ISSN 1229-800X The Transactions of the Korean Institute of Electrical Engineers Vol. 66P, No. 1, pp. 43~47, 2017
http://doi.org/10.5370/KIEEP.2017.66.1.043

안전 무결성 등급을 이용한 제어기의 구성에 따른 안전성 평가

Safety Evaluation according to Controller Configuration using Safety Integrity Level

김 종 훈* · 이 대 종* · 이 호 현** · 전 명 근†
(Jong-Hoon Kim · Dae-Jong Lee · Ho-Hyun Lee · Myung-Geun Chun)

Abstract - A SIL(Safety Integrity Level) assignment method is used for preventing failure action. The goal of safety system for processing automation is to reduce the human fatal risk. Even if we have developed the processing automation according to developing technology, we are also realized on increasing the human fatal risk cause of unexpected accidents. This study is directed the solution of decision for safety level for safety system and the best architecture for safety system in process automation.

Key Words : SIS(Safety integrity level), Safety evaluation, Controller configuration

1. 서 론

18세기 제임스 와트의 증기기관을 시작으로 제어의 역사는 실로 눈부시게 발달해 왔다. 현대에 들어서 제어시스템의 중요 분류는 크게 PLC(Programmable Logic Controller)와 DCS(Distributed Control System)로 나누어지는데, 기술에 발전에 따라 이러한 시스템의 구분도 모호해 지는 것이 현재의 상황이다. 이러한 제어시스템도 각 부품들이 모듈화 됨에 따라 좀 더 복잡해지고 다양해지고 있다. 또한 단순히 제어시스템의 기능만 나누어진 것이 아니라, 어떤 분야, 어떤 공정에 적용하느냐에 따라 기본 구성품의 요건이 단일 구성이 아닌 이중화 또는 삼중화 구성으로 설계되어 고장이 발생하더라도 공정운영에 영향을 주지 않고 지속적으로 운전할 수 있게 요구하는 것이 현대 산업공정에서의 자동화시스템에 대한 요구사항이다[1, 2]. 이러한 요구사항에 대한 반영으로 산업공정의 이윤적인 측면에 있어서는 크게 증대되고 있는 것이 사실이지만, 인본주의 입장에서 안전에 대한 관심도 더불어 커지고 있으며, 이 두 가지 측면의 최적의 요건을 갖추는 것이 현대 산업공정의 커다란 이슈가 되고 있다. 하지만 안전에 대한 제어시스템 구성에 있어, 여러 가지 이해관계 및 정보공유의 부족으로 인해 산업공정에 적용되는 사례가 미비한 상황이다.

영국의 대표적인 안전기관인 HSE(Safety and Health Executive)에서 조사한 사고원인 분포를 살펴보면 공장의 시운전 시험 후에 공정변환에서 발생하는 경우가 전체사고의 60%이상을 차지하고 있는 것으로 조사되었다. 실제로 이러한 문제점을 해결하기 위하여 미국에서는 1996년 ISA(Instrument Society of America)와 IEC(International Electrotechnical Commission)에서 “Safety Instrumented System 표준”을 발표하였다. 우선 Safety Instrumented System을 수행하기 전에 시스템의 안전무결성 등급(SIL : Safety Integrity Level) 설정이 선행되어야 한다. ISA/IEC에서 제시한 정성적인 결정 방법으로 발생할 수 있는 문제점을 해결하기 위하여 정량적 위험성 평가방법인 툴을 사용한 제어시스템의 안전 무결성 등급1 결정방법을 제시하였다[3-5].

본 연구에서는 현대 산업공정의 안전 기준이 되고 있는 IEC(International Electrotechnical Commission)의 SIL를 기반으로 제어시스템의 점검 주기 및 구성에 따른 안전등급을 계산하여 제어기의 최적화 운영방안을 제시하고자 한다.

