기술보고

Safety Control System 개념

김덕기 (현대중공업)

1. 서 론

최근 고부가가치 선박인 LNG(Liquid Natural Gas)운반선이나 FSRU(Floating Storage Regasification Unit, 부유식저장재기화설비)와 같은 해양플랜트 프로세스 공정에는 안전장치화가 되어 있는 상태로 그 목적은 프로세스의 제어 밖의 위험을 감소시켜 안전사고 및 안전재해를 사전에 방지하고 이로 인한 운용상의 경제적 이익을 도모하기 위한 것이다.

현재 산업현장에서 안전은 그 무엇보다 중요시 되고 있고, 또한 안전과 관련된 시스템을 개발하는 산업이 발전하고 있는 실정이다.

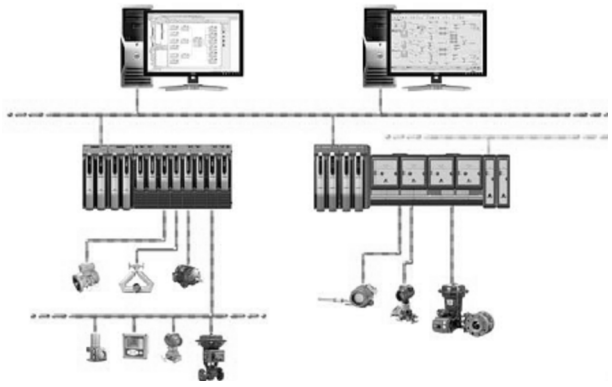

그림 1. 프로세스 제어시스템 구성도

산업 프로세스 공정에 적용되는 안전시스템의 역사를 간단히 살펴보면 1970년대 중반에는 Relay based Hardware System에서 시작하여, 1980년대 중반에는 PLC(Programmable Logic Controller) Based Control System, 1985년부터 현재까지는 Microprocessor Based Safety System 기반으로 이어지고 있다[그림1].

오늘날의 전문적인 안전시스템의 출현은 1985년부터 TMR(triple modular redundant) Based System 회사와 Diagnostic Based Redundant System 회사들이 자사의 시스템을 독일의 안전 진단 전문 기구인 TUV (Technischer Uberwashungs Vercin)로부터 인증을 획득한 후 발전하게 되었다.

2. 안전시스템(Safety System)

2.1 안전시스템이란

안전시스템은 산업현장이 위험해질 수 있거나 적절한 대응을 취하지 않을 경우 결국 위험한 상황에 직면하게 되는 상황에 대처할 수 있게 설계 되어 지는 시스템이다.

안전시스템으로는,

- Emergency Shutdown System (ESD)
- Safety Instrumented System (SIS)
- Fire & Gas Protective System (F&G)
- Process Shutdown System (PSD)
- Instrument Protective System (IPS) 등이 있다.

이전의 공정 제어에서 흔히 사용된 경보(alarm)와 안전 인터록(safety interlock) 장비들은 압력, 유량, 레벨 및 온도 스위치로 구성되어 있었다. 이 스위치들은 간단한 기계식 또는 전기기계식 기구로 위험 상황 감지 시 밸브나 모터 또는 다른 공장 장치를 작동시켜 공정을 안전 상태로 유도한다. 지금도 사용되고 있는 기계식 장비는 burst plate와 전기 퓨즈(Fuse)와 같은 물리적 힘(physical forces)을 이용하고 있다.

전기기계식이나 solid state relay의 발전은 공정의 더욱 복잡한 안전 시스템의 설계를 가능케 한다. 1960년대의 전자 분야의 발달과 더불어 fail-safe 모듈을 갖춘 Hardwired system은 공정 산업에 유연성 있고 모듈식(Modular)으로 된 시스템을 제공했다. 이 Hardwired System은 최상의 신뢰도를 갖는 고유의 fail-safe인 것이다. 그러나, 높은 신뢰도에도 불구하고 공정 제어에 사용되는 컴퓨터 근간의 시스템과 연결될 수 있는 한층 더 유연한 시스템으로의 대체가 산업계에서 요구되어 졌다. 이러한 요구가 1970년대 들어 와서 마이크로 프로세서 근간의 프로그램 가능한 안전 시스템의 출현을 가속화하였고 이 시스템은 기존 시스템과 유사한 확장성과 신뢰도 및 현대 제어시스템에서 요구 되어 지는 수월한 configuration을 제공하고 있다.

