International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33العدد
Part 2 المجلد
January 2024 يناير
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

IMPROVING OVERFILLING PREVENTION SYSTEM OF CRUDE OIL STORAGE TANKS

Ibrahim M. Shaluf, Nuha M. Krir
Department of Chemical Engineering, Faculty of Engineering Sabratha
Sabratha University
ibrahim.m.shaluf@gmail.com, nuhakrir@gmail.com

Abstract
Major hazard installations (MHIs) such as refineries, petrochemical plants and terminals use large capacity storage tanks for storing crude oil and by-products. The major hazards that result from the operation of MHIs are fire, explosion and toxic release. Due to overfilling of the storage tanks, there have been several incidents occurred globally. API 2350 recommends that tanks with flammables should be provided with an Automatic Overfilling Prevention System (AOPS). This is known as a Safety Instrumented System (SIS). The SIS should be reliable and independent from the Basic Process Control System (BPCS) of the tank. For the SIS to be reliable and to perform its function properly, the Safety Integrity Level (SIL) of every Safety Integrity Function (SIF) of SIS should meet targeted criteria. This paper presents some background on SIS, BPCS and SIL levels. This paper also presents the improvement of the overfilling prevention system of crude oil storage tanks in an oil terminal (actuated valve). The basic SIS consists of a sensor, logic solver and final element. Four SIS design options have been studied. The SIS that consists of redundancy of each subsystem is more reliable and should be adopted to prevent the overfilling of the storage tanks

Key words: Storage Tank, Overfilling Prevention System, Safety Instrumented System, Safety Integrity Level, Safety Integrity Function.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33 العدد
Part 2 المجلد
January 2024 يناير
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/ 2024م

تحسين نظام منع الامتلاء الزائد لخزانات النفط الخام

د. ابراهيم محمد شلوف، ا. نهى مختار كرير
قسم الهندسة الكيميائية – كلية الهندسة صبراتة– جامعة صبراتة
ibrahim.m.shaluf@gmail.com, nuhakrir@gmail.com

الملخص:

المنشآت الصناعية ذات الدرجة العالية من الخطورة مثل مصافي تكرير النفط، مجمعات البتروكيماويات ومواني تصدير النفط، تستخدم خزانات ذات أحجام كبيرة لتخزين النفط الخام ومشتقاته وقد ينتج عن تشغيل هذه المنشئات حوادث خطيرة مثل الحرائق والانفجارات وتسرب الغازات السامة ونتيجة الامتلاء الزائد عن الحد المسموح به للخزانات فقد حصلت عدة حوادث في العالم. المعهد الأمريكي للمعايير والمواصفات القياسية 2350 يوصي بضرورة تزويد الخزانات التي تحتوي على مواد قابله للاحتراق بأنظمة أوتوماتيكية (آلية) لمنع الامتلاء الزائد عن الحد المسموح به للخزانات وهو ما يعرف بنظام السلامة الآلي. وأنظمة السلامة الآلية يجب أن تكون لها درجة اعتمادية عالية ومستقلة عن أنظمة التشغيل والمراقبة والتحكم الآلي للخزانات. وللحصول على اعتمادية عالية لنظام الحماية الآلي ليقوم بوظيفته كاملة فيجب أن يكون مستوى أداء السلامة لكل وظيفة من وظائف نظام الحماية مطابقة للمعايير المصمم من اجلها. هذا المقال يقدم ملخص على أنظمة السلامة الآلية وأنظمة التحكم الآلي ومستويات أداء أنظمة السلامة الآلية؛ وأيضا يقدم طرق تحسين مستويات أداء أنظمة السلامة الآلية لخزانات النفط، وذلك عن طريق دراسة خزانات ميناء نفطي. لقد تبين من هذه الدراسة أن أداء أنظمة السلامة الآلية والتي تتكون من حساس ونظام معالجة وصمام طوارئ قد ينجح في أداء وظيفته لمنع الامتلاء الزائد للخزان ولكن أي عطل في هذا الحساس أو نظام المعالجة أو صمام الطوارئ فإن هذا النظام لن يعمل بسبب عدم وجود نظام بديل له يمكن أن يقوم بنفس الوظيفة. لقد تمت دراسة أربع تصاميم لنظام الحماية الآلي للخزانات وأثبتت هذه الدراسة أن نظام السلامة الآلي الذي يتكون من

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

حساسين ونظامي معالجة وصمامي طوارئ للقيام بوظيفة حماية الخزانات من الامتلاء الزائد عن الحد المسموح به هو النظام الأمثل.

الكلمات الدالة: خزانات النفط، أنظمة منع امتلاء الخزان، أنظمة السلامة الآلية، أنظمة المراقبة والتحكم وتشغيل الخزانات.

Introduction

Major hazard installations (MHI) such as refineries, petrochemical plants and terminals use large capacity storage tanks for storing crude oil and by-products. The major hazards that result from the operation of MHI are fire, explosion and toxic release. Of these three, fire is the most common (Daniel A. Crowel and Joseph F. Louvar, 2002). When dealing with tanks operating in process industries or those that store products at a tank farm or terminal, one of the major hazards to avoid is overfilling the tanks. This is especially important with chemicals that may explode, catch on fire or affect the health of people or the environment.