2. 안전 무결성 등급 및 제어기의 구성

2.1 안전 무결성 등급 (SIL)

SIL은 단위공정에 대한 일정한 기간 내에 만족스럽게 수행할 확률의 등급이다. 일반적으로 SIL은 표 1에서 보는 바와 같이 년간 고장확률인 PFD(Probability of Failure on Demand per year)의 값에 따라 1등급에서 4등급까지 분류

표 1 PFD에 따른 SIL
Table 1 SIL according to PFD

SIL	PFD
SIL 4	$10^{-5} \leq PFD < 10^{-4}$
SIL 3	$10^{-4} \leq PFD < 10^{-3}$
SIL 2	$10^{-3} \leq PFD < 10^{-2}$
SIL 1	$10^{-2} \leq PFD < 10^{-1}$

† Corresponding Author : School of Electronics Engineering, Chungbuk National University, Korea
E-mail : mgchun@cbnu.ac.kr
* School of Electronics Engineering, Chungbuk National University, Korea
** K-water Research Institute, Korea Water Resources Corporation, Korea
접수일자 : 2017년 2월 6일
최종완료 : 2017년 2월 27일

하며, 등급의 숫자가 높을수록 정상적으로 수행되어질 확률이 더 높아짐을 의미한다[6, 7].

PFD 값을 계산하기 위해서는 신호검출부, 제어기, 출력부 각각의 점점주기인 PTI(Proof Test Interval), 평균 복구시간인 MTTR(Mean Time To Repair), 진단범위인 PTC(Proof Test Coverage) 등 다양한 설정값들을 이용하여 계산한다.

2.2 제어기의 구성 [8, 9]

(1) 1oo1 구성

그림 1에서 보는 바와 같이 1oo1 구성은 각 채널이 단일 채널로 이루어져 있다. 여기서 모든 위험 측 고장은 요구 시 안전기능의 고장으로 이어진다. 이 구성에서는 고장 허용(fault tolerance)을 제공하지 않으며, 고장 모드(failure mode) 보호를 제공하지 않는다.

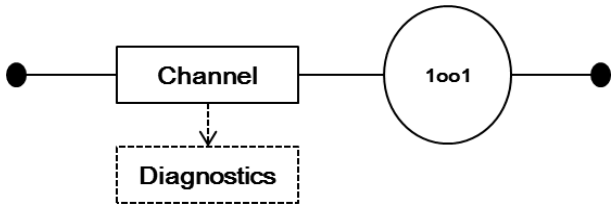

그림 1 1oo1 구성도
Fig. 1 1oo1 Diagram

(2) 1oo1D 구성

1OO1D 구성은 그림 2에서 보는 바와 같이 각 채널은 단일 채널로 구성되어 있다. 정상 운영 중에, 안전 기능이 발생하기 전에 채널은 안전기능을 요구하는 것이 필요하다. 진단 시험에 의해 채널에서 결함이 발견되거나 채널에 할당될 수 없는 불일치가 발견되면, 산출물은 안전한 상태로 된다. 이 구성은 안전 어플리케이션에 사용되는 강화를 나타낸다. 진단은 감지된 위험 고장을 안전 고장으로 변환할 수 있다. 일반적으로, 추가적인 고장률이 추가 진단 채널을 고려하여 정량적 분석에 포함되어야 한다.

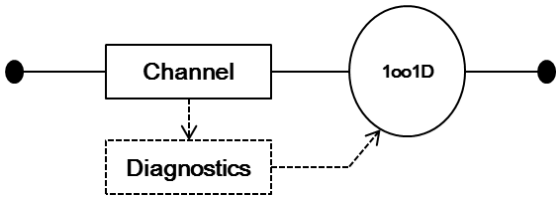

그림 2 1001D 구성도
Fig. 2 1oo1D Diagram

(3) 1oo2 구성

1oo2구성은 그림 3에서 보는 바와 같이 각 채널이 안전기능을 처리할 수 있도록 병렬로 된 두 개의 채널로 구성된다. 그러므로 요구 시 안전 기능이 고장 나기 전, 양 채널에 위험, 즉 고장이 있을 수 있다. 진단 시험은 발생한 고장을 표시하며, 출력상태 또는 출력 보팅을 변화시키지 않는다.

