

개질형 On-Site 수소충전소의 리스크 감소를 위해 요구되는 SIL 등급 달성 방안에 관한 연구

이진호* · 임재용**†

A Study on the Achievement of Required Safety Integrity Level to Reduce Risk for SMR On-Site Hydrogen Refueling Stations

Jin Ho Lee* · Jae-Yong Lim**†

†Corresponding Author

Jae-Yong Lim

Tel : +82-2-970-6388

E-mail : jaeyong.lim@gmail.com

Received : October 16, 2020

Revised : December 10, 2020

Accepted : December 21, 2020

Abstract : In recent years, hydrogen has received much attention as an alternative energy source to fossil fuels. In order to ensure safety from the increasing number of hydrogen refueling stations, prevention methods have been required. In this regard, this study suggested an approach to reduce the risk of hydrogen refueling station by increasing Safety Integrity Level (SIL) for a Steam Methane Reformer (SMR) in On-Site Hydrogen Refueling Station. The worst scenario in the SMR was selected by HAZOP and the required SIL for the worst scenario was identified by LOPA. To verify the required SIL, the PFDavg.(1/RRF) of Safety Instrumented System (SIS) in SMR was calculated by using realistic failure rate data of SIS. Next, several conditions were tested by varying the sensor redundancy and proof test interval reduction and their effects on risk reduction factor were investigated. Consequently, an improved condition, which were the redundancy of two-out-of-three and the proof test interval of twelve months, achieved the tolerable risk resulting in the magnitude of risk reduction factor ten times greater than that of the baseline condition.

Key Words : hydrogen refueling station, SIL (Safety Integrity Level), LOPA (Layer of Protection Analysis), PFD (Probability of failure on demand), SIL verification

Copyright©2020 by The Korean Society of Safety All right reserved.

1. 서론

지구온난화가 가속화되면서 기존 사용하던 화석에너지를 대체할 수 있는 신재생에너지에 대한 관심과 개발이 이루어지고 있으며, 수소에너지는 그 중 차세대 에너지원으로 가장 각광받고 있다¹⁾. 특히, 운송수단 분야에서 친환경자동차로써 수소전기차의 관심과 수요가 꾸준히 증가하고 있어서 수소충전소 확대가 예상된다.

수소 가스의 효율적이고 안정적인 사용을 위해서는 수소에 대한 생산, 운송, 저장 기술에 대한 연구가 많이 이루어지고 있는데, 수소의 넓은 폭발범위와 낮은 착화에너지 등을 고려하여 정성적, 정량적 안전성 평가 및

사고 차단 기술 개발 등과 같은 연구가 필요하다²⁾.

수소충전소에 대해 위험성을 다룬 기존의 연구들을 살펴 보면, 수소 충전소의 화재 위험성 평가^{1,2)}, 수소 가스 누출로 인한 피해거리 평가³⁾ 및 3D CFD 시뮬레이션 모델링 평가⁴⁾ 등의 정량적 위험성 연구는 많이 수행되었다. 하지만 위에서 언급되었듯이 화재 및 폭발 사고 피해를 줄이기 위한 연구가 지속적으로 이루어지고 있는 반면에, 어떻게 사고를 사전에 차단하여 예방할 수 있을지에 대한 연구는 부족한 실정이다.

따라서 본 연구에서는 사고를 예방할 수 있는 기능안전(Functional Safety) 측면에서 안전계장시스템(Safety Instrumented System : SIS)의 안전무결수준(Safety Integrity Level : SIL)을 높임으로써 수소충전소의 안전성을 확

*서울과학기술대학교 안전공학과 석사과정 (Department of Safety Engineering, Seoul National University of Science and Technology)

**서울과학기술대학교 안전공학과 교수 (Department of Safety Engineering, Seoul National University of Science and Technology)

보할 수 있는지 연구하고자 한다. 이번 연구를 통해 현재 수소 충전소의 위험도 수준을 확인할 수 있고 이전 연구에서는 다루지 못했던 기능안전 측면에서 얼마나 위험도를 감소시켜야 하는지 정량적으로 분석하고자 한다.

연구 방법으로는 수소 충전소의 가장 위험한 화재, 폭발 사고 시나리오가 무엇인지 확인하기 위하여 정성적 위험성 평가의 기법인 HAZOP(Hazard and Operability)을 사용하였고, 해당 시나리오에서 요구되는 안전무결 수준(SIL)을 도출하기 위해 LOPA(Layer of Protection Analysis : 방호계층분석) 기법을 통해 분석하였다. 그리고 도출된 요구되는 SIL값을 현재 설계 기준으로 맞출 수 있는지 검증하기 위해 소프트웨어를 활용하여 산출된 SIL값과 비교하였다. 산출된 SIL값이 요구되는 SIL수준을 맞추지 못할 경우에는 SIS의 구성 요소 대한 복수화(Redundancy) 및 점검주기(Proof Test Interval)와 같은 여러 조건에 대한 분석을 통해 SIL을 향상시키기 위한 방안을 제시하였고 수소충전소의 리스크를 허용 가능한 수준까지 낮추고자 한다.

2. 연구 대상 및 방법

2.1 연구 대상

본 연구에서는 수증기 개질형 On-Site 수소충전소 내 수소를 생산하는 개질 반응기(Reformer) 공정을 대상으로 연구를 진행하고자 한다.

