해	발생빈도	위험도
원자로	반응속도 제어	반응속도 제어	노의 반응정지	비정상 입·출력	반응속도 제어불능	방사성누출 및 오염	치명적 (1000명이상 사망가능)	3×10^{-5}/h	2
항공기	구조 설계	(해당없음)	비행유지	비정상 입·출력	상태획득 및 제어불능	추락	치명적 (1000명이하 사망가능)	1×10^{-5}/h	4
	기능 시스템	기능제어							
도로교통 제어	신호기제어	신호기제어	신호기 기능유지	비정상 입·출력	이상출력	충돌	치명적 (10명이하 사망가능)	25×10^{-5}/h	8
엘리베이터	구조 설계	(해당없음)	일정속도 초과금지	비정상 입·출력	과속운행	추락	치명적 (10명 이하사망)	5×10^{-5}/h	8
	속도 제어	속도제어							

표4에서 제시한 각 시스템을 해당분야에 적용하여 제어하는 경우에 표5와 같은 위험도를 예측할 수 있다. 컴퓨터에서 발생할 수 있는 위험원은 여러 가지가 있을 수 있으나 "비정상적인 입력과 출력"이 대표적인 위험원이다. 이 위험원을 중심으로 그림4와 같이 원인분석과 결과분석을 수행하여, 표5와 같이 "비정상적인 입력과 출력"의 위험원에 대한 간단한 위험성 분석결과를 제시하였다.

따라서 각 응용분야에서 도출된 위험도에 따라서 위험을 감소시키고 안전성을 향상시키기 위한 대책을 강구하여야 한다. 표5에 나타난 각 시스템에 사용된 컴퓨터의 고장발생빈도를 감소시킴으로써 시스템의 안전성을 향상시킬 수 있다. 표6에서는 각 시스템의 안전성을 향상시키기 위한 방법을 제시하였다. 컴퓨터에서 기인되는 위험원을 능동하드웨어 여분구조의 이중계로 설계하여 위험원을 감소시킬 수 있으며, 이 경우 2개의 컴퓨터가 동시에 고장이 발생하여 비정상 입·출력을 발생할 확률은

$$F_{failure\ rate} = \prod_{i=1}^{2} F_i$$

이므로,

$$F_{failure\ rate} = F_i^2$$

이 된다[9].

표 6은 각 시스템을 하드웨어 여분구조로 설계하여 시스템의 안전성을 향상시킨 예이다. 하드웨어 여분구조에는 결함의 검출을 위한 능동구조와 결함의 억제를 위한 수동구조로 나누어 볼 수 있으며, 이러한 구조들은 사용되는 모듈의 수와 결함의 검출 및 억제를 위한 방법에 따라 대기이중계방식, 투표기를 이용한 삼중계방식, 이중계를 동기식으로 운전하여 결함을 검출하고 결함발생시 동일한 이중계구조를 여분으로 갖는 듀얼듀플렉스 구조 등의 대표적 기술들이 있다.

본 논문에서는 위험원 완화를 위해 결함의 검출기능을 내장하는 동일구조의 단일모듈 2개로 구성된 이중계를 사용하여 동작계와 대기계에서 동시에 결함발생을 검출하지 못하는 경우에 위험출력이 발생하는 단순구조의 이중계를 제안하여 위험측고장률이 감소됨을 보였다.

표 6. 각 분야에서의 안전측과 안전확보를 위한 적용기술의 예

Table 6. Safe state and safety solution examples for different applications

시스템	안전성기술	비정상 입·출력 억제방안	대책방안	고장율	개선전 위험도	개선된 위험도
원자로	·Fail Safe ·Full Proof ·고장검지·진단	·Redundancy ·고장검치·진단	이중계	9×10^{-10} /h	2	12
항공기	·다중화 ·Fail Soft ·위험측 고장을 저감		이중계	1×10^{-10} /h	4	12
도로교통 제어	·다중화 ·Fail Soft		이중계	6.25×10^{-10} /h	8	12
엘리베이터	·안전여유율 향상 ·Back up		이중계	0.25×10^{-10} /h	8	12

5. 결 론

본 논문에서는 컴퓨터를 이용한 제어시스템에서의 안전성을 확보하기 위한 방법을 제시하였다. 컴퓨터를 이용한 시스템 혹은 그렇지 않은 시스템에서도 안전성을 확보하기 위해서는 위험원의 도출과 분석, 그 위험원에 대한 위험도 분석을 수행하여야 한다. 그 위험도에 따라서 위험도를 적정수준까지 낮추기 위해 다양한 방법을 적용한다.

본 논문에서는 간소화된 방법으로 시스템의 안전성 확보를 위한 체계를 제시하였으며, 실제 시스템 안전성을 확보하기 위한 절차는 상당히 복잡할 수 있으나 기본적인 절차는 본문에서 제시한 방법을 기본으로 수행할 수 있는 적용분야별 체계적인 위험원 도출, 분석 및 위험도 분석 방법에 대한 연구가 필요하며, 위험도를 낮추기 위한 방법에 의해, 안전이 확보되었다는 객관적 절차의 개발이 필요하다.

참 고 문 헌

[1] 鐵道總研, '安全性評價技術', 教育資料

[2] IEC, 'IEC 61508 1~6'

[3] 鐵道總研, 'コンピュ -タ 制御信號 システムの安全性·信賴性技術', 教育資料

[4] Lorna Love et al., 'Using Diagrams to Support the Analysis of System 'Failure' and Operator 'Error'', http://www.dcs.gla.ac.uk/~johnson/papers/aft.htm

[5] Felix Redmill et al. 'System Safety : HAZOP and Software HAZOP', John Wiley & Sons, 1999

[6] Defence Standard 00-58, 'HAZOP Studies on System Containing Programmable Electronics', 2000

[7] U.S. Nuclear Regulatory Commission, 'Fault Tree Handbook', 1981

[8] BS, 'Reliability of systems, equipment and components part 5. Guide to failure mode and criticality analysis', British Standard, 1991

[9] Dhiraj K. Pradhan, 'Fault-Tolerant Computer System Design', Prentice-Hill, pp135~235, 1996

저 자 소 개

신 덕 호(辛 德 浩)

1975년 4월 1일생. 1998년 광운대학교 제어계측공학과 졸업, 2000년 광운대학교 제어계측공학과 대학원 석사, 2002년 광운대학교 제어계측공학과 박사수료, 2002년-현재 한국철도기술연구원 전기신호연구본부 주임연구원

이 종 우(李 鍾 宇)

1959년 3월 20일생. 1983년 한양대학교 공과대학 기계설계과 졸업, 1986년 Ecole Centrale de Nantes 석사, 1993년 Universite de Paries VI 공학박사, 1994~현재 한국철도기술연구원 전기신호연구본부 책임연구원