Overfills have resulted in significant process safety incidents. Long for (Australia, 1998), Texas City (United States, 2005), and Buncefield (United Kingdom, 2005) can be traced to the loss of level control leading to a high level and ultimately to loss of containment (Angela E. and William H., 2010). A study of storage tank accidents for the period of 1960 - 2003 covered 242 tank farm accidents. 15 overfill incidents were reported, of which 13 resulted in a fire and explosion (James I., and Cheng-Chung Lin, 2006), (William L., 2014). Insurance data shows that for all the tanks around the world, there is one overfilling incident for every 3,300 filling operations (Lydia Miller, 2019). A study done on tank overfilling incidents by HSE found that an inadequate Layer of Protection Analysis (LOPA) on the processing units was the leading cause, and human factors were the leading source of initiating these events (Colin Jamison, 2019). Experts indicate that the solution to this problem involves the application of a layer of risk reduction which is called safety instrumented systems (SIS) that is specifically designed to perform functions that maintain a process in a safe state when any risk is detected، ensuring the integrity of people,

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

equipment and avoids environmental impacts (Summers and Raney, 1999). Industrial standards API STD 2350 and IEC 61508 / 61511 have been developed to prevent tank overfilling.

This paper presents an overview of SIS, BPCS, and SIL levels. This paper also presents a tank farm storage tanks safeguarded against overfilling by manual overfilling prevention systems. The paper proposes four options of SIS for the improvement of the overfilling prevention system. Option (4), the SIS that consists of redundant of each subsystem is more reliable and should be adopted. Although a redundant system is more reliable, however the redundant system is subjected to common cause failure (CCF). CCF can be overcome by adopting and adapting the Belt and Brace strategy. The provision of SIS does not guarantee overfilling prevention unless the SIL-targeted criteria are maintained during the life cycle of the SIS.

Safeguarding systems

Safeguard systems are an important part of the process plant and equipment, which protects personnel, plant, and the environment from abnormal operating conditions. The safeguarding system consists of layers of protection. The layers of protection are independent measures that reduce the likelihood of undesirable adverse event or the consequence of that event. Generally, all process facilities have more than one protection layers performing its function in a hierarchical manner for maintaining the safe state of the facility if the previous protection layer has failed to protect. The layers of protection are shown in Figure 1.

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

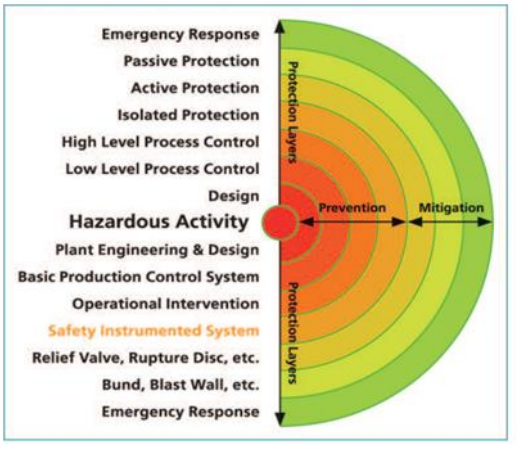

Figure 1. Layers of hazard protection (Richard Harvey, 2009).

BPCS and SIS

BPCS is a system or device which responds to input signals and generates an output signal which causes the equipment or process under control to operate in a particular manner. BPSC is to assist or to replace the operator in maintaining normal process operations despite deviations.

SIS is an instrumentation system that detects out-of-control process conditions, and automatically returns the process to a safe state. It is last line - or near last line - of defense against a chemical process hazard, and it is not part of the BPCS (Kevin J. and Todd M., 2017). SIS as perInternational Electrotechnical Commission IEC 61511 is an instrumented system used to implement one or more safety instrumented functions (SIF) (Prasad Goteti, 2020). There are many other names for SIS for example, Automated Overfill Prevention Systems (AOPS), safety shutdown system, emergency shutdown system, safety interlock, protective instrumented system, or safety critical system. In most cases, each function in SIS consists of three components, a sensor, a logic device, and a final control device as shown in Figure 2.

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

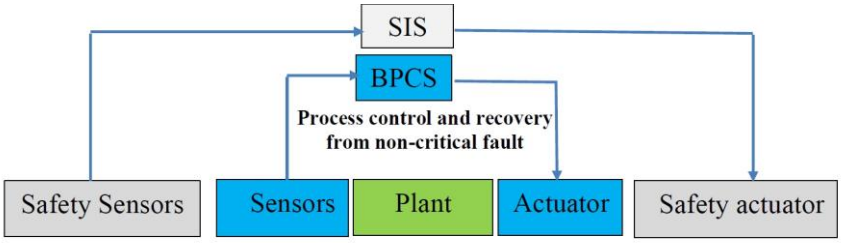

Figure 2. BPCS and SIS for a process (Reinaldo Júnior et al 2011).

Safety Instrumented Function (SIF) is an individual function that has the capability to evaluate a process condition and take action in response to a prescribed unsafe condition. The SIS may implement a single function or multiple functions to protect against various process hazards in a plant. All elements that form the SIS must be designed or selected in accordance with the International Electrotechnical Commission IEC 61508 or IEC 61511 standards (NOGA, 2018). The 3-stage subsystem framework for a SIS, as described in IEC 61508, is shown in Figure 3.

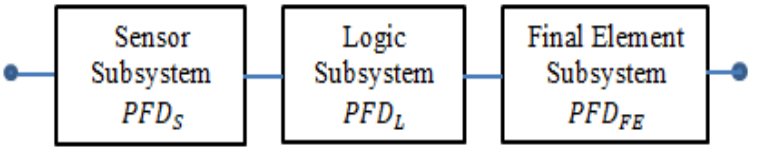

Figure 3. SIS Subsystem framework (Leonard W. Moore, 2015)

This representation can also be seen as a Reliability Block Diagram (RBD) model. As the model consists of three series blocks, the simple rule can be applied that the PFD (probability of failure on demand or failure rate, for that matter) for each block can be summed to establish the relevant parameter$(PFD\ or\ \lambda)$for the system (Leonard W. Moore, 2015).

$$PFD_S + PFD_L + PFD_{FE} = PFD_{SYSTEM} \quad (1)$$

Where:

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

PFD_{SYSTEM} is the probability of failure on demand of the system.
$PFD_S$is the probability of failure on demand of the sensors.
PFD_L is the probability of failure on demand of the SIS logic solver .
PFD_{FE} is the probability of failure on demand of the final control elements.

