NAFTA-GAZ

Nafta-Gaz 2024, no. 7, pp. 434–441, DOI: 10.18668/NG.2024.07.05

Development of the functional safety system in primary oil refining

Projektowanie systemu bezpieczeństwa funkcjonalnego w procesie rafinacji ropy naftowej

Farid H. Agayev[1], Almaz M. Mehdiyeva[1], Qadir A. Gafarov[1], Sevinj V. Bakhshaliyeva[1], Natella V. Shirinzade[2]

[1]*Azerbaijan State Oil and Industry University*
[2]*Technip Energies Italy S.p.A.*

ABSTRACT: The main objective of this work is to design a Functional Safety System based on a control and measuring devices that ensures the safe and highly efficiency operation of the hydrogen production facility and complies with IEC61508, IEC61511, and IEC60812 international functional safety standards. Providing the proposed project with economically efficient hardware and software is a sub-goal of the work. The objectives set for the designed system have been achieved as follows. The designed Functional Safety Circuits automatically bring the system into a safe state when parameters approach the emergency threshold or in the event of an emergency process violation. They also activate light and sound warning alarms indicating the current condition in the hydrogen production unit. This minimizes the risk of human casualties and environmental damage. As a result of the research, it is suggested that the pressure swing adsorption section of the hydrogen production unit, based on control and measuring devices with functional safety circuits, can operate safely and with higher productivity (producing H_2 gas with a purity of 99.9%, lower carbon emissions) and with enhanced reliability. In the pressure swing adsorption unit, two different functional safety circuits have been implemented. These circuits prevent explosive accidents that could result in human casualties and long-term environmental impact. They work independently of the technology process automation control system to mitigate the consequences of such events. With the proper selection of equipment, the frequency of unplanned and planned maintenance work by engineering and technical staff is reduced, ensuring comfortable operation of the equipment. The proposed control and measuring devices-based Functional Safety Circuits prevent system stops based on safe fault signals by applying SIL2 and SIL3 equipment.

Key words: functional safety, oil refining, technological process, hydrogen, automation.

STRESZCZENIE: Głównym celem niniejszej pracy jest zaprojektowanie systemu bezpieczeństwa funkcjonalnego opartego na urządzeniach kontrolno-pomiarowych, który zapewni bezpieczną i wysoce wydajną pracę instalacji do produkcji wodoru i będzie zgodny z międzynarodowymi normami bezpieczeństwa funkcjonalnego IEC61508, IEC61511 i IEC60812. Podrzędnym celem pracy jest zaopatrzenie proponowanego projektu w ekonomicznie wydajny sprzęt i oprogramowanie. Cele wyznaczone dla zaprojektowanego systemu zostały osiągnięte w następujący sposób. Zaprojektowane obwody bezpieczeństwa funkcjonalnego automatycznie wprowadzają system w stan bezpieczny, gdy parametry zbliżają się do progu awaryjnego lub w przypadku naruszenia procesu awaryjnego. Aktywują one również świetlne i dźwiękowe alarmy ostrzegawcze wskazujące aktualny stan w instalacji do produkcji wodoru. Minimalizuje to ryzyko ofiar w ludziach i szkód środowiskowych. Wyniki badań wskazują, że sekcja adsorpcji zmiennociśnieniowej instalacji do produkcji wodoru, oparta na urządzeniach kontrolno-pomiarowych z funkcjonalnymi obwodami bezpieczeństwa, może działać bezpiecznie i z wyższą wydajnością (wytwarzanie gazu H_2 o czystości 99,9%, niższa emisja dwutlenku węgla) oraz ze zwiększoną niezawodnością. W instalacji adsorpcji zmiennociśnieniowej zastosowano dwa różne funkcjonalne obwody bezpieczeństwa zapobiegające wybuchom, które mogłyby skutkować ofiarami w ludziach i długoterminowym wpływem na środowisko. Działają one niezależnie od systemu sterowania automatyzacją procesu technologicznego, łagodząc skutki takich zdarzeń. Dzięki odpowiedniemu doborowi urządzeń ograniczona zostaje częstotliwość nieplanowanych i planowanych prac konserwacyjnych wykonywanych przez personel inżynieryjno-techniczny, co zapewnia komfortową eksploatację urządzeń. Zaproponowane obwody bezpieczeństwa funkcjonalnego oparte na urządzeniach kontrolno-pomiarowych zapobiegają zatrzymaniu systemu na podstawie bezpiecznych sygnałów błędów poprzez zastosowanie urządzeń z zabezpieczeniami o poziomach SIL2 i SIL3.