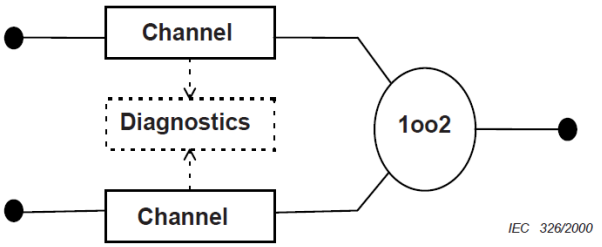

그림 3 1oo2 구성도
Fig. 3 1oo2 Diagram

(4) 2oo2 구성

2oo2구성은 그림 4에서 보는 바와 같이 각 각 채널이 병렬로 연결된 두 개의 채널로 구성된다. 따라서 안전기능이 발생하기 전에 양 채널은 안전기능을 요구하는 것이 필요하다. 진단 시험은 발생한 고장을 표시하며, 출력상태 또는 출력 보팅을 변화시키지 않는다.

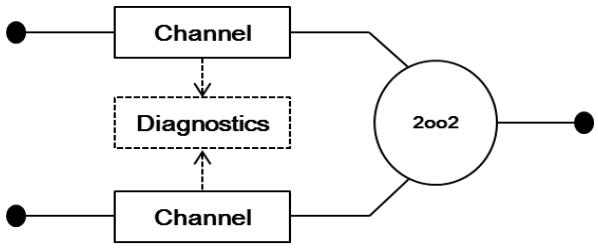

그림 4 2oo2 구성도
Fig. 4 2oo2 Diagram

(5) 2oo3 구성

2oo3 구성은 그림 5에서 보는 바와 같이 출력 신호에 대하여 다수 보트 장치를 가진 병렬로 연결된 세 개의 채널로 구성된다. 그러므로 출력 상태는 단지 하나의 채널이 다른 두 개의 채널과 일치하지 않을 때에는 변경되지 않는다. 진단 시험은 발생한 고장을 표시하며, 출력상태 또는 출력 보팅을 변화시키지 않는다.

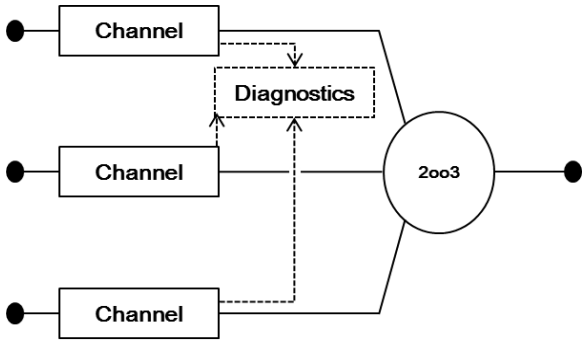

그림 5 2oo3 구성도
Fig. 5 2oo3 Diagram

(6) 1oo3 구성

1003 구성은 그림 6에서 보는 바와 같이 각 채널이 병렬

로 된 세 개의 채널로 구성되며 출력상태는 1oo3 보팅을 따른다. 진단 시험은 발생한 고장을 표시하며, 출력상태 또는 출력 보팅을 변화시키지 않는다. 구성도는 2oo3과 동일하지만, 출력은 세 개의 입력중 하나만 정상이어도 출력을 보장한다.

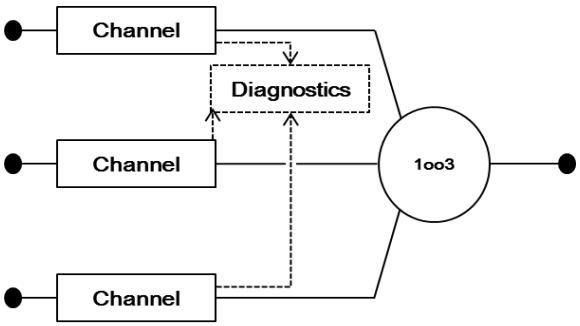

그림 6 1oo3 구성도
Fig. 6 1oo3 Diagram

(7) 3oo3 구성

3oo3 구성은 그림 7에서 보는 바와 같이 각 채널이 병렬로 된 세 개의 채널로 구성되며 출력상태는 3oo3 보팅을 따른다. 진단 시험은 발생한 고장을 표시하며, 출력상태 또는 출력 보팅을 변화시키지 않는다. 구성도는 2oo3과 동일하지만, 출력은 세 개의 입력 모두가 정상이어야만 출력을 보장한다.