Safety Integrity Level (SIL)

SIL is an abbreviation for the term Safety Integrity Level which is a safety rating assigned to a safety loop known as Safety Instrumented Function (SIF). SIL determination comes after a detailed analysis and design of a safety's requirement for a process. It can be determined by quantitative or qualitative methods. SIL can also be interpreted as how much of a risk can be reduced, and what the probability is of a failure on demand for an instrument. The average PFD of the system that performs the safety function is one of the key parameters that define the SIL for the safety function, as summarized in Table 1 (IEC 61508, 2000).

Table 1: SIL ranges for low demand safety instrumented functions

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{AVG})
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

The three basic attributes of the SIS that require design consideration and evaluation in order to achieve the SIL are:
1- The architectural constraints for each subsystem are at least SIL 'n' - Constraints are specified in IEC 61508 and IEC 61511 and require minimum degrees fault tolerance. Architectural constraints are established according to the required SIL of the subsystem (i.e., sensors, logic solvers, and final elements), "type" of components used, and Safe Failure Fraction (SFF) of the subsystem's components. Type A components are simple devices not incorporating microprocessors whose failure modes are well

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

understood, and Type B devices are complex devices such as those incorporating microprocessors (Mary A. and Marvin R., 2018).
SFF is a measure of how safe the components respond in the presence of faults. The total failure rate is the sum of failure rates for 'safe' failures, those causing a trip (λ_S), plus the rate of 'dangerous' failures detected by on-line diagnostics (λ_{DD}) and rate of 'dangerous' failures that remain undetected (λ_{DU}):

$$\Sigma\lambda_S = \Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU} \qquad (2)$$

The SFF is the proportion of failures that are either 'safe'(λ_S), or are 'dangerous' but detected by on-line diagnostics(λ_{DD}):

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/\Sigma\lambda \qquad (3)$$

Understandably, equipment suppliers and designers have been creative in trying to prove that SFF ≥ 60% (Generowicz M., 2015). Fault tolerance is an expression of the number of faults that a component, a subsystem, an overall SIF can tolerate and continue to perform its intended function in the presence of such faults. The required minimum fault tolerance per IEC 61511 (2003) is a function of the required SIL level as shown in table 2.

Table 2. Architectural constraints of type A and B elements or subsystems.

Safe Failure Fraction (SFF)	Type A Element or Subsystem			Type B Element or Subsystem		
	Hardware fault Tolerance (HFT)			Hardware fault Tolerance (HFT)		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	No SIL	SIL 1	SIL 2
60% - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% to < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

2- The systematic capability of each subsystem is at least SC 'n' – There are limits to what SIL capability can be claimed for a combination of multiple (redundant) elements in respect of

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

systematic capability. The SC of a combination of elements (arranged in redundancy) is limited to the lowest SC (1, 2, 3) of the elements + 1, providing there is sufficient independence.

3- The probability of failure on demand, PFD_{AVG}. The average PFD of the system that performs the safety function is one of the key parameters that define the SIL for the safety function. PFD is a measure of the effectiveness of an instrument or a safety function. It expresses the likelihood that the instrument or safety function does not work when required to. The PFD_{AVG} for a loop depends on the failure rates of all the components in the loop, and the proof test interval, hence the need to know PFD_{AVG} data for all items in a loop when determining safety integrity level of a loop. Table 3 summarizes the equations of the PFD_{AVG} for 1oo1, 1oo2, 2oo2, and 2oo3 SIS (Kevin J. and Todd M., 2017).

Table 3: Equations of probability of failure on demand

SIS configuration	PFD_{avg}
1oo1	$\left[\lambda_{DU} \times \frac{TI}{2}\right]$
1oo2	$\left[(\lambda_{DU})^2 \times \frac{(TI)^2}{3}\right] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2}\right]$
2oo2	$[\lambda_{DU} \times TI]$
2oo3	$[(\lambda_{DU})^2 \times (TI)^2] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2}\right]$

Crude oil terminal facilities

The terminal provides facilities for crude oil storage, pumping, metering, exporting and services facilities. The terminal has been divided into; tank farm; industrial area; offshore marine facilities; camp area and fire and environmental systems (Ibrahim and Salim, 2010). Figure 4 shows the terminal facilities and Figure 5 shows the tank farm flow diagram.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33 العدد
Part 2 المجلد
January 2024 يناير
ISTJ
تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