2.1.1 수소충전소의 종류

수소충전소는 크게 Off-Site 수소충전소 및 On-Site 수소충전소로 분류할 수 있다. Off-Site 수소충전소는 외부로부터 수소를 튜브트레일러 배관을 통해 충전소에 공급하는 방식이고, On-Site 수소충전소는 충전소 내에서 수소를 직접 생산하는 방식이다⁵⁾.

On-Site 수소충전소는 다시 개질형 및 수전해형으로 나뉘고, 이 중에 개질형 On-Site 수소충전소는 Fig. 1과 같이 주로 천연가스 또는 LPG 개질을 통하여 수소를 충전소 내에서 자체 생산하는 수증기 개질형(Steam Methane Reforming : SMR) 방식이 쓰인다.

개질형 On-Site 수소충전소의 경우 개질 장치 등이 필요해 충전소 설치 비용이 Off-Site 충전소보다 높다는 단점이 있으나, 수소 수요량이 증가하여 이송비용이 증가할 경우 오히려 비용의 장점이 있어 경제적이다¹⁾. 따라서 향후 수증기 개질형 On-Site 수소 충전소가 늘어날 것으로 전망되었기 때문에 이번 연구의 대상으로 선정하였다.

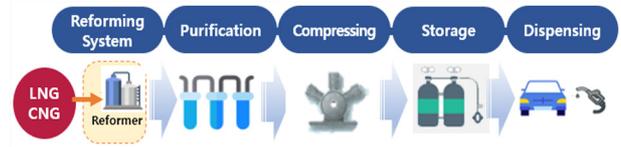


Fig. 1. SMR On-site hydrogen refueling station.

2.1.2 수증기 개질형 (Steam Methane Reforming : SMR) 수소 생산 시스템

수증기 개질형 수소 생산 방식은 물과 탄화수소 분자에 포함된 수소를 최대한 추출하는 방식으로 메탄 1몰당 수소생산 수율이 가장 높으며, Fig. 2와 같이 주요 구성 요소는 개질 반응기(Reformer), 수성전환 반응기(Water Gas Shift) 및 PSA(Pressure Swing Adsorption)가 있다⁶⁾.

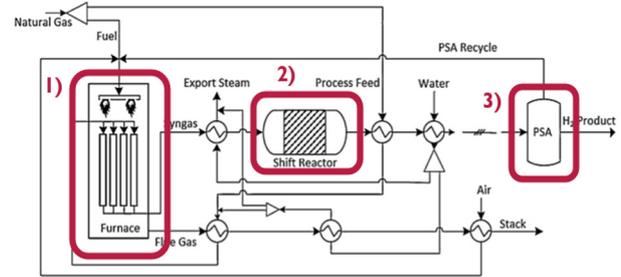


Fig. 2. Hydrogen production system of SMR⁷⁾
1) Reformer 2) Water Gas Shift 3) PSA.

2.1.3 개질 반응기 (Reformer)

개질 반응기는 반응기 내부에 촉매층을 가진 이중관 구조의 개질 튜브로 구성되어 있고, 수증기가 천연가스와 혼합되어 약 850 kPa의 압력과 약 850~1000°C의 온도에서 촉매층을 통과하면서 천연가스-수증기 개질 반응으로 수소를 포함한 합성가스를 생산한다⁶⁾.

2.2 연구 방법

수소충전소 내 개질 반응기의 리스크 감소를 위해 이번 연구에서는 HAZOP 및 LOPA 기법을 활용하여 위험성 평가를 우선 진행하였다. 이를 통해 허용 가능한 위험 수준에 도달하기 위한 개질 반응기의 SIS에 요구되는 SIL 값을 도출하였다. 그리고 실제 SIS의 PFD_{avg} 값이 요구되는 SIL 값을 만족하는지 소프트웨어를 활용하여 검증(Verification)을 수행하였다.

2.2.1 HAZOP (Hazard and Operability)

HAZOP을 수행하기 위해 개질 반응기 시스템을 간략화하였고, 아래 Fig. 3과 같이 개질 반응기(Reformer) 공정을 HAZOP 검토 대상(Node)으로 선정하였다.

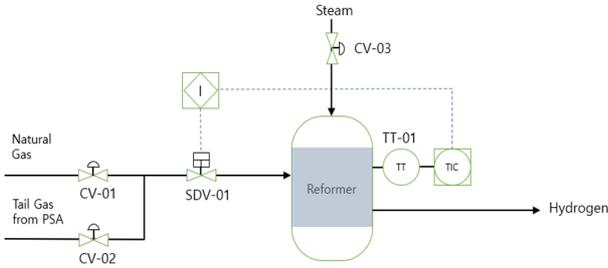


Fig. 3. HAZOP node of reformer.

Table 1. Risk matrix⁸⁾

		Likelihood		
		Likely	Possible	Rare
Consequence Severity		3	2	1
Fatality, Significant Damage	4	5	5	3
Injury, Major Damage	3	4	4	2
No injury, Slight Damage	2	3	2	1
No injury, No Damage	1	2	1	1

[Risk Criteria]

5 - Very High Risk / 4 - High Risk / 3 - Medium Risk
2 - Low Risk / 1 - Very Low Risk

HAZOP Node를 바탕으로 개질 반응기의 설계 의도에서 벗어나는 공정 이탈 (Deviation)을 파악하였다.