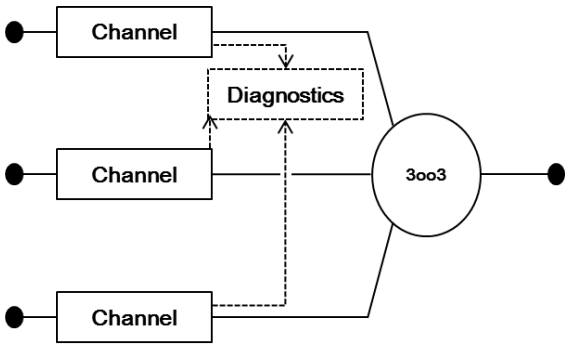

그림 7 3oo3 구성도
Fig. 7 3oo3 Diagram

3. SIL기법을 이용한 제어기의 안정성 평가

3.1 제어기의 안정성 평가 방법

본 논문에서는 제어기의 점검 주기 및 구성요소에 따른 안정성을 평가하기 위하여 그림 8과 같이 시스템을 구성하였다. 그림 8에서 센서는 유량계를 의미하고, 출력부는 유량제어를 위한 밸브를 나타낸다. 제어기는 안전 등급이 높아 원자력 및 석유화학공정에 널리 사용되는 RTP(Real Time Products)를 고려하였다. 그림 9에 나타낸 RTP 제어기는 전원공급기, 입출력카드, 중앙처리장치 등이 모두 모듈화 되어 있어, 각각의 모듈을 단일, 이중, 삼중화 또는 사중화로 구성이 가능하다.

본 연구에서는 제어기의 점검주기 및 구성요소에 따른 전체 시스템의 SIL 등급을 평가하고자 한다. SIL 등급 판정을 위해 입력요소인 유량센서와 출력요소인 밸브의 평균 복구시간(MTTR)은 24시간, 진단범위(PTC)는 모두 90[%], 점검주기(PTI)는 1년으로 설정하였으며, exida에서 제공하는 exSILentia 프로그램을 이용하여 제어기의 안정성을 평가하였다[10].

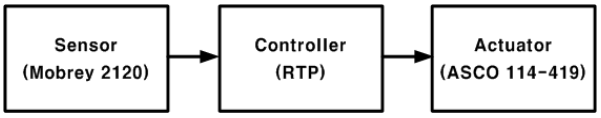

그림 8 시스템 구성
Fig. 8 System configuration

그림 9 RTP 제어기
Fig. 9 RTP controller

3.2 제어기의 점검 주기에 따른 안정성 평가

제어기의 점검 주기에 따른 안정성을 평가하기 위하여 제어기의 구성은 2oo3, 평균복구시간(MTTR)은 24시간, 진단범위(PTC)는 90[%]로 설정한 후 점검 주기에 따른 제어기의 안정성을 평가하였다. 점검 주기는 1달, 3달, 6달, 9달, 1년, 2년, 3년, 4년, 5년, 6년, 7년, 8년, 9년, 점검이 없는 경우로 구분하여 제어기의 안정성 평가를 진행하였다.

그림 10과 그림 11에서는 점검을 하지 않은 경우 시간에 따른 PFD와 점검주기가 1년인 경우 시간에 따른 PFD을 나타냈다. 그림 10에서 보는 바와 같이 점검주기가 없는 경우 제어기의 SIL은 2등급으로 판정되었다. 반면에 점검 주기가 1년인 경우 제어기의 SIL은 3등급으로 나타나, 적절한 점검주기를 두고 운영하면 원하고자 하는 SIL 등급 내에서 건전하게 운영할 수 있다는 것을 알 수 있다.