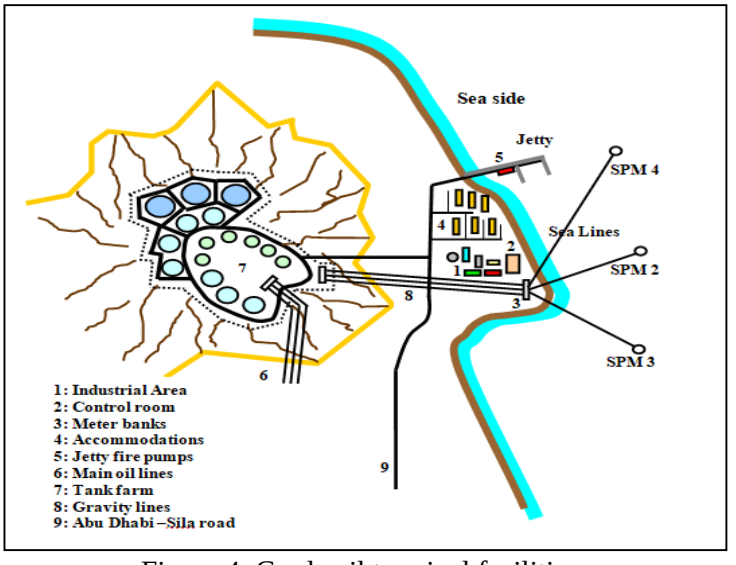

Figure 4: Crude oil terminal facilities

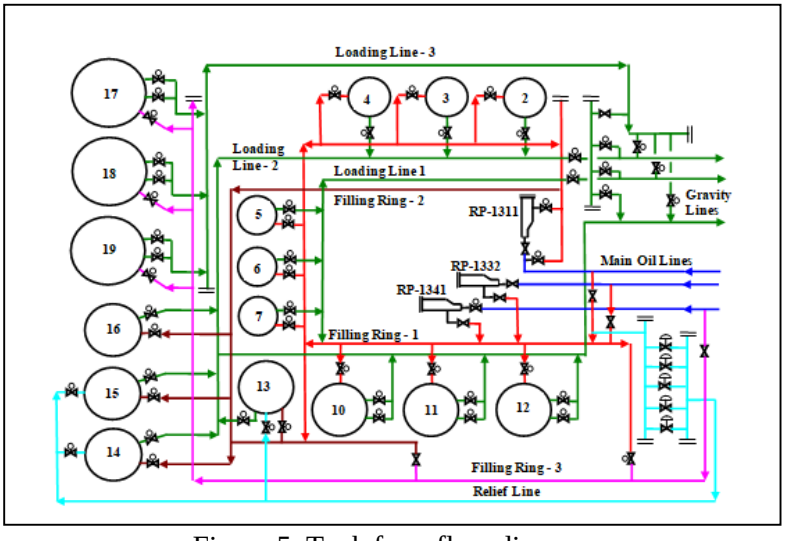

Figure 5. Tank farm flow diagram

Crude oil storage tank farm

A tank farm consists of sixteen floating roof storage tanks with capacity of 8.3 Million Barrels. The tanks are classified as six small, seven medium and three large tanks. Storage tank sizes, capacity,

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

flow rates in and out and the elevation above the sea level are summarized in Table 4.

Table 4: JD floating storage tanks information.

Description	Small tanks (TT 2 – TT 7)	Medium tanks (TT 10 – TT16)	Large tanks (TT 17 – TT19)
Diameter	165 ft	260 ft	335 ft
Overall height	64 ft	64 ft	64 ft
Overall weir	60 ft	60 ft	60 ft
Maximum Operating height	56 ft	56 ft	56 ft
Minimum operating height	6 ft	6 ft	6 ft
Maximum operating capacity	213164 barrels	529558 barrels	823452 barrels
Maximum flow in	5708 b/h	18333 b/h	41667 b/h
Maximum flow out	16126 T/h	32252 T/h (TT10 - 12) 24922 T/h (TT13 - 16)	73300 T/h
Elevation above sea level	210.5 ft	210.5 ft	223.5 ft

The storage tanks are atmospheric floating roof tanks. The small and large tanks have double deck roofs. The medium tanks have pan roofs. Floating roof tanks require special precautions to safeguard against the possibility of overflowing the tank and damaging the seals, sinking a roof, or damaging a roof by landing it inadvertently. The storage tanks are operated remotely from the central control room in the industrial area. However, there is a tank farm control room from which tank farm operations could be handled in emergency situations except the fire alarms which are operable from the central control room only. Supervisory Control and Data Acquisition (SCADA) control system is housed in the central control room. The SCADA incorporates the crude measurement system, electronically operates all motorized valves, loading pump controls, proving sequencers, remote tank level indicators and telecommunication with Company Main Office. Each storage tank has a minimum operating height to avoid inadvertent landing of

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33العدد
Part 2 المجلد
January 2024 يناير
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

roofs during normal operations which would result in considerable damage and present fire hazards. Each storage tank also has a maximum operating height to prevent overfilling with resultant roof shoes and seals damage, also potential fire risk and oil spill. High and low level alarms are provided in all tanks, which actuate in the central control room. Figure 6 shows the tank TT-15 level heights during 2010. The lowest level height was recorded 6.5 feet and the maximum level height was 54.2 feet.

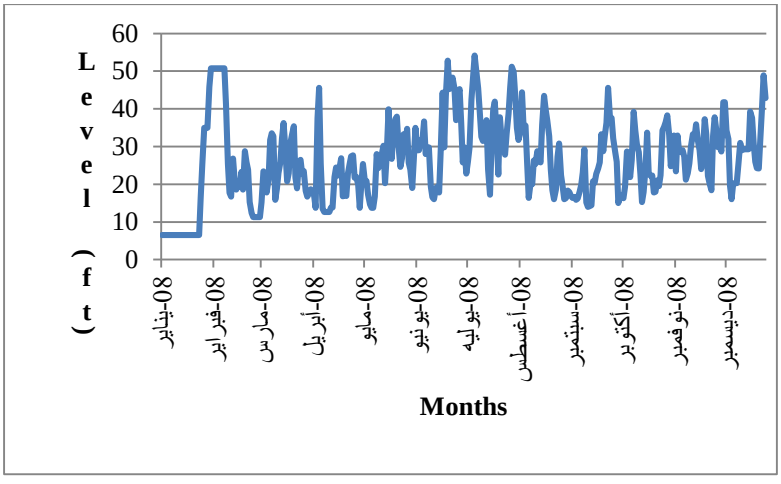

Figure 6. Tank 1503 level heights

Existing Condition

Capacity determination is the one of the first steps in designing the tank. The maximum capacity of the tank is shown in Figure 7. The maximum or total capacity is the sum of the inactive capacity (minimum operating volume remaining volume in tank), actual or networking capacity and overfill protecting capacity. The networking capacity is the volume of available product under normal operating conditions, which is between the low liquid level (LLL) and the high liquid level (HLL) (Kuan, Siew Yeng, 2009).