Słowa kluczowe: bezpieczeństwo funkcjonalne, rafinacja ropy naftowej, proces technologiczny, wodór, automatyzacja.

Corresponding author: A.M. Mehdiyeva, e-mail: *almaz.mehdiyeva@asoiu.edu.az*

Article contributed to the Editor: 11.03.2024. Approved for publication: 26.06.2024.

Introduction

The course of any technological process inherently involves the risk of accidents. These risks can manifest as short-term system stoppages, unexpected interruptions in the technological process, and damage to people and the environment, leading to losses.

Numerous technological process accidents worldwide practice underscore the necessity of implementing functional safety systems. Increasing incidents of deaths due to asphyxiation from the deadly gas, as well as the spread of toxic MIC gas to nearby towns, highlight the inadequacies of poorly designed risk reduction measures and industrial activity protections. Such events have also caused extensive environmental damage, rendering nearby water sources toxic and unusable, and resulting in the substantial loss of animal life.

Functional safety aims to prevent accidents that harm people and the environment, disrupt the technological process, or lead to large-scale incidents such as fires and explosions. It involves reducing these risks to acceptable levels within automated management systems for technological processes. The Technology Process Automation Control System (TP ACS) alone is insufficient for managing technological process. It cannot create a safe and loss-free environment during process management (considering both system errors and complex factors influencing the system). The issue arises from the nature of the technological process itself, the failure to consider the error margins of the components selected for technical support during the design process, and the improper formation of control circuits relative to the accident potential of the technological process.

By designing the control-measuring devices (CMD)-based Functional Safety System according to international standards and conducting thorough technical and software verification procedures, it is possible to reduce or eliminate potential risks to an acceptable minimum level during technological processes (Wilson, 2005; Smith, 2011). The necessity of applying the system to a specific technological process and the reliability of the safety system itself are determined in accordance with international standard. This determination is based on the analysis and inspection procedures outlined in the standards, as well as data on the progress chronicle collected from the engineering staff of the technological process, dispatchers working with the existing system, and the technologists.

Development of a functional safety system

The operational requirements of the Pressure Swing Adsorption (PSA) section highlight two critical aspects essential for its functionality, product quality, and ensuring system, human, and environmental safety during operation:

- the unit must be cleaned with nitrogen gas during maintenance;
- the control valves should be opened and closed periodically according to a specific schedule.

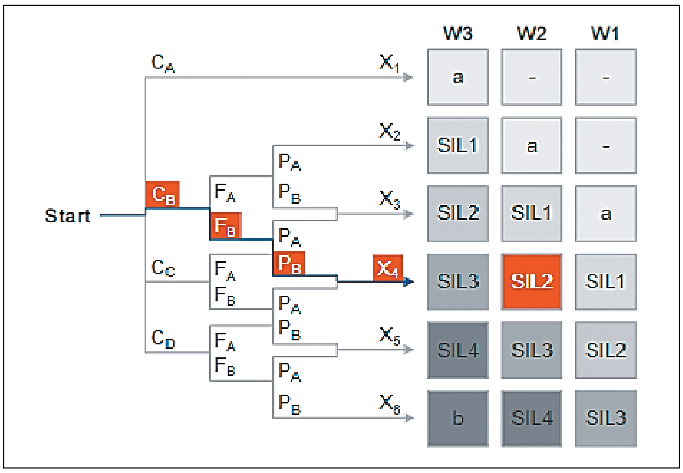
In the SIL (Safety Integrity Level) assessment conducted during the design of the CMDs-based Functional Safety Circuit (FSC) that meets both requirements, it is crucial to address common device and equipment issues observed during the operation of the PSA unit in the hydrogen plant at the oil refineries.