지금까지 가장 잘 알려진 안전시스템으로 보면 이중화(Dual Redundant), 삼중화(Triple Redundant) 시스템들이 있다. Redundant System의 MTTR(Mean Time to Repair, 평균

수리시간) 이나 MTBF (Mean Time Between Failure, 평균무고장시간) 가 TMR 시스템에 비하여 상대적으로 열세이었으나 2000년에는 기존의 Redundant System에서 한층 신뢰도가 높은 사중화(Quadruple Modular Redundant) 시스템이 산업현장에서 많은 호응을 얻고 있고, 산업안전에 한 차원 높은 신뢰를 줄 수 있게 되었다.

또한, 안전규정(Safety Standard)은, 산업혁명 후 국가들은 산업 플랜트에서 많은 안전사고와 인명피해를 입은 후 안전에 대한 중요성을 인식하면서 안정규정을 수립하게 되었고, 인증기관도 설립하게 되었다. 이런 안전시스템의 규정 및 인증기관을 최초로 설립한 곳이 독일의 TUV 이다[그림 2].


CERTIFICATE

No. B 05 02 55466 001

Holder of Certificate: Shenzhen Zanty Electronics Co. Ltd.
1/F C2 Building,
Jihua Industry District, Buji Town,
518112 Shenzhen
PEOPLE'S REPUBLIC OF CHINA

Production Facility(ies): 55466

Certification Mark:

Product: Electric pumps (Electromagnetic Pump)

Model(s): SDPU-4073

Parameters: Rated Input Voltage : 230 V AC 50 Hz
Rated Power Input : 17 W
Supply Connection : Quick-Connect Termination
Remark : This electromagnetic pump can only be used as a component for household appliances. All the requirements of the mentioned standard must be fulfilled when installing the pump to end product.

Tested according to: EN 60335-1/A11:2004

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. See also notes overleaf.

Test report no.: 68110405602

Date, 2005-02-18

Page 1 of 1

그림 2. TUV 인증서

TUV는 1980년대 초에 마이크로프로세서 근간의 안전 시스템에 대한 연구를 시작하여 독일 표준이 된 DIN VDE 0801, 이후 DIN V 19250의 문서를 작성하였다. 본 인증은 위험 분석에 따른 8개의 필요 등급으로 분류되어 있다. 그림 3은 DIN V19250 규정에 따른 위험도가 나타내고 있다.

IEC 61508

1996년초, ANSI/ISA가 공정 산업을 위한 안전 계기 시스템(safety instrumented systems, SIS)의 적용을 위해 세계 표준인 S84.01를 발표하였다. 100국 이상의 사용자 대표를 포함하는 S84 위원회는 사용자와 공급자가 합의하는 표준을 작성하였고 IEC도 61508 draft of international standards를 발표하였는데 이것은 여러 가지 면에서 S84.01 표준과 유사하다.