Deviation은 No/Less/Low(없음/감소/낮음) 및 More/High(많음/높음)와 같은 가이드워드(Guideword)와 공정상의 변수인 Flow(흐름), Temperature(온도) 및 Pressure(압력)을 조합하여 표현한다. 각 Deviation을 일으킬 수 있는 원인(Cause)을 파악하였고, 그로 인한 결과(Consequence) 및 사고를 예방할 수 있는 안전장치(Safeguard)가 무엇인지 분석하였다.

또한 Table 1의 위험도 대조표(Risk Matrix)를 활용하여 각 시나리오에 대해 위험도를 분석하였는데, 발생 빈도(Likelihood) 및 심각도(Severity)에 따라 Risk는 “1 (Very Low Risk)”부터 “5 (Very High Risk)”까지 구분하였다.

2.2.2 방호계층분석 (LOPA)

HAZOP을 통해 나온 최악의 사고 시나리오를 방지할 수 있는 SIS에 대해 요구되는 안전무결수준(SIL)을 확인하기 위하여 LOPA를 수행하였다⁹⁾.

LOPA는 사고의 빈도나 강도를 감소시킬 수 있는 독립방호계층(Independent Protection Layer : IPL)의 효과성을 평가하는 기법으로¹⁰⁾ SIS의 안전무결수준(SIL)을 정량적으로 나타내 줄 수 있어서 효과적이다¹¹⁾.

Table 2에서 볼 수 있듯이, 안전무결수준(SIL)의 등급은 안전계장시스템(Safety Instrumented System, SIS)의 작동 요구 시의 연간 평균 고장 확률 (Average Probability

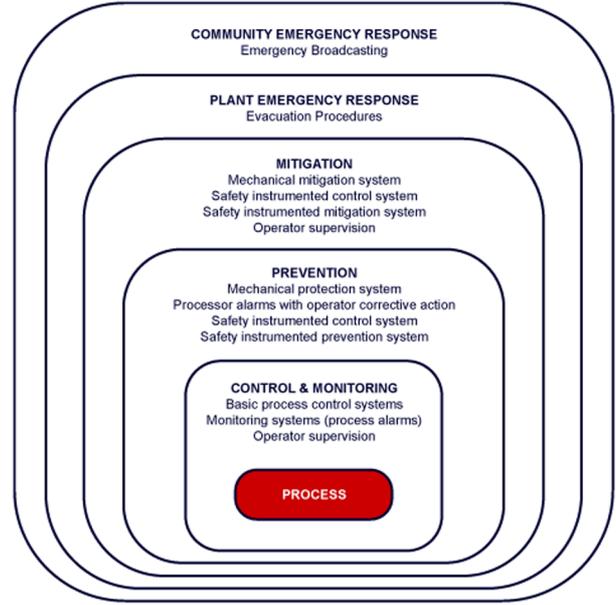


Fig. 4. Independent protection layer (IPL) used for LOPA.

Table 2. Safety integrity level^{14,15)}

SIL	PFD _{avg.}	Risk reduction factor*
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10,000 to $\leq 100,000$
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1,000 to $\leq 10,000$
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to $\leq 1,000$
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

* Risk Reduction Factor (RRF) = 1 / PFD_{avg.}

Table 3. Target mitigated event likelihood TMEL

Consequence severity	Target mitigated event likelihood
4	$< 1 \times 10^{-6}$ (per year)
3	$< 1 \times 10^{-5}$ (per year)
2	$< 1 \times 10^{-4}$ (per year)
1	$< 1 \times 10^{-3}$ (per year)

of Failure on demand, PFD_{avg.})의 값에 따라 ‘SIL 1’에서 ‘SIL 4’까지 나누어 표현한다^{12,13)}.

LOPA는 이전 HAZOP 분석에서 나온 가장 위험한 최악의 사고 시나리오를 대상을 분석하였다. 먼저 해당 시나리오의 Consequence Severity(강도)에 따라서 허용 가능한 위험 수준(Risk Tolerable Criteria)을 만족하기 위해 필요한 목표 빈도를 정해야 한다. 이 목표 빈도는 Table 3과 같이 ‘허용 가능한 완화된 사고빈도 (Target Mitigated Event Likelihood, TMEL)’로 표현하여 정하였다.

이어서 사고의 초기 원인(Initiating Cause)의 발생 빈도와 사고 결과를 발생시키는 조건(Conditional Modifier)의 확률을 곱해 주어 ‘완화되지 않은 결과 빈도값

(Frequency of unmitigated consequence)을 구한다.

초기 원인으로써 ‘Temperature Control Failure’와 같은 BPCS (Basic Process Control System)의 고장으로 인한 발생 빈도는 일반적으로 1×10^{-1} (per year)로 고려한다¹⁶⁾.

사고 결과를 발생시키는 조건(Conditional Modifier)은 화재 및 폭발 사고로 인한 인명 피해 시나리오의 경우에는 점화될 확률(Probability of Ignition), 사고 영향 범위 내 사람이 있을 확률(Probability of personnel in affected area) 그리고 사망 확률(Probability of Fatal Injury)을 고려하였다.