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

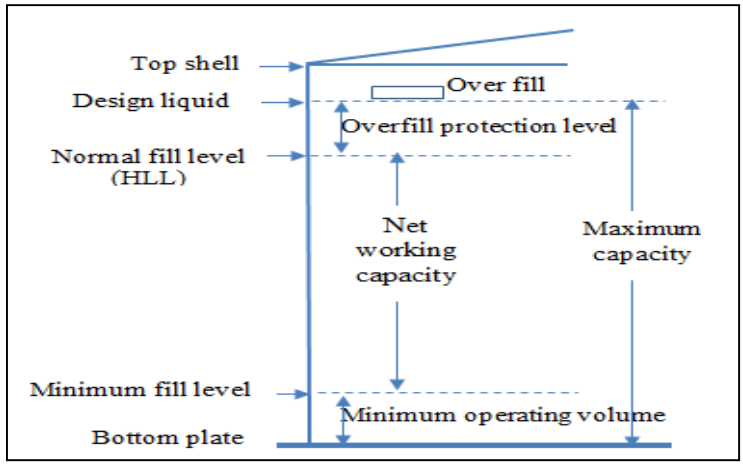

Figure 7. Maximum capacity of storage tank (Kuan, Siew Yeng, 2009), (Mark Baker, 2009).

Storage tank level control system uses one independent sensor for automatic continuous tank gaging. It uses a separate level sensor for high liquid level detection for overfill protection system alarm. In case of emergency the isolation valve can be shut off local or through remote hand switch. Figure 8 shows the Level control and manual overfill prevention systems.

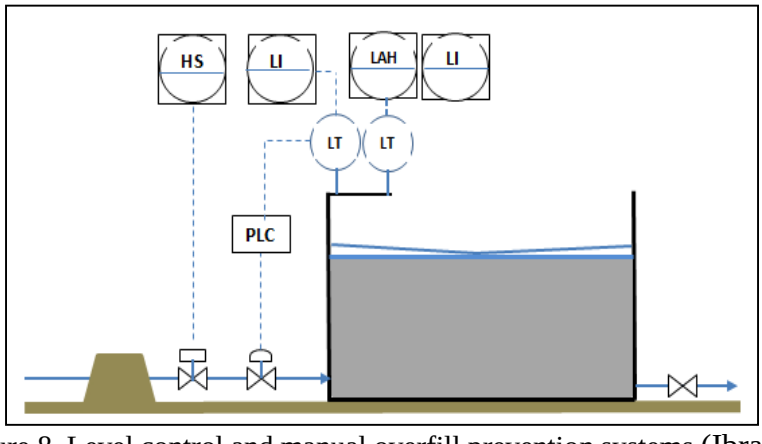

Figure 8. Level control and manual overfill prevention systems (Ibrahim and Salim, 2010).

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

SIS of the storage tanks

Codes (ANSI/API 2350), (Colin Chambers et al., 2009), (IChemE, 2007), (EI, 2013) recommend an Automated Overfill Prevention Systems (AOPS) for tanks with flammables and complex operations. The AOPS should be a reliable system. The reliable system often uses redundancy techniques. A parallel system will be more reliable than systems made up with only single components using no redundancy at all.

Therefore the SIS of the storage tank should be upgraded and it has to be reliable system. The SIS should be designed to include high high level sensors (HHLS), logic solvers and emergency shutdown valves. There is an existing emergency shutdown valve located inside the tank bund provided with fire proof box which can with stand fire up to half an hour. Figure 9 shows an existing control system and a proposed SIS system for atmospheric storage tank

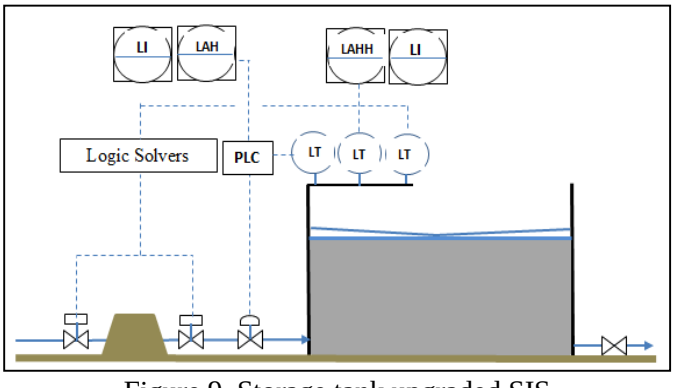

Figure 9. Storage tank upgraded SIS

Identification of hazards and SIL determination

Hazard and Operability Study (HAZOP) is used to identify where protection and the safety functions are required, whilst SIL determination methods such as fault tree analysis, LOPA or risk graph are used to determine the required target SIL i.e. identification of the 'safety integrity'.HAZOP study is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

personnel or equipment, or prevent efficient operation. HAZOP is a qualitative technique based on guide-words. The objectives of the HAZOP is to identify all deviations, their causes, the hazards and operability problems associated with these deviations, and actions are required to control the hazards and/or the operability problems (Stein Haugen and Marvin Rausand, 2011). The HAZOP of the storage tanks was carried out and summarized in Table 5.

Table 5: The HAZOP of the storage tank

Deviation	Cause	Consequences	Measure
Level high	Faulty level measurement, defective sensor	Over flow, possible damage of floating roof and major fire	Over fill protection
Level high	Defective valve, valve fail open	Over flow, possible damage of floating roof and major fire	Over fill protection

Risk graph method

The original Risk Graph is in principle a qualitative method. The method included in IEC 61508 Part 5 Annex E (IEC 61508, 2010). This method allows selection the SIL level by a simplified analysis based on the knowledge of the risk factors associated to the process and its control system. The method consists of a tree-like graph where each stage represents one risk factor and the branches the different values that each factor can take. A Risk Graph intends to make a graded assessment a hazardous scenario based on a series of parameters that represent those risk factors considering that there is not a SIF in place. The SIL is worked out selecting each parameter from a pre-determined set of values (Alejandro Torres-Echeverria, 2014).