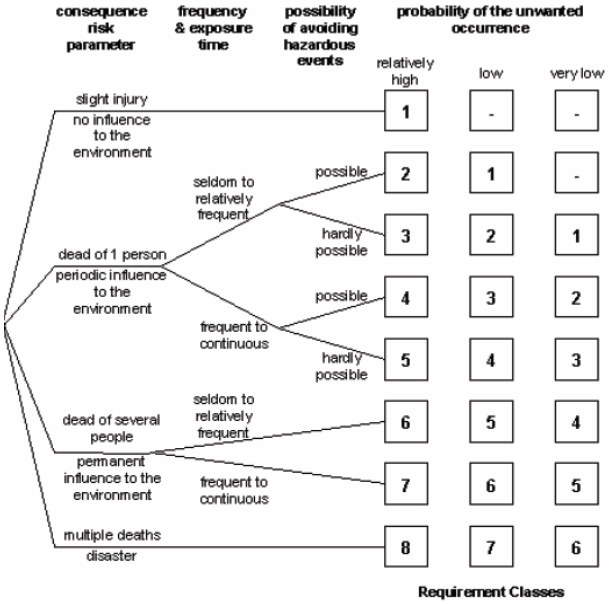

그림 3. TUV DIN V19250 규정

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

그림 4. Safety Integrity Level

이런 표준들이 안전 인식을 제고 하고 사용자들 사이에 안전시행의 표준화에 기여해 오고 있다. 미국에서는 S84.01 표준에 명기되어 있는 요구가 필수 사항 일 뿐만 아니라 OSHA-PSM 과 EPA-RMP의 좋은 엔지니어링 Practice에 의해 더 강화되고 있다.

S84.01 표준은 3개의 중요 부문으로 나뉘어진다.

- 필수 요건의 표준이 본문
- 유익한 부록
- 안전 무결 수준(safety integrity level, SIL) 분석을 위한 기술 보고

성취된 위험 분석을 분류하기 위하여 ANSI/ISA S84.01와 IEC 61508 표준은 위험 감소 요인을 4단계로 나누는 안전 무결 수준(safety integrity levels, SIL)을 명기하였다.

SIL 1 ~ SIL 4. 이 SIL은 완벽한 안전 루프 또는 안전 기능을 위하여 양적과 질적의 요구 사항을 명시한다[그림 4]. 이들

은 위험 감소 요인들이 지켜야 할 고장 가능성 기준을 제공하기도 한다. 안전 기능은 확실한 위험 감소를 이룰 수 있도록 설계되기 때문에 안전 무결 수준이 그들에게 할당될 수 있는 것이다.

2.2 Fail Safety Control System

Fail Safety Control System 은 민감하고 중요한 프로세스에 적합한 높은 신뢰성과 안정성을 갖춘 Safety System 이다. 주로 선박이나 해양플랜트 제어시스템에 적용되는 분산제어시스템(DCS, Distributed Control System) 은 Total Process Solution System의 한 제어부분으로서 중앙제어부와 신호인터페이스(Signal Interface)가 가능하고, 또한 독립적인 Stand-alone system으로도 구성이 가능하다.

Fail Safety Control System은 광범위의 안전이 요구되는 프로세스에 적용이 가능한 마이크로 프로세서기반(Microprocessor-Based) 안전시스템으로서 그 적용범위는 아래와 같다.

- High-Integrity Process Control
- Burner/Boiler Management System (BMS)
- Emergency Shutdown (ESD) system
- Fire and Gas Detection System
- Pipe and Instrumentation Monitoring System
- Process Safeguarding System, etc.

단순한 단 루프 제어기(single loop controller)와 챠트 레코더(chart Recoder)로 시작된 제어 시스템은 복잡한 분산형 제어시스템(DCS)과 PLC 근간의 시스템으로 발전되어 왔다. 이들 시스템은 공정 제어와 최적 조업뿐만 아니라 위험한 상황에 대비하는 첫 단계의 안전 장치 기능을 제공한다. 그러나, 많은 산업 현장의 공정들은 종래의 제어 시스템이 일반적으로 제공하는 것 보다 추가적인 안전 장치를 요구하고 있다. 이는 중대한 공정 변수의 감지와 위험 상황 발발 시 공정을 안전 상황으로 유도하는 기능들이다. 그 목적은 제어 불가 공정(out-of-control process)의 위험도를 사람의 안전(human safety), 환경 영향(impact on environment)과 경제적 이득을 고려하여 바람직한 수준으로 저감 시키는 것이다. 공정에서 요구되는 위험도 저감은 필수적인 제어와 안전 가동정지 시스템(safety shutdown system) 또는 안전 시스템(safety system)에 의해 가능하다. 이 시스템들은 "fail-safe" 와 "fault-tolerant" 로, 이는 한 개체의 고장이 시스템의 안전 기능에 영향을 주지 않음을 의미한다. 그림 5에 전형적인 공정의 안전보호계층이 보여 진다.