그림 12에서는 제어기의 점검주기에 따른 제어기와 시스템(SIF)의 년간 고장확률인 PFD를 비교하여 나타냈다. 그림 12에서 첫 번째 막대(청색)는 시스템(SIF)의 PFD_{avg}를 나타내며, 두 번째 막대(적색)는 제어기의 PFD_{avg}를 나타낸다. 그림 12에서 보는 바와 같이, 점검주기가 짧을수록 PFD_{avg}이 낮아지는 것을 확인할 수 있다. 또한, 점검 주기가 1년이 되는 시점에 시스템의 PFD_{avg}가 10^{-3}보다 작아져서 SIL 등급이 SIL 2에서 SIL 3으로 상향되는 것을 확인할 수 있다.

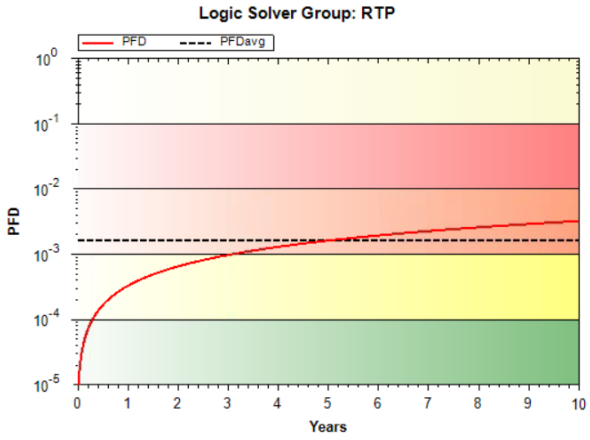

그림 10 점검을 하지 않은 경우 시간에 따른 PFD
Fig. 10 PFD without proof test according to time

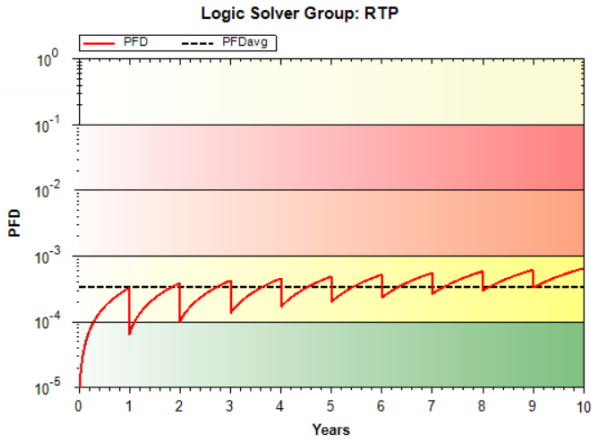

그림 11 점검주기가 1년인 경우 시간에 따른 PFD
Fig. 11 PFD with proof test(1 year) according to time

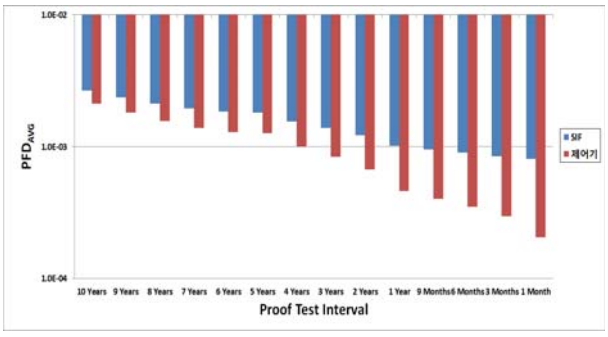

그림 12 점검주기에 따른 제어기 및 시스템의 PFD
Fig. 12 PFD for controller and system according to proof test interval