Evaluation of the CMDs-based Functional Safety Circuit

Let's determine, using the Risk Analysis Diagram method, the SIL degree of the CMDs-based Functional Safety Circuit for the process of cleaning with nitrogen in the PSA section. The function of CMDs-based FSC is to generate an emergency signal (siren and light) when there is no nitrogen flow to the system, to prevent the restart of the PSA cycle, and to display an emergency alarm with a respective symbol and message on the SCADA screen (Hyatt, 2003; Cruz-Campa and Gruz-Gómez, 2010). Components of the CMDs-based FSC include a flow meter that monitors nitrogen flow to the PSA unit during the cleaning process, a cut-off valve that closes the inlet gas line (feed line) if nitrogen flow is absent, and a controller that ensures proper circuit operation according to the designed algorithm (Hyatt, 2003). Failure to purge the system with nitrogen gas may lead to accidents resulting in severe injury or death to one or more persons, as well as temporary or significant environmental damage due to nitrogen's toxic effects. This corresponds to point CB in the diagram (Figure 1).

The presence of employees and technical personnel in the PSA department corresponds to the FB clauses. When an accident occurs, it is impossible to avoid its dangerous consequences, so the choice in the diagram is made according to point PB. From the options in the risk diagram, we get CB → FB → PB → X4. Based on the nature of the technological process and the small probability of risk formation, selecting the W2 clause yields a SIL2 level for the CMDs-based FSC.

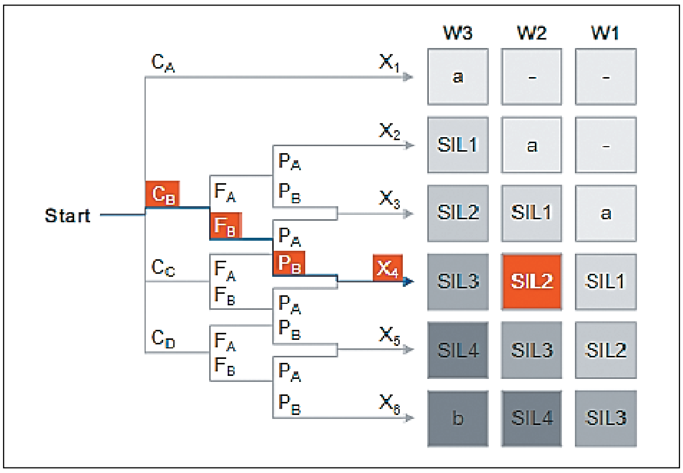
A SIL evaluation of the CMDs-based FSC for PSA compartment valves is shown in Figure 2. The function of the proposed CMDs-based FSC is to measure the pressure in the absorbent beds in the PSA section, determine when the pressure reaches the emergency limit, close the pressure safety valves on the system's inlet gas line, release the current system gas to the air, and generate the alarm (siren and light) (Thomson, 2013). This event is also displayed on the SCADA screen with the corresponding alarm symbol and message (Rausand, 2005; Hauge et. al., 2010). The components of the CMDs-based FSC include pressure switches that indicate if the valves are not activated, a cut-off valve that closes the inlet gas line (supply line) of the PSA unit in such a case, pressure safety valves that release the gas in the unit to the air, and a controller that ensures the circuit operates according to the designed algorithm. If the valves in the absorbent bed are do not open or close according to the given time in the cyclic processes, it can result in low-quality product production, system stoppage, and potential valve leakage, which can lead to an explosion with minimal system impact (Great Britain. Health and Safety Executive, Out of Control, 2003; Centre for Chemical Process Safety (CCPS), 2010; Goble, 2010; Walters and Ross, 2011; Rausand, 2011; Nolan, 2014). This also corresponds to the CC point on the diagram, evaluated as causing the death of several people and long-term environmental damage. According to the diagram, there is a high probability of employees and technical personnel being in the PSA section, so we chose the FB section. Since it is impossible to avoid the consequences of an accident once it occurs, we choose item PB in the diagram. The Risk Analysis CC → FB → PB → X5 is obtained from the choices we make according to the diagram. Due to the nature of the FSC and the probability of failure of the valves is moderate, by selecting item W2, the final SIL3 level is obtained (a feature of the system architecture) (Chen et. al., 2020; Penelas and Pires, 2021).