사고 시나리오의 독립방호계층(IPL)으로서, Fig. 4에서 나온 여러 방호 계층 중에서 사고를 발생시키는 공정이탈을 사전에 제어와 감시할 수 있는 BPCS와 긴급 차단밸브(Shutdown Valve)를 통해 사고를 예방할 수 있는 SIS를 고려하였다. 고려한 모든 방호계층이 갖고 있는 ‘작동 요구시 고장 확률 (PFD)’을 곱해 주면 해당 사고 시나리오의 ‘완화된 결과 빈도값 (Frequency of Mitigated Consequence)’을 산출할 수 있다.

위 설명한 시나리오의 ‘완화된 결과 빈도값’을 산출하는 방식은 아래 식 (1)과 같이 표현된다.

$$F_{scenario} = F_I \times P^i \times P^p \times P^f \times \left(\prod_{i=1}^n PFD_i \right) \quad (1)$$

where $F_{scenario}$ = Frequency of mitigated consequence

F_I = Frequency of initiation event

P^i = Probability of ignition

P^p = Probability of person present

P^f = Probability of fatality

마지막으로 산출된 ‘완화된 결과 빈도값’이 허용 가능한 위험 기준 (Risk Tolerable Criteria)의 사고 빈도값과 비교하여 만족할 수 있는지 확인하였고, 만족하지 못할 경우에는 추가로 얼마만큼의 확률값이 필요한지 산출하였다.

Table 4. SIS realistic failure rate

SIS Element	Description	Tag.no.	Failure rate (* λ_{DU})	Source
Sensor	Temperature transmitter	TT-001	3.10E-08	**SERH (Vendor data)
Logic solver	PLC	-	7.40E-09	
Final element	Valve body	SDV-01	5.69E-07	
	Solenoid driver		1.50E-08	
	Actuator		2.26E-07	

* λ_{DU} : Rate of dangerous undetected (DU) failures

**SERH : Safety equipment reliability handbook by exida

2.2.3 SIL 검증 (Verification) 방법

LOPA를 통해 도출된 요구되는 SIL등급의 확인은 Exida사의 상용 소프트웨어를 활용하여 PFD_{avg} 을 구하여 검증하였다.

SIL검증(Verification)하기 위한 SIS의 각 구성 요소 (Sensor, Logic Solver, Final Element)에 대한 고장율은 Table 4와 같이 고려하였다.

추가적으로 PFD_{avg} 를 구하기 위해 운전 기간 (Mission Time), 점검주기 (PTI, Proof Test Interval), 평균 복구시간 (MTTR, Mean Time To Repair) 등과 같은 다양한 변수들에 대한 설정값이 필요하다¹⁷⁾.

주요 변수들에 대한 초기 설정값은 아래와 같이 고려하였고, 진단범위 및 공통원인고장은 IEC 61508, Part 6¹⁴⁾을 참고하였고 Final Element의 경우에 Full Stroke Test로 고려하였다.

- 1) 운전 기간 (Mission Time) : 30 years
- 2) 점검 주기 (Proof Test Interval) : 60 months
- 3) 진단 범위 (Proof Test Coverage, C_{pt}) : 90%
- 4) 평균 복구 시간 (MTTR) : 72 hours
- 5) 공통원인고장 (Common Cause Failures) : 10%

SIS의 PFD_{avg} 값은 각 SIS element의 고장율, 주요 변수들을 적용하면 식 (2)를 통해 산출된다.

$$PFD_{avg} = \lambda_{DD} \times MTTR + [C_{PT} \times \lambda_{DU} \times \frac{TI}{2}] + [(1 - C_{PT}) \times \lambda_{DU} \times \frac{MT}{2}] \quad (2)$$

where PFD_{avg} =Average probability of failure on demand

MT = Mission time

TI = Test interval

C_{pt} = Proof test coverage

MTTR = Mean time to restore

소프트웨어를 활용하여 산출된 PFD_{avg} 결과값이 요구되는 SIL등급 및 PFD_{avg} 를 만족하지 못하는 경우에는 추가적인 대안을 고려한 Case Study를 수행하였다.

3. 연구 결과

3.1 HAZOP 수행 결과

개질 반응기에 대한 HAZOP 분석을 통해 비정상 상태의 발생 원인과 결과 그리고 안전 장치를 분석하였다. 분석한 결과는 Table 5와 같다. HAZOP 분석 결과 가장 위험성이 높은 시나리오는 아래와 같다.

Table 5. HAZOP worksheet

Deviation	Cause	Consequence	Safeguards	Risk Ranking			Recommendation
				Likelihood	Severity	Risk	
More flow	Natural gas control valve fully opened	More natural gas flow and pressure increase leading to pipe leakage of natural gas. Potential jet fire	Natural gas flow high alarm	1	4	3 (Medium risk)	
No / Less flow	Control valve blocked	Decrease of flow and delay of H2 production	Hydrogen flow low alarm	1	3	2 (Low risk)	
High temperature	Temperature control failure	Reformer temperature increase leading to reformer damage and rupture. Hydrogen leakage and potential jet fire and explosion. Personnel fatality	Temperature high alarm	2	4	5 (Very high risk)	
			Temperature high high (TAHH-01) close to SDV-01				
Low temperature	Failure of heating device	Reforming Failure and incomplete reaction. Low production of H2	Temperature low alarm	1	3	2 (Low risk)	
High pressure	Pressure control failure	Pressure increase leading to reformer damage and incomplete reaction.	Pressure high alarm	2	3	4 (High risk)	
Low pressure	Pressure control failure	Pressure decrease and incomplete reaction. low production of H2.	Pressure low alarm	2	3	4 (High risk)	