3.3 제어기의 구성에 따른 안정성 평가

제어기의 점검주기는 1년으로 고정한 상태에서 제어기의 구성에 따른 제어기 및 시스템의 년간 고장확률인 PFD를 분석하였다. 그림 13에서 첫 번째 막대(청색)는 시스템(SIF)의 PFD_{avg}를 나타내며, 두 번째 막대(적색)는 제어기의 PFD_{avg}를 나타낸다. 그림 13에 보는 바와 같이 제어기의 구성이 달라짐에 따라 제어기의 PFD가 변화하며, 그에 따라 전체 시스템 PFD가 변화하는 것을 확인할 수 있다. 특히 3oo3에서 2oo2로 제어기 구조가 변경되면, 시스템의 PFD가 10^{-3}보다 작아져서, SIL 등급이 SIL 2에서 SIL 3으로 증가하는 것을 확인할 수 있다.

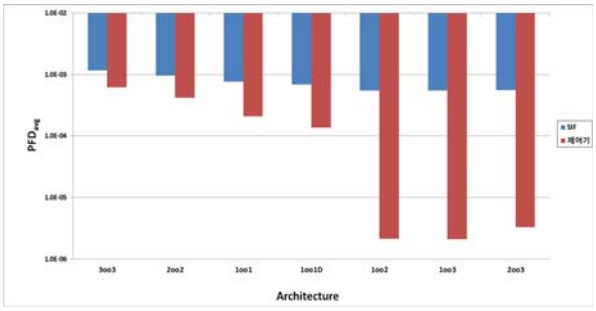

그림 13 제어기의 구성에 따른 PFD
Fig. 13 PFD according to controller configuration

여기서 단순히 안전등급을 결정하는 PFD값만 논의하는 것보다, 공정 효율에 중요시되는 가용성과의 상관관계를 논의하는 것이 필요하다. 가용성(Availability)은 시스템이 장애 없이 정상적으로 기능을 수행할 수 있는 능력을 나타내며, 식 (1)과 같이 표현된다. 식 (1)에서 MTTF(Mean Time To Failure)는 현재 고장시점에서 다음에 고장이 발생할 때까지의 평균시간을 의미하고, MTTR(Mean Time To Repair)는 평균 복구시간을 의미한다.

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \tag{1}$$

제어기의 구성에 따른 전체 시스템의 가용성과 PFD를 비교하여 그림 14에 나타냈다. 그림 14에서 첫 번째 막대(청색)는 시스템의 가용성을 나타내고, 두 번째 막대(적색)는 시스템의 PFD를 나타낸다. 그림 14에서 보는 바와 같이 제어기의 구성이 2oo3일 때 가용성 및 PFD값이 모두 양호함을 확인할 수 있다.

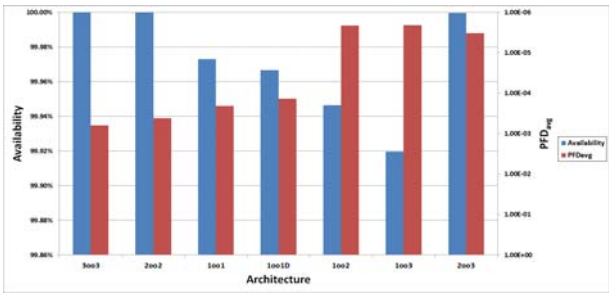

그림 14 제어기 구성요소에 따른 가용성 및 PFD
Fig. 14 Availability and PFD according to controller configuration

4. 결 론

본 논문에서는 원자력 및 석유화학분야에서 널리 사용되는 센서(유량계)-제어기(RTC)-출력(밸브)로 구성된 모델을 이용하여 점검주기 및 제어기 구성에 따른 년간 고장확률인 PFD을 평가하였으며, 평가된 PFD를 이용하여 안전 무결성 등급(SIL)을 판정하였다. 점검 주기에 따른 평가결과 점검 주기가 1년 이내인 경우 SIL 등급이 2에서 3으로 상향됨을 확인하였다. 또한, 제어기 구성에 따른 안전성 평가 결과 2oo3 제어기 구성은 안전등급에 영향을 주는 PFD값이 SIL 3의 임계점 및 시스템이 장애 없이 정상적으로 기능을 수행할 수 있는 가용성 측면에서 모두 양호한 결과를 도출하여 제어계통 설계 시, 최적의 방안이라는 것을 알 수 있었다. 본 실험을 응용하여 모든 산업분야에 인류의 안전과 직결된 안전하면서도 가용성을 보유한 제어시스템을 구축하는데 기여할 수 있을 것이라 판단된다.