	W3	W2	W1
X_1	a	-	-
X_2	SIL1	a	-
X_3	SIL2	SIL1	a
X_4	SIL3	SIL2	SIL1
X_5	SIL4	SIL3	SIL2
X_6	b	SIL4	SIL3

Figure 1. Risk Analysis Diagram to determine the SIL rate for CMDs-based FSC for the nitrogen purge system

Rysunek 1. Schemat analizy w celu wyznaczenia wskaźnika poziomu nienaruszalności bezpieczeństwa dla systemu bezpieczeństwa funkcjonalnego opartego na urządzeniach kontrolno-pomiarowych dla systemu oczyszczania azotem



	W3	W2	W1
X_1	a	-	-
X_2	SIL1	a	-
X_3	SIL2	SIL1	a
X_4	SIL3	SIL2	SIL1
X_5	SIL4	SIL3	SIL2
X_6	b	SIL4	SIL3

Figure 2. Risk Analysis Diagram to determine the SIL rate for CMDs based FSC for control of valves

Rysunek 2. Schemat analizy w celu wyznaczenia wskaźnika poziomu nienaruszalności bezpieczeństwa dla systemu bezpieczeństwa funkcjonalnego opartego na urządzeniach kontrolno-pomiarowych dla zaworów sterujących

Selecting of the architecture of the CMDs-based Functional Safety Circuit

The process of selecting the logical architecture of the CMDs-based FTD designed to address the two main risk factors identified in our proposed PSA section is carried out as follows. Since for smart devices well-defined failure modes, deterministic operating behavior, sufficiently reliable failure rate data are predetermined, the equipment support of the circuit is organized based on these devices when designing the CMDs-based Functional Safety Circuit.

The selection of the logic control architecture according to the SIL determined by the Risk Analysis Diagram is based on the appropriate threshold values of the Hardware Fault Tolerance and Safe Fault Fraction parameters. For the nitrogen purging system, SIL2 has been set as the safety level for the CMDs-based Functional Safety Circuit (Ramachandran and Menon, 1998; da Cruz and de Oliveira, 2008; Brau, 2013). The system components include a flow meter showing the flow of nitrogen to the PSA unit, shut-off valves that close the inlet gas line (feed line) of the PSA unit when there is no flow, and the Nitrogen cleaning system, and a controller that forms a command based on the algorithm designed for this function.

It is desirable to choose a 1-to-1 (1oo1) architecture as the logical architecture so that the designed CMDs based FSC is also economically viable. At this time, the Hardware Assurance Fault Tolerance N for the components of the CMDs-based FSC takes a value of zero. The feeder, shut-off valve, and logic controller should be selected from Type A devices with a minimum of 60% and a maximum of 90% for Safe Error Fraction to meet the SIL2 rating in a 1-to-1 logic control architecture. The integration of the CMDs-based Functional Safety Circuit into the technological scheme of the PSA unit for the nitrogen purging system has been developed.