- Deviation : High Temperature
- Cause : Temperature Control Failure
- Consequence : Reformer Damage 및 Rupture로 인한 화재, 폭발 사고 발생 및 인명 사망 사고

Table 1의 Risk Matrix를 참고하여 보면, 인명 사망 (Fatality) 사고의 경우 강도(Severity)는 가장 높은 '4, 치명적'으로 분류되고, 이에 따라 위험도(Risk)는 '5, Very High Risk'로 분석되었다.

해당 시나리오에 대한 안전장치로서 BPCS의 High Temperature Alarm 및 안전계장기능(Safety Instrumented Function: SIF)의 Temperature High High 기능이 있는 것으로 확인하였고, 해당 SIF는 개질기의 온도 상승을 Temperature Transmitter(TT-01)에서 감지하여 Logic Solver를 통해 긴급차단밸브(Emergency Shutdown Valve)인 SDV-01을 차단시켜 사고를 방지할 수 있다.

해당 SIF를 통해 시나리오의 리스크가 허용 가능한 수준 (Tolerable)까지 낮출 수 있도록 LOPA수행을 통해 요구되는 SIL값을 확인하였다.

3.2 LOPA 수행 결과

HAZOP 분석을 통해 확인된 가장 위험성이 높은 화재, 폭발 시나리오에 대해 요구되는 SIL값을 확인하기 위해 LOPA를 수행한 결과는 Table 6과 같다.

LOPA 분석 결과 Severity 4, (치명적)에 대한 허용 가능한 위험 (Tolerable) 수준의 사고 빈도는 Table 3에 의해 $< 1 \times 10^{-6}$ 이다. 이 빈도값을 맞추기 위해 요구되는 SIL의 평균고장확률은 2×10^{-3} (RRF=500)보다 작아야 되는 것으로 확인되었다. RRF 500은 Table 2를 참고하면 'SIL 2'에 해당하는 수준임을 알 수 있다.

Table 6. LOPA worksheet

	Description	Probability	Frequency (per year)
Consequence /Severity	Reformer temperature increase and pressure increase leading to Reformer damage and Rupture. Potential fire and explosion. Personnel fatality		
	/ Severity category 5		
Risk tolerable criteria	Tolerable		$< 1 \times 10^{-6}$
Initiating event	Loop failure of BPCS (Temperature control failure)		1×10^{-1}
Conditional modifier	Probability of ignition	0.1	
	Probability of personnel in affected area	0.5	
	Probability of fatal injury	1	
Frequency of unmitigated consequence			5×10^{-3}
Independent protection layers	BPCS - Temperature high	1×10^{-1}	
	SIF (To be verified - See actions)	$< 2 \times 10^{-3}$	
Safeguards (non-IPLs)	Pressure alarm is not an IPL as it is part of the BPCS system already credited in temperature high		
Total PFD for all IPLs			$< 2 \times 10^{-4}$
Frequency of mitigated consequence			1×10^{-6}
Risk tolerance criteria met?			Yes, with actions for SIF.
Actions required to meet risk tolerance criteria : To be verified the SIF with PFD of $< 2 \times 10^{-3}$ (*RRF = 500, SIL2)			

3.3 SIL 검증 수행 결과

Exida사에서 개발한 상용 소프트웨어인 'exSILentia'를 활용하여 작동 요구 시 평균 고장 확률 (PFD_{avg})값을 구하여 SIL검증을 실시하였다.

3.3.1 Base Condition 기준 결과

현재 설계 기준 SIS에 대한 구성은 Fig. 5와 같다.

- Sensor : TT-01 (1oo1, 1 out of 1)
- Logic Solver : PLC (1oo1, 1 out of 1)
- Final Element : SDV-01 (1oo1, 1 out of 1)

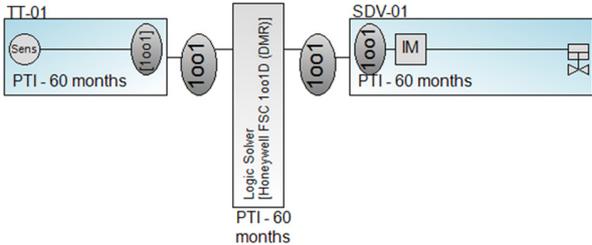


Fig. 5. Base condition SIS configuration.

Base Condition 설계 기준을 토대로 소프트웨어를 활용한 SIS에 대한 PFD_{avg} 값 결과는 1.27×10^{-2} (RRF=79)이다. 하지만 이 결과값은 이전 LOPA 결과에서 나온 허용 가능한 위험 수준을 맞추기 위해 필요한 PFD_{avg} 값이었던 2×10^{-3} (RRF=500)을 만족시키지 못하는 것으로 확인되었다. 따라서 SIL등급을 향상시키기 위한 추가적인 방안을 적용하여 RRF 값이 500이 넘도록 하여야 한다.