감사의 글

본 논문은 중소기업청에서 지원하는 2016년도 산학연협력 기술개발사업(No. C0395356)의 연구수행으로 인한 결과물임을 밝힙니다.

References

[1] Sung-Kyun Ryou, Jae-Young Park, Hak-Sun Yun, “An Allocation of Safety Integrity Level to Inductive Loop type Train Control System,” *JKIECS*, vol. 8, no. 12, pp. 1905-1910, 2013.

[2] Deung-Ryeol Yoo, Key-Seo Lee, “A Study on Architecture Design of Power Supply for SIL4 Safety Related System,” *JKIECS*, vol. 10, no. 9, 1001-1008, 2015.

[3] J. Beugin, D. Renaux, L. Cauffriez, “A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems,” *Reliability Engineering and System Safety*, vol. 92, pp. 1686 - 1700, 2007.

[4] Hamid Jahaniana, QamarMahboobb, “SIL determination as a utility-based decision process,” *Process Safety and Environmental Protection*, vol. 102, pp. 757 - 767, 2016.

[5] Feng Wang, Ou Yang, Ruibo Zhang, Lei Shi, “Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database,” *Journal of Loss Prevention in the Process Industries*, vol. 44, pp. 212-222, 2016.

[6] IEC61511-1, 2003. Functional Safety-Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements. International Electrotechnical Commission.

[7] IEC61508-4. 2010. Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Part 4: Definitions and Abbreviations. International Electrotechnical Commission.

[8] IEC61508-6, 2000. Functional Safety of Electrical/ Electronic /Programmable Electronic Safety-Related Systems. Part 6. Guidelines on the Application of IEC61508-2 and IEC61508-3. International Electro -technical Commission.

[9] IEC61508-6 2010. Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Part 6. Guidelines on the Application of IEC61508-2 and IEC61508-3. International Electro-technical Commission.

[10] http://www.exida.com/exSILentia

저 자 소 개

김 종 훈 (金 鐘 勳)

2000년 충주대학교 컴퓨터공학 졸업. 2017년 충북대학교 대학원 전기전자반도체공학과 졸업(공학석사), 2005년~ 현재 RTP코리아(주) 재직

E-mail : jhkim@rtpkorea.com

이 대 종 (李 大 鍾)

1995년 충북대학교 전기공학과 졸업. 1997년 동 대학원 졸업(공학석사), 2002년 동 대학원 졸업(공학박사). 2006년~2008년 충북대학교 BK21충북정보기술사업단 초빙조교수

E-mail : leebigbell@gmail.com

이 호 현 (李 鎬 賢)

1998년 원광대학교 전자공학과 졸업. 2010년 한국과학기술원 대학원 졸업(공학석사), 2016년 충북대학교 대학원 졸업(공학박사). 1998년~현재 한국수자원공사 재직

E-mail : lhh@kwater.or.kr

전 명 근 (全 命 根)

1987년 부산대학교 전자공학과 졸업. 1989년 : 한국과학기술원 전기및전자공학과 대학원 졸업(공학석사). 1993년: 한국과학기술원 전기및전자공학과 대학원 졸업(공학박사). 1993년~1996년 삼성전자 자동화 연구소 선임연구원. 2000년~2001년 University of Alberta 방문 교수. 2010년~2011년: Temple University 방문 교수. 1996년~현재 충북대학교 전자공학부 교수. 2008년~현재 : TTA PG505 표준위원회 의장

E-mail : mgchun@cbnu.ac.kr