The risk graph was carried out for the storage tanks and shown in Figure 10.

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

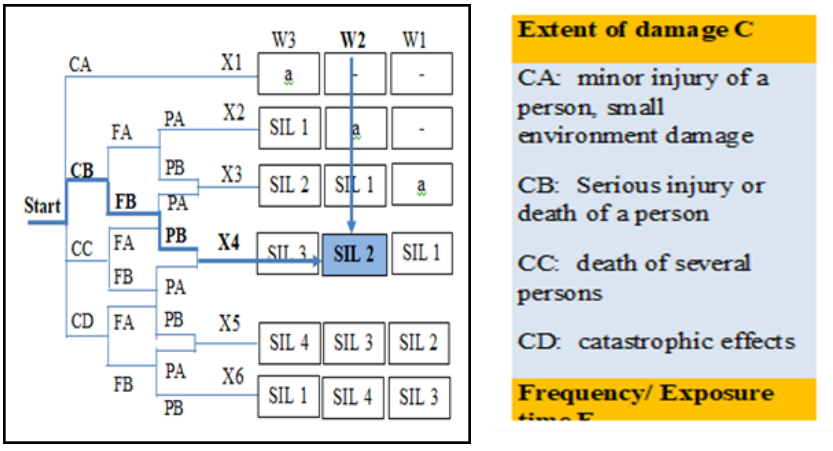

Figure 10. Risk graph of the storage tank

As per the risk graph findings the SIS should be designed and maintained during operation to meet at least SIL2. Therefore the Architectural Constraints (AC) of the SIS and it capability to carry out its safety function as well as the probability of failure on demand should be studied to design SIS meets the targeted SIL2.

Architectural Constraints

Four options have been considered for the SIL estimation of the storage tank SIS. The subsystem configuration, type of the safety subsystem, SFF, HFT, SC, AC and finally the SIL for the system for each option was estimated and summarized in Table 6.

Table 6: AC and the SIL for each option.

Safety function							
Options	**Subsystem**	**Type**	**SFF**	**HF**	**SC**	**AC**	**SIS**
Option (1)	**Level Transmitter (1oo1)**	A	90 – 99%	0	1	SIL3	SIL2
	Logic solver (1oo1)	B	90 – 99%	0	1	SIL2	
	Actuated valve (1oo1)	A	60 – 90%	0	1	SIL2	
Option (2)	**Level Transmitter (1oo2)**	A	90 – 99%	1	2	SIL4	SIL2

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

	Logic solver (1oo1)	B	90 – 99%	0	1	SIL2	
	Actuated valve (1oo1)	A	60 – 90%	0	1	SIL2	
Option (3)	**Level Transmitter (1oo2)**	A	90 – 99%	1	2	SIL4	SIL2
	Logic solver (1oo1)	B	90 – 99%	0	1	SIL2	
	Actuated valve (1oo2)	A	60 – 90%	1	2	SIL3	
Option (4)	**Level Transmitter (1oo2)**	A	90 – 99%	1	2	SIL4	SIL3
	Logic solver (1oo2)	B	90 – 99%	1	2	SIL3	
	Actuated valve (1oo2)	A	60 – 90%	1	2	SIL3	

In option (1) the system consists of one level sensor, one logic solver and one actuated valve. The level sensor is Type A and has SFF of 90 - 99%. With reference to Table 2 when used on its own it has HFT = 0, with system capability (SC1) the input subsystem has AC that meets SIL 3. The logic solver is Type B and has SFF of 90 - 99%. With reference to Table 2, with HFT = 0, SC1 the logic subsystem has AC that meets SIL 2.
The actuated valve is Type A and has SFF of 60 - 90%. With reference to Table 2, with HFT = 0, SC1 the output subsystem has architecture constraint AC meets SIL 2. SIS meets the AC and SC for SIL2.

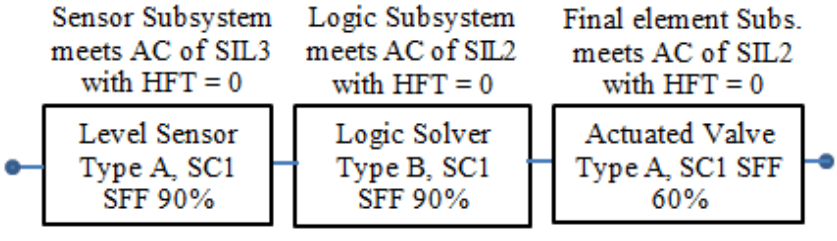

Figure 11. Reliability block diagram for option (1)

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

SIL2 can be achieved for the system with single element in each subsystem. This is reflected in the reliability block diagram (RBD) in Figure 11 for the system.

In option (2) the system consists of two level sensors, one logic solver and one actuated valve. The level sensor is Type A and has SFF of 90 - 99%. With reference to Table2 when one sensor out of two sensors (1oo2) used, the subsystem has HFT = 1, with SC2 and the input AC that meets SIL 4. The logic solver is Type B and has SFF of 90 - 99%, with HFT = 0, SC1 and the logic subsystem has AC that meets SIL 2. The actuated valve is Type A and has SFF of 60 - 90%, with HFT = 0, SC1 the output subsystem has architecture constraint AC meets SIL 2. The option (2) SIS meets the AC and SC for SIL2. Figure 12 shows the reliability block diagram.