추가적인 방안으로는 현재 설계되어 있는 SIS의 구성을 복수화 (Redundancy)하여 보다 높은 신뢰성을 갖도록 하는 방안을 고려할 수 있고, SIS의 점검 주기를 줄여서 평균 고장 주기를 줄이는 방안도 고려하고자 한다^{7,18,19)}.

3.3.2 복수화 (Redundancy)방안

첫 번째 방안으로 SIS의 Sensor 및 Final Element에 대한 복수화를 반영한 결과는 Table 7과 같다.

우선 현재 센서인 Temperature Transmitter가 1oo1(1 out of 1)으로 설계되어 있지만, 센서를 다양한 Voting 구성으로 복수화하였을 경우들에 대한 PFD_{avg} (1/RRF) 값을 산출하였다.

Fig. 6에서 볼 수 있듯이 1oo2, 1oo3, 1oo4로 센서의 개수를 늘릴수록 PFD_{avg} 값이 작아져서 RRF가 증가됨을 알 수 있다. 또한 Final Element인 SDV-01의 개수를 하나 추가하여 1oo2 구성을 할 경우에는 RRF가 크게 증가하였다. 하지만, 센서의 개수가 증가될수록 센서의 오작동될 확률도 증가될 수 있어서 원하지 않는 운전 중단(Shutdown)을 야기시킬 수 있다.

따라서 운전 가용성 (Availability)측면을 같이 고려할 필요가 있다¹¹⁾. 또한 센서의 개수를 늘릴수록 경제적 비용이 증가하므로 개수를 늘리는 것을 최소화하면서

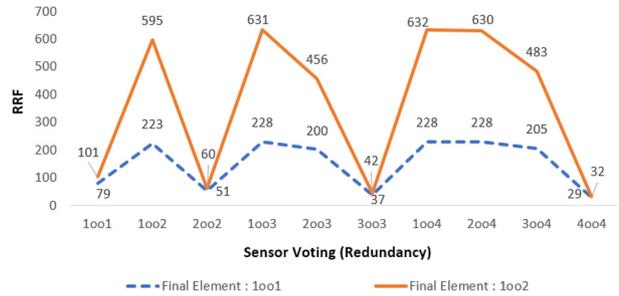


Fig. 6. Evaluation of RRF for redundancy sensors & final elements.

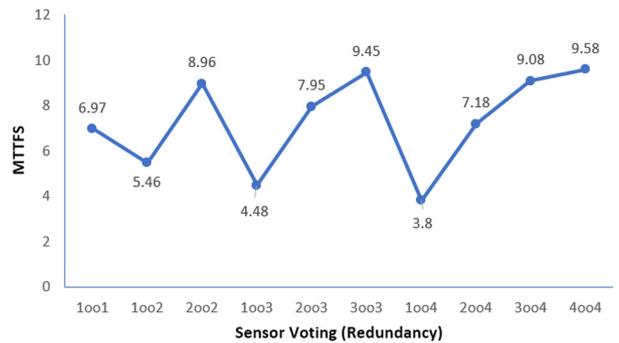


Fig. 7. Evaluation of MTTFS for redundancy of sensors.

최대한의 가용성(Availability)을 가질 수 있는 구성이 필요하다.

Fig. 7은 오작동률을 나타내주는 평균 오작동 고장 시간(Mean Time To Failure Spurious: MTTFS)이다. MooN (M out of N) 구조로 생각하면 센서의 개수인 N을 고정한 상황에서 실제 SIF가 작동하게 만드는 유효한 센서의 개수인 M을 늘릴수록 오작동 발생하는데 걸리는 고장 시간이 늘어나므로 가용성은 향상됨을 알 수 있다¹⁸⁾.

3.3.3 점검 주기 (Proof Test Interval) 변경 반영 결과

두 번째 방안으로 SIS의 점검 주기에 대해 변경하여 반영한 결과를 확인하였다. 현재 점검 주기가 60개월

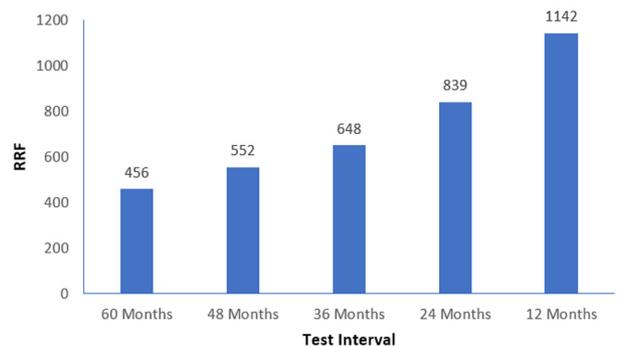


Fig. 8. Evaluation of RRF for proof test intervals.

로 설정하였지만 48, 36, 24, 12개월로 주기를 줄이면서 RRF값을 산출하였다. Fig. 8에서 볼 수 있듯이 점점 주기를 줄일수록 산출된 RRF값이 높아지는 것을 알 수 있다. 초기 설정하였던 60개월에서 12개월로 줄이면 RRF가 2.5배까지 증가하였다.