When the maintenance mode is selected from the SCADA, the CMDs-based Functional Safety Circuit sends a close command to the controller of the KK10 shut-off valve to close the inlet line of the PSA unit. Once the KK10 valve is closed, the KK20 shut-off valve of the nitrogen purge system is opened (Goble, 2010; Mehdiyeva and Quliyeva, 2022; Mehdiyeva et al., 2022; Mehdiyeva, 2023). During the maintenance period, the flow meter FTA1 monitors the presence of nitrogen flow to the PSA unit. If FTA1 detects zero flow, the FSC controller generates an alarm and closes the KK20 and KK21 valves. For the PSA section, a SIL3 grade was selected for the components of CMDs-based FSC. These components are designed to prevent losses and accidents in the event of a failure in the shut-off valves controlling the H_2 product line, inlet and exhaust gas line, cleaning gas line, and H_2 product line. Since CMDs-based FSC devices can fail, it is critical to use smart devices with known failure behavior.

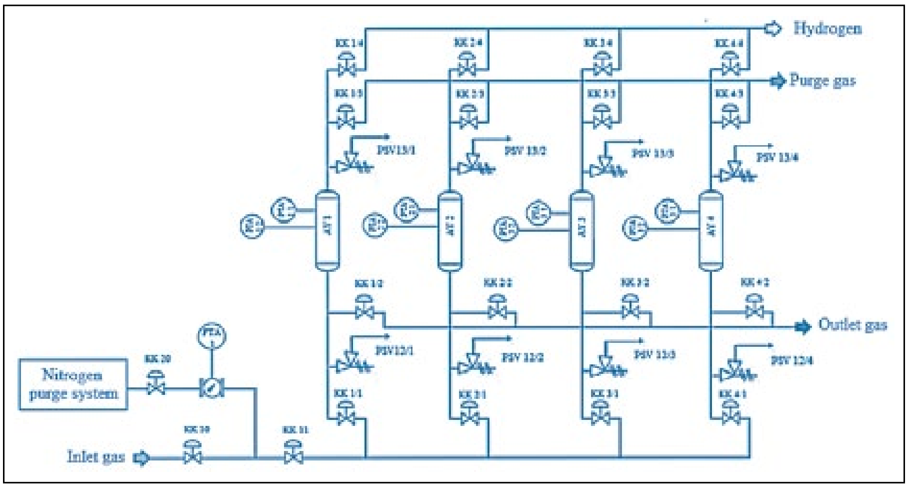


Figure 3. Integration of FSC for valve failure

Rysunek 3. Integracja systemu bezpieczeństwa funkcjonalnego pod kątem awarii zaworu

The CMDs-based FSC equipment includes pressure transmitters PTA1/2–PTA4/2 installed in the absorbent beds, KK 11 cut-off valve installed in the inlet gas (feed gas) line, PSV12/1–PSV12/4 and PSV13, respectively, located in the outlet line below and above the absorbent beds /1–PSV13/4 include pressure safety valves. If a valve in absorbent beds fails, a command is sent to an additional valve in the absorbent bed. If this additional valve also fails, the FSC controller generates a command to close the valve of the inlet gas line based on the fault threshold received from the pressure transmitters (Kuo, 2000; Pulster, 2015; Stin and Vance, 2018). Subsequently, the pressure safety valves PSV12/1–PSV12/4 and PSV13/1–PSV13/4 in the downstream and upstream outlet lines of the main absorbent beds of the CMDs-based FSC will open, releasing the gas from the system. The integration of our proposed CMDs-based FSC into the PSA unit is shown in Figure 3.

Hardware of Functional Safety System

Two types of control valves are suitable for PSA applications: globe (conical) and rotary (butterfly) valves. Each must meet specific leakage requirements and incorporate features specifically designed for fast operation.

Conical valves meet tight sealing requirements using durable soft seats that allow for long-lasting Class VI sealing in accordance with ANSI/FCI 70-2. To further ensure a tight fit, the unbalanced plug design contours only the fit.

When necessary, PTFE should contact the soft seat. The seat ring keeps the plug centered as it enters the seat, creating a concentric seal and ensuring long valve shutoff over the life of the valve.

Three important features allow conical control valves to achieve over a million cycles and maintain tight shutoff, making them ideal for high-cycle applications:

- reliable actuator performance;
- fast hitting speed;
- precise valve positioning.