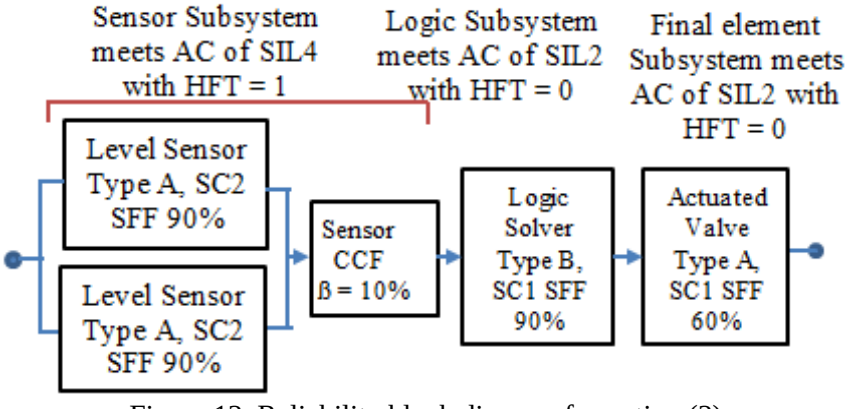

Figure 12. Reliability block diagram for option (2)

In option (3), SIS meets the AC and SC for SIL2 and in option (4) SIS meets the AC and SC for SIL3.

Probability of failure on demand

The failure rate data used for the calculation are collected from literature (Paul Reeve, 2014), (Leonard W. Moore, 2015) and summarized in Table 7.

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

Table 7. The failure rate data.

Parameter	Level Transmitter	Logic solver	Actuated valve
Dangerous undetected failure rate, $\lambda_{DU}(hr)^{-1}$	2.5×10^{-8}	8.6×10^{-8}	2.8×10^{-7}
Dangerous detected failure rate, $\lambda_{DD}(hr)^{-1}$	1.4×10^{-7}	1.7×10^{-7}	4.5×10^{-7}
Safe failure rate, $\lambda_S(hr)^{-1}$	1.3×10^{-7}	6.6×10^{-7}	4.5×10^{-7}
Common cause factor for undetected failures, β	10%	10%	10%
Proof Test Interval, TI	**1yr (8760 hr.)**	**1yr (8760 hr.)**	**1yr (8760 hr.)**

The average probability of failure on demand was calculated for each option as per the equations in Table 3. The SIL rating was determined from Table 1 for each option. Table 8 summarizes PFD_{AVG} and SIL rating for each option.

Table 8. PFD_{AVG} and SIL rating for each option.

Options	Subsystem	PFD_{AVG}	PFD_{AVG}	SIL
Option (1)	LT ($1oo1$)	1.1×10^{-4}	1.7×10^{-3}	SIL2
	LS ($1oo1$)	3.7×10^{-4}		
	AV ($1oo1$)	1.2×10^{-3}		
Option (2)	LT ($1oo2$)	1.1×10^{-5}	1.6×10^{-3}	SIL2
	LS ($1oo1$)	3.7×10^{-4}		
	AV ($1oo1$)	1.2×10^{-3}		
Option (3)	LT ($1oo2$)	1.1×10^{-5}	5.6×10^{-4}	SIL3
	LS ($1oo1$)	3.8×10^{-4}		
	AV ($1oo2$)	1.7×10^{-4}		
Option (4)	LT ($1oo2$)	1.1×10^{-5}	2.2×10^{-4}	SIL3
	LS ($1oo2$)	3.8×10^{-5}		
	AV ($1oo2$)	1.7×10^{-4}		

Discussions

The floating roof storage tanks receive crude oil from oil fields for the aim of storage and exporting. The BPCS maintain the liquid

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

level less than 85% and higher than 1% in order to keep the valve open. The crude oil storage tanks provided with manual overfill prevention system. The system consists of level sensor, programmable logic controller (PLC) and high level alarm (HLA). If the level reaches above 85% high level alarm will be activated and warns the operator in the control room to close the inlet valve remotely. Although the tank farm did not experience any overfilling incidents however there have been several incidents occurred globally. In addition to that API 2350, IChemE etc. recommend an Automated Overfill Prevention Systems (AOPS) for tanks with flammables and complex operations. Therefore the crude oil storage tanks should be provided with automatic prevention system.

In this case study it is proposed to install an automatic overfill a prevention system which is known as SIS. The SIS system consists of level sensor (high high level sensor), logic solver and emergency shutdown valve.

Another margin in the tank level should be given to install the high high level sensor with high high level alarm (HHLA). If the high high level is reached the HHLA will be activated in the control room and SIS will automatically shut down the trip valve. The SIS of the storage tanks should be designed to be reliable to prevent any overfilling conditions. As per the risk graph analysis, SIL2 rating is required to prevent any overfilling situation. Four options have been studied. Although option (1) which consists of level sensor, logic solver and actuated valve meets the SIL2, however the HFT is zero for each subsystem therefore failure of any subsystem will not return back the process to safe state. Option (2) meets the target SIL but the HFT is zero for the logic solver and actuated valve, so if the logic solver or the valve are failed the SIS does not capable to return back the process to safe condition. Option (3) meets SIL2 targeted criteria but the HFT of the valve is zero so if the valve fail open the SIS cannot prevent the overfill operation of the tank. Each subsystem in option (4) is configured on (2oo2) and has HFT equal one. As far as the actuated valve is concerned, the existing valve is already installed inside the tank bund but the redundant valve should be placed outside the bund.

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

In SIS option (4) if any element of the subsystem fails the whole system can fulfill its function and return back the process to safe state in addition to that option (4) SIS meets SIL3 which is more than the SIL targeted requirements. Although option (4) is more expensive in terms of the cost of redundant subsystems and their proof testing, however the system is more reliable. Therefore SIS option (4) should be adopted.

Conclusions

The crude oil storage tanks are monitored and operated by BPCS. The storage tanks are provided with manual overfilling prevention system. The system depends on an operator to close the valve remotely in case of high level alarm is activated. If the operator fails to respond to the high level alarm it will expose the tanks to overfilling.