3.3.4 Improved Condition 반영 기준 결과

복수화 방안 적용을 통해 나온 결과들 중에서 신뢰도와 운전 가용성을 둘 다 고려하기 위해 일정 수준을 기준하여 선별 작업하였다. 신뢰도의 경우 Fig. 6에서 RRF의 값을 400으로 기준하여 이보다 넘는 케이스들을 우선 선택하였고, 운전 가용성은 Fig. 7의 평균 오작동 고장 시간 (MTTFS)이 7 years 이상의 케이스들만 선택한다면, 2003, 2004, 3004 세 가지 케이스들이 RRF 400 이상, MTTFS 7년 이상의 조건을 만족하는 구성으로 선별할 수 있었다. 이 중에 센서의 개수가 4개인 2004, 3004로 구성할 경우에는 경제적 비용의 부담이 있으므로 센서의 개수를 3개로 제한한다면 가장 최적화된 센서 구성은 2003라고 판단할 수 있다. 또한 Final Element의 개수도 하나 더 추가한 1002 구성을 통해 RRF를 추가로 증가시킬 수 있도록 반영하였다.

점검 주기 (Proof Test Interval)는 초기 설정값이었던

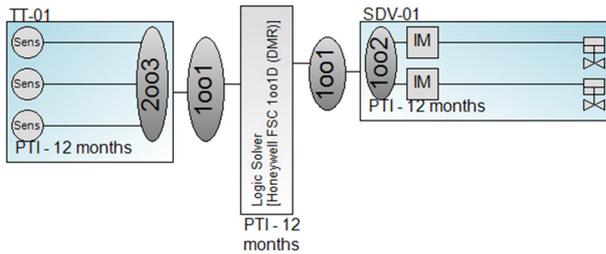


Fig. 9. Improved SIS configuration.

Table 7. PFDavg. & RRF results for voting cases

Voting case	Sensor (TT-01) voting cases		Final element (SDV-01) 1002 case		
	PFD _{avg.}	RRF	PFD _{avg.}	RRF	MTTFS [years]
1001	1.27E-02	72	9.87.E-03	101	6.97
1002	4.48E-03	223	1.68.E-03	595	5.46
2002	1.95E-02	51	1.68.E-02	60	8.96
1003	4.39E-03	228	1.58.E-03	631	4.48
2003	5.00E-03	200	2.20.E-03	456	7.95
3003	2.67E-02	37	2.40.E-02	42	9.45
1004	4.39E-03	228	1.58.E-03	632	3.8
2004	4.39E-03	228	1.59.E-03	630	7.18
3004	4.87E-03	205	2.07.E-03	483	9.08
4004	3.39E-02	29	3.12.E-02	32	9.58

Table 8. PFDavg. result of improved condition

	PFD _{avg.}	RRF	SIL
Improved condition	8.76E-04	1142	SIL 3
Base condition	1.27E-02	79	SIL 1

60개월에서 12개월로 줄여서 반영함으로써 크게 향상된 신뢰도를 갖는 SIS로 만들 수 있다.

결론적으로 두 방안을 모두 반영한 Improved condition으로 PFD_{avg.}를 최적화되게 낮출 수 있는 향상된 SIS의 구성은 Fig. 9와 같다. 향상된 SIS의 Improved Condition 구성을 반영하여 PFD_{avg.}값을 소프트웨어를 이용하여 산출하였고, 결과는 Table 8과 같이 PFD_{avg.}값이 8.76 × 10⁻⁴ (RRF=1142)로 나왔다. 이 값은 LOPA 결과에서 나온 허용 가능한 위험 수준을 맞추기 위해 필요한 값이었던 2 × 10⁻³ (RRF=500) 결과값을 만족시킬 뿐 아니라 ‘SIL 3’ 등급으로 향상시켰다.

4. 결론 및 고찰

본 연구를 통해 On-Site 수소충전소 개질기의 Temperature High High 기능을 갖고 있는 SIS의 안전무결수준(SIL) 향상을 통해 충전소의 리스크를 허용 가능한 수준까지 감소시킬 수 있는 것을 확인하였다.

개질기에서 발생 가능한 최악의 사고 시나리오 확인 및 SIS의 요구되는 SIL값을 결정하기 위해 HAZOP, LOPA 분석을 하였고, 소프트웨어를 활용한 SIL 검증을 통해 요구되는 SIL값을 만족시키는지 확인하였다. 또한 추가 대안을 반영하여 SIL을 향상하여 요구되는 SIL 값을 만족함으로써 충전소의 리스크를 줄였다.

연구 결과를 요약하면 아래와 같다.

1) HAZOP 분석을 통해 개질기의 Temperature Control Failure로 인한 개질기 Rupture 및 화재·폭발 사고로 인한 인명 피해 시나리오를 확인하였다.

2) LOPA 분석을 통해 Temperature High High 기능을 갖는 SIS의 요구되는 SIL 값은 ‘SIL 2’이고, PFD_{avg.} 값은 2 × 10⁻³ (RRF=500) 임을 확인하였다.

3) 소프트웨어를 활용하여 Base Condition의 PFD_{avg.} 값을 검증하였지만, 산출된 PFD_{avg.} 결과값은 1.27 × 10⁻² (RRF=79), SIL 1’ 수준으로 만족하지 못하였다.

4) SIS 구조의 복수화 및 점검주기를 줄이는 방안을 고려하였고, 방안이 고려된 Advanced Condition의 PFD_{avg.} 값은 8.76 × 10⁻⁴ (RRF=1142)로써 ‘SIL 3’까지 향상하여 요구되는 SIL값을 만족시켰다.