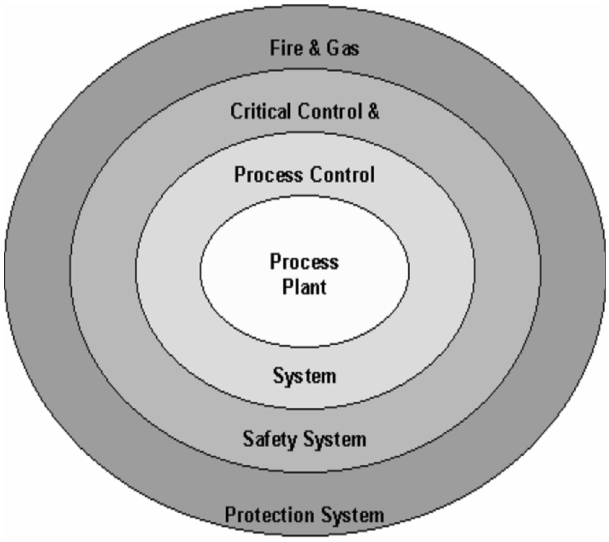

그림 5. Safety Protection Layer

이에 더하여, 안전 시스템(safety system)은 화재나 가스 누출과 같은 특정한 위험에 대해서도 보호 기능을 갖는다. 열량, 연기, 온도 및 유독 가스 농도를 계속 감시하여 이중 어느 하나라도 미리 선정된 한계를 벗어 날 경우, 안전 시스템은 경보(alarm)를 울리며 안전 상태로 유도하는 행동을 자동적으로 수행한다.

3. 안전성 (Safety)

그림 6에 AND gate의 기능적 회로도가 나타나있다 (출처: HIMA사의 Hardwired System). Fail-safe 모듈의 기능상 중요 원칙은 전자 부품 사이에 8 kHz의 주파수가 전달되어야 하는 것이다(이것은 1초에 8,000번의 자체 검사를 가능케 함). 이 주파수는 전체 부품이 정확히 작동하고 AND 조건이 충족 될 경우에만 transformer로 이동한다. 모듈내의 부품의 어떤 결함이나 현장으로부터 의 E1 또는 E2 신호 문제시 출력(A, safety state)을 de-energize 한다. 따라서 이 모듈은 본질적으로 fail-safe 하다.

최근까지는 이런 형태의 fail-safe 모듈이나 그 외 전기자장 릴레이(non-programmable systems)만이 사람의 생명이나 환경 문제가 위태로운 경우에 사용이 허용되어왔다. 마이크로프로세서 근간의 안전 시스템(programmable system)은 아무리 근소하더라도 기능장애에 따라 공장의 안전을 위태롭게 할 수 있는 가능성을 갖고 있다. 예를 들어 출력모듈의 무변화 장애 와 energized 상태에 고착된 channel등이다.

위험한 상태를 유발 가능한 고장을 극복하기 위하여 많은 시스템 벤더(Vendor)들이 이제는 CPU 검사, 입력 모듈 검사

와 출력 모듈 검사 등을 포함, 각기 자체 OS 소프트웨어에서의 포괄적인 진단 기능을 제공하고 있다.