In this case study it is proposed to install SIS as recommended by international standards. The SIS has to be designed to include high level sensors, logic solvers and emergency shutdown valves. The SIS of the storage tanks should be designed to be reliable.

As per the risk graph analysis SIL2 rating is required to prevent any overfilling situation. Four options of SIS have been evaluated for the improvement of overfilling prevention system. Option (4), the SIS that consists of redundant of each subsystem is more reliable than other options and it should be adopted.

Although redundant system is more reliable however the redundant system is subjected to common cause failure (CCF). CCF can be overcome through adopting and adapting the Belt and Brace strategy (diversity).

References

Alejandro Torres-Echeverria, 2014, On the Use of LOPA and Risk Graphs for SIL determination, 17th Annual International Symposium, October, 28 – 30, 2014. College Station, Texas.

Angela E. Summers, William Hearn, 2010, Overfill Protective Systems - Complex Problem, Simple Solution, SIS TECH

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

ANSI/API Standard-2350, 2012, Overfill Protection for Storage Tanks in Petroleum Facilities, 4th Edition 2012, American Petroleum Institute.

Colin Chambers, Jill Wilday & Shane Turner, 2009, A Review of Layers of Protection Analysis (LOPA) Analyses of Overfill of Fuel Storage Tanks, RR716, Health and Safety Executive (HSE).

Colin Jamison (2019) "A Study of Tank Overfill Incidents" https://engineering.purdue.edu/P2SAC/presentations/documents/Analysis_of_Tank_Overflow_Incidents_Fall2019.pdf

Crowl, D. A., Louvar, J. f., 2000, Chemical Process Safety Fundamentals with Applications, Second Edition, Prentice Hall International Series.

Energy Institute (EI), 2013, Model Code of Safe Practice Part 2 - Design, Construction and Operation of Petroleum Distribution Installations, 4th Ed 2013.

Ibrahim Shaluf, and Salim Abdulla, 2010, An Overview on ADCO Crude Oil Storage Tanks, Disaster Prevention and Management Journal, Vol. 19 no. 3.pp. 370 – 383.

IChemE, 2007, Recommendations on the Design and Operation of Fuel Storage Sites, Buncefield Major Incident Investigation Board.

IEC 61508, 2000, Functional safety of electrical/electronic/ programmable electronic safety-related systems, International Electrotechnical Commission, Geneva.

IEC 61508. 2010, Functional Safety of Electrical / Electronic / Programmable Electronic Safetyrelated systems, Parts 1-7, 2nd Edition. International Electrotechnical Commission, Geneva, Switzerland, 2010.

IEC 61511, 2003, Functional safety – Safety instrumented systems for the process industry sector, International Electrotechnical Commission, Geneva.

James I. Chang, Cheng-Chung Lin, 2006, A Study of Storage Tank Accidents, Journal of loss prevention in process industries, 19, 51 – 59, (2006).

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

Kevin J. Mitchell and Todd M. Longendelpher, 2017, Safety Instrumented Systems, Engineering Handbook, Kenexis Consulting Corporation – Columbus, OH

Kuan, Siew Yeng, 2009, Design, Construction and Operation of the Floating Roof Tank, A dissertation Bachelor of Engineering, Faculty of Engineering and Surveying, University of Southern Queensland.

Leonard W. Moore, 2015, Logic Solver for Tank Overfill Protection, Moore Industries International Inc.

Lydia Miller, 2019, A systemic approach to storage tank overfill protection, https://www.piprocessinstrumentation.com/instrumentation/level-measurement/article/15564213/a-systemic-approach-to-storage-tank-overfill-protection Accessed on (5 August 2023)

Mark Backer (2009), The Basic of API 650 – National Institute For Storage Tank Management – Conference and Trade Show, September 11, 2009, Houston, Texas.

Mary Ann Lundteigen and Marvin Rausand, 2018, Extension to Chapter 2. Architectural Constraints, NTNU-Trondheim, Norwegian University of Science and technology.

Mirek Generowicz, 2015, Achieving Compliance in Hardware Fault Tolerance, Safety Control Systems Conference.

Norwegian Oil and Gas Association (NOGA), 2018, Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, Norwegian Oil and Gas Association.

Paul Reeve, 2014, Practical SIS design and SIL verification, The Institute of Measurement and Control, Silmetric Ltd.

Prasad Goteti, 2020, SAFETY LIFE CYCLE PER IEC / ISA 61511, Purdue Process Safety and Assurance Center (P2SAC), https://engineering.purdue.edu/P2SAC/presentations/documents/Safety_Life_Cycle_Per_IEC_ISA_61511_1.pdf Accessed on (20 July 2023)

Reinaldo Squillante Júnior, Diolino J. dos Santos Filho , Luis Alberto M. Riascos, Fabrício Junqueira , Paulo E. Miyagi, 2011, Mathematical Method for Modelling and Validating of Safety Instrumented System Designed According to IEC61508

تم استلام الورقة بتاريخ: 2023/12/28م وتم نشرها على الموقع بتاريخ:31/ 1/2024م

and IEC 6151, 21st InternationalCongress of Mechanical Engineering, October 24 - 28, 2011, Natal, RN, Brazil.

Richard Harvey, 2009, SIL explained, www.valve-world.netAccessed on (25 July 2023)

Stein Haugen and Marvin Rausand, 2011, Risk Assessment - HAZOP, RAMS Group, Department of Production and Quality Engineering, NTNU.

Summers and Raney, 1999, Common Cause and Common Sense, Designing Failure out of Your Safety Instrumented Systems (SIS), ISA Transactions, Volume 38, Issue 3, July 1999, Pages 291-299

William L. Mostia (2014) “Prevent Tank Farm Overfill Hazards” https://www.controlglobal.com/protect/safety-instrumented-systems/article/11330176/prevent-tank-farm-overfill-hazards accessed on (5 July 2023).