결론적으로 개질기의 최악의 사고 시나리오에 대해 허용 가능한 위험도 수준으로 SIL값을 향상시켜 만족

시킴으로써 수소 충전소의 리스크를 감소시켰다.

이번 연구를 통해 안전계장시스템의 복수화 구성 (Sensor의 2oo3 구성, Final Element 1oo2 구성) 및 점검 주기의 감소가 작동 요구 시 고장 확률(PFD_{avg})을 최소화하고 시스템의 SIL값을 향상시켜 안전성을 확보할 수 있으므로 수소충전소의 위험도를 줄이기 위한 중요한 요소임을 확인하였다.

다만, 안전계장시스템의 구성 및 점검 주기의 변경은 실제 수소 충전소의 경제적 비용 및 실제 운용 측면을 고려하여 반영될 수 있도록 추가 연구가 필요하다.

References

- 1) H. R. Gye and C. J. Lee, "Fire Risk Assessment on Urban Hydrogen Refueling Station Using Probit Model", *Korean Journal of Hazardous Materials*, Vol. 7, No. 1, pp. 19-26, 2019.
- 2) D. H. Lee, I. H. Jung and J. W. Ko, "A Study on Safety of Hydrogen Station", *Journal of the Korean Institute of Gas*, Vol. 13, pp. 45-51, 2009.
- 3) H. Kim, S. K. Kang and Y. S. Huh, "Accidents Analysis of Domestic and Overseas Refueling Stations and Assessment of Dangerous Distance by Gas Leak", *Journal of Energy Engineering*, Vol. 26, No. 4, pp. 7-13, 2017.
- 4) S. I. Hwang, S. K. Kang and Y. S. Huh, "A Study on the Safety Improvement by CFD Analysis for Packaged Type Hydrogen Refueling System", *Trans. of Korean Hydrogen and New Energy Society*, Vol. 30, No. 3, pp. 243-250, 2019.
- 5) J. N. Park, "Status of Hydrogen Station Technology and Policy", *Applied Chemistry for Engineering*, KIC News, Vol. 21, No. 3, pp. 10-19, 2018.
- 6) J. O. Han, "A Development of Engine and Fuelling Station for HCNG Fueled City Bus", Final Report for Project - A Development of Engine and Refueling Station for HCNG Fueled City Bus, Korea Environmental Industry & Technology Institute, 2016.
- 7) H. S. Kwak and D. J. Park, "A Study on the Improvement of Reliability of Safety Instrumented Function of Hydrodesulfurization Reactor Heater", *J. Korean Soc. Saf.*, Vol. 32, No. 4, pp. 7-15, 2017.
- 8) Y. C. Jin, "Technical Guide for HAZOP Methodology of Continuous Process System", The Korea Occupational Safety and Health Agency (KOSHA), P-82-2012, 2012.
- 9) A. Kumar, M. Baldea and T. F. Edgar, "A Physics-based Model for Industrial Steam-methane Reformer Optimization with Non-uniform Temperature Field", *Computers and Chemical Engineering*, Vol. 105, pp. 224-236, 2017.
- 10) G. S. Lee, "Technical Guide for LOPA Methodology", The Korea Occupational Safety and Health Agency (KOSHA), P-113-2012, 2012.
- 11) A. C. Torres-Echeverria, "On the use of LOPA and Risk Graphs for SIL Determination", *Journal of Loss Prevention in the Process Industries*, Vol. 41, pp. 333-343, 2016.
- 12) K. Tae. Song and S. I. Lee, "Quantitative Risk Reduction Model according to SIL Allocated by Risk Graph for Railway Platform Door System", *J. Korean Soc. Saf.*, Vol. 31, No. 5, pp. 141-148, 2016.
- 13) M. S. Baek, H. A. Jang, and H. M. Kwon, "A Model of Operational Situation Analysis with Functional Safety for ASIL Determination", *J. Korean Soc. Saf.*, Vol. 29, No. 4, pp. 160-167, 2014.
- 14) International Electrotechnical Commission, "IEC 61508: 2010 Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems", Part 1-7, 2010.
- 15) International Electrotechnical Commission, "IEC 61511: 2010 Functional Safety-Safety Instrumented Systems for the Process Industry Sector", Part 1-4, 2010.
- 16) A. M. Dowell, "Layer of Protection Analysis: Simplified Process Risk Assessment", Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), 2001.
- 17) J. H. Kim, D. J. Lee, H. H. Lee and M. G. Chun, "Safety Evaluation according to Controller Configuration using Safety Integrity Level", *The Transactions of the Korean Institute of Electrical Engineers*, Vol. 66P, No. 1, pp. 43-47, 2017.
- 18) A. C. Torres-Echeverria, S. Marotrell and H. A. Thompson, "Modeling Safety Instrumented Systems with Moon Voting Architectures Addressing System Reconfiguration for Testing", *Reliability Engineering and System Safety*, Vol. 96, pp. 545-563, 2011.
- 19) I. J. Lee and R. H. Kim, "Safety Enhancement of LPG Terminal by LOPA & SIF Method", *Korean Chem. Eng. Res.*, Vol. 53, Issue 4, pp. 431-439, 2015.