배선시스템(hardwired system)에서 사용된 fail-safe 원리가 마이크로프로세서 근간의 안전 시스템에 이용 되어져 그 신뢰도를 높이고 있다. Fail-safe binary 출력 모듈에서, 이 fail-safe AND gate가 logic output 및 watchdog signal과 함께 사용된다. TUV RC (Requirement Class) 6의 요건을 충족하기 위해서는 두 개의 독립적인 fail-safe AND gate이 출력 모듈에 제공되어야 한다.

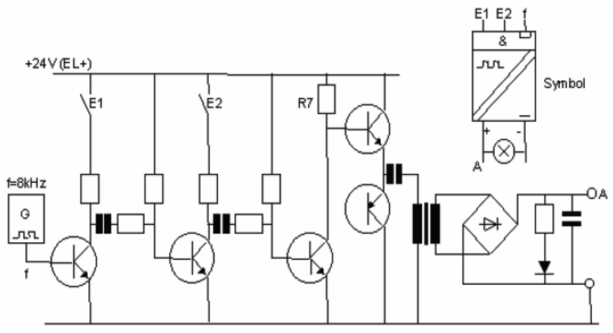

그림 6. Principle of the Fail Safety Module

PES(Programmable Electronic System)의 진간 검사에서 그 외로 중요한 관점은 안전 시간(safety time)이다. 안전 시간은 잘못된 출력 신호에 대해 공정의 안전을 위태롭게 하지 않고 운전 가능케 하는 최대 시간을 의미한다. 예를 들면, burner 제어의 안전 시간은 1s(초)이다(TRD 규정에 따른 steam vessel의 기술 규정).

따라서 각각의 단일 고장과 규정된 안전 조치(safety reaction)는 안전 시간 내에 수행되어야 한다. 이 조치 시간(reaction time)은 cycle time의 최대 2배로 규정되어 있다. 요구 되는 안전 시간이 1초일 경우 cycle time은 500 msec를 초과하면 안된다.

4. 신뢰도 (Reliability)

신뢰도(reliability)란 기기가 가동 기간 중에 그 기능을 충족시키는 능력을 의미한다. 수치화하기가 자주 까다롭다. 그래서 MTBF (Mean Time Between Failure) 라는 정의가 종종 신뢰도를 측정하는 방법으로 채택된다. 이것은 가동 중인 시스템에 의해 통계학적으로 또는 사용된 부품의 고장율로 계산된다.

신뢰도는 시스템의 안전과는 무관하다. 신뢰도가 낮은 시스템도 각 개체의 고장이나 각각의 위험 상황에 대해 공장을 안전 상태로 유도할 수 있다면 그 시스템은 안전하다고 볼 수 있기 때문이다.

EC Technical Committee에 따라 안전 시스템의 수명(life cycle) 중 고장의 원인에 대한 분류를 나타낸다[그림 7과 8].

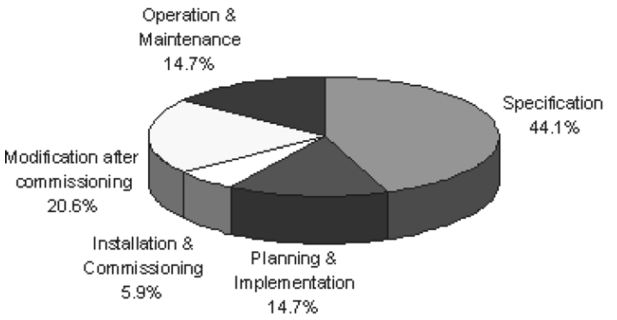

그림 7. 고장 발생 요인에 의한 분류

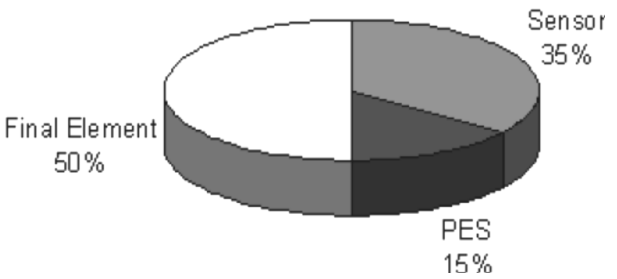

그림 8. 고장 부위에 따른 분류

5. 이용가능성 (Availability)