Reliable actuator performance is enhanced by special diaphragm materials that reduce problems such as air oxidation, thermal aging, embrittlement at low temperatures, and storage loss. Unlike a piston actuator, a spring and diaphragm actuator does not have a large diameter sliding seal subject to wear. A two-sided diaphragm inside the transmitter helps reduce failure caused by mechanical wear. The fast stroke rate feature enables the driver to handle high cycle counts at specific stroke speeds while providing tight process control.

Digital valve controllers provide the ability to achieve precise valve positioning and rapid response to process changes while increasing valve assembly reliability. Rotary control valves meet critical sealing requirements using seal rings with pressure-assisted sealing action and spring-loaded shafts that center the disc on the seal. Rotary throttle valve assemblies can achieve one million cycles under load conditions with a spring and diaphragm actuator similar to the sliding body spring and diaphragm design. Advantages of these transmission designs include no O-rings to wear out, defined position with respect to air failure, low transmission pressures for operation, and double-sided diaphragms.

Although both rotary and conical valves can be used for a variety of PSA applications, conical valves are more suitable for applications requiring valve travel over intermediate distances. Conical valves offer a better range of motion than rotary valves, increasing stability and allowing users to follow the desired motion point set more closely by their controls.

A critical feature often overlooked when selecting appropriate valves for a PSA unit is the positioner's diagnostic capability. The ideal positioner should offer online, in-service, non-intrusive performance testing, real-time monitoring, and data acquisition capabilities. This ensures earlier detection of valve degradation and provides technicians with the necessary troubleshooting to make informed repair decisions. For the CMDs-based FSC for nitrogen purging, which is graded SIL2, the components must meet the SIL2 safety completeness level, and the overall PDF-failure probability parameter of the circuit must be evaluated according to our chosen logic control architecture and SIL2 grade. Research indicates that the SIL2-grade conical valve is a more reliable choice for a nitrogen purge system, such as the cut-off valves of a CMDs-based FSC.

Therefore, the SAMSON 241 valve is considered more suitable for KK20 and KK21 valves.

As a logical controller, the SYL3 level controller should be selected to meet the requirements of each system. A HIMA modular controller system, consisting of HIMA AI8 01 analog input card, HIMA F60 CPU 01 controller, and HIMA AO8 01 analog output card, is chosen to meet the SIL3 degree requirement. Since dry nitrogen is used in the nitrogen cleaning system, the Krohne OPTISWIRL 4200 vortex type flow meter is selected to meet the SIL2 requirement.

To demonstrate that the hardware provision meets the defined above safety completeness for the CMDs-based Functional Safety Circuit, the logic control architecture, flowmeter, and controller system (including analog input, central computing block, including analog output cards) should be calculated for the execution mechanism, or the values given in the SIL certificates and operating instructions of those devices should be considered.

For the proposed logical architecture, the probability of not fulfilling the PFD (Probability of Failure on Demand) requirement is calculated as follows:

$$PFD = \lambda_{DU} \frac{TI}{2} \tag{1}$$

where: TI – test interval of the device, taken as 8760 hours for 1 year. The probability of not meeting the overall average requirements for FTD (Fault Tree Diagram) is obtained by summing the calculated values for each component:

$$PFD_{CO} = PFD_{transducer} + PFD_{controller} + PFD_{actuator} \tag{2}$$

where:

PFD_{CO} – probability of failure on demand for the complex,

$PFD_{transducer}$ – probability of failure on demand for the transducer,

$PFD_{controller}$ – probability of failure on demand for the controller,

$PFD_{actuator}$ – probability of failure on demand for the actuator.

Given that λ_{DU} is 150 FITS for the OPTISWIRL 4200 flowmeter and 54.9 FITS for the SAMSON 241 valve, and the architecture is chosen as 1 out of one 1, formula (1) yields $0.655 \cdot 10^{-3}$ and $0.24 \cdot 10^{-3}$, respectively. For the HIMA controller system, these values and PFD values are provided by the manufacturer:

- HIMA AI8 01 – $0.0175 \cdot 10^{-3}$;
- HIMA F60 CPU 01 – $0.0488 \cdot 10^{-3}$;
- HIMA AO8 01 – $0.0268 \cdot 10^{-3}$.