이용가능성(availability)은 시스템이 정상적으로 작동하는 확률이다. 이것은 MTBF(Mean Time Between Failure)와 MDT (Mean Down Time)를 이용한 다음의 식으로 표현된다:

$$V = \frac{MTBF}{MTBF + MDT} \times 100\%$$

MDT (Mean Down Time)는 고장 감지 시간(fault detection time)과 모듈 시스템의 경우 장애 모듈 교체에 필요한 시간으로 구성된다. 따라서 시스템의 이용가능성은 MDT가 짧아짐에 따라 크게 증가 된다. 현대 PES에서의 빠른 고장 감지는 자동 검사기능과 상세한 진단 환면으로 가능하다.

이용가능성은 이중화(redundancy) 또는 삼중화(triplicated)로 증가 될 수 있다. 예를 들면 중앙 장치는 병렬로 하고 I/O 모듈은 이중화하며 측정 장소에 여러 개의 센서를 설치하는 것이다.

단일 시스템의 MTBF가 같으면, 이중화 시스템의 MTBF가

삼중화 시스템의 MTBF 보다 더 높은 수치를 갖는다. 일반적으로 삼중화 시스템이 신뢰도가 높은 반면 시스템 전체적으로 볼 때 이중화 시스템이 삼중화 시스템보다 MTBF는 더 높은 것이다. 앞에서 정의된 이용가능도 V의 식을 생각하면, 한정된 MDT를 갖는 계에서 MTBF가 큰 것이 이용 가능성이 높음을 의미한다.

삼중화 시스템이 이중화보다 일반적으로 신뢰도가 높다. 일례로 HIMA 사는 중앙 장치 수준에 HIQuad 기술(2-out-of-4)을 적용하여 TMR (triple modular redundant) 시스템의 고질적인 이용가능성 문제를 해결 하였을 뿐만 아니라 동시에 기존의 이중화 시스템의 신뢰도 문제를 해결하도록 신뢰도를 높혀 왔다.

맺 음 말

서두에 간단히 기술한 바와 같이, 최근 고부가가치선박인 LNG운반선이나 해양플랜트 프로세스 공정 현장에서 안전사고가 끊임없이 발생되고 있고 안전 사고 방지에 많은 노력을 기울이고 있다. 또한 안전시스템 설계에도 중요시 되어가고 있다. 하지만 우리는 아직 선진국가들과 비교하면 안전에 대한 인식과 전문성이 아직도 많이 부족한 실정이다.

본 기술보고에 언급한 안전시스템인 Fail Safety Control System은 TMR System에서 한 단계 높은 안전성을 제공한 시스템이며 선박 및 해양플랜트와 같이 현재 산업현장에서 요구하는 여러 안전요구에 대하여 유용성 있게 구성할 수 있는 안전시스템 설계가 필요하다.

끝으로 안전시스템 설계시 안전시스템의 중요성을 인지하고 안전 표준에 대한 공통의 해석과 인증 절차를 확고히 한다면, 사용자(선주사)와 공급자(조선소) 양측에 큰 도움을 줄 것으로 예상된다. 그리고 신뢰도에 대한 인증은 중요 제어, 안정 가동정지 시스템 및 관련 제품의 신뢰도(Reliabiliyt)와 이용가능성(availability)을 객관적으로 평가해 줄 것이다.

참 고 문 헌

IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Rated Systems.

TUV DIN V19250.

김 덕 기

■ 1975년생
■ 2009년 한국해양대학교 공학박사
■ 현 재 : 현대중공업 조선사업본부 기본설계2부/과장
■ 관심분야 : LNG-FPSO, LNGC, LPGC, FSRU, DRILLSHIP, SUBSEA
■ 연 락 처 : 052-203-3692
■ E - mail : sense315@hhi.co.kr