The probability of non-fulfillment of the overall average requirements for the CMDs-based FSC is calculated based on the values given in Table 1 according to formula (2):

$$PFDCO = 0.9981 \cdot 10^{-3} \tag{3}$$

Table 1. Parameters for calculating PFD

Tabela 1. Parametry do obliczania prawdopodobieństwa awarii przy żądaniu usługi (PFD)

FTD component	Undefined dangerous fault	PFD
OPTISWIRL 4200	150 FITS	$0.6550 \cdot 10^{-3}$
HIMA AI8 01	–	$0.0175 \cdot 10^{-3}$
HIMA F60 CPU 01	–	$0.0488 \cdot 10^{-3}$
HIMA AO8 01	–	$0.0268 \cdot 10^{-3}$
SAMSON 241	54.9 FITS	$0.2400 \cdot 10^{-3}$

Table 2. Parameters for calculating PFD

Tabela 2. Parametry do obliczania prawdopodobieństwa awarii przy żądaniu usługi (PFD)

FTD component	Undefined dangerous fault	PFD
ASHCROFT D7	52.25 FITS	$0.02285 \cdot 10^{-3}$
HIMA F6217	–	$0.02860 \cdot 10^{-3}$
H41q-MS CPU	–	$0.02890 \cdot 10^{-3}$
HIMA F3330 DO	–	$0.00820 \cdot 10^{-3}$
SAMSON 3241	51.9 FITS	$0.02273 \cdot 10^{-3}$

Based on the relationship between PFD (Probability of Failure on Demand) and SIL (Safety Integrity Level) rate in Table 2, and the value of PFDCO from (3), the proposed CMDs-based FSC with selected hardware meets the calculated SIL2 rating and the selected 1 out of 1 (1oo1) logic control architecture.

In the event of valve failure in the PSA section, the components of our proposed second CMDs-based Functional Safety Circuit must meet the SIL3 rating so that the probability of failure of the overall circuit meets the SIL3 rating.

Table 3. Hardware of CMDs-based FSC

Tabela 3. Sprzęt systemu bezpieczeństwa funkcjonalnego opartego na urządzeniach kontrolno-pomiarowych

FTD component	Appointment	Position	SIL grade	Amount, pc.
OPTISWIRL 4200	Measures consumption in the nitrogen line	FTA1	SIL2	1
HIMA AI8 01	Analog input card of the HIMA system	AI1	SIL2	1
HIMA F60 CPU	Central processor of the HIMA system	CPU1	SIL3	1
HIMA AO8 01	Analog output card of the HIMA system	AO1	SIL2	1
SAMSON 241	Controls nitrogen line	KK20	SIL2	1
SAMSON 241	Controls the inlet gas line of the PSA system	KK21	SIL2	1
ASHCROFT D7	Measures the pressure in the absorbent bed	PTA1/2–PTA4/2	SIL3	4
HIMA F6217	Analog input card of the HIMA system	Aİ2	SIL3	1
H41q-MS CPU	Central processor of the HIMA system	CPU2	SIL3	1
HIMA F3330 DO	Discrete output module of the HIMA system	DO2	SIL3	1
SAMSON 3241	Controls the inlet gas line of the PSA system	KK11	SIL3	1
ARMAS 22	Drains the bottom outlet line of absorbent beds	PSV12/1–PSV12/4	SIL3	4
ARMAS22	Clears the upper output line of absorbent beds	PSV13/1–PSV13/4	SIL3	4

When the pressure in the absorbent bed rises, the pressure is released to the air through PSV12/1–PSV12/4 and PSV13/1–PSV13/4 valves in the upper and lower outlet lines of the bed. The ARMAS 22 valve was chosen as the pressure safety valve (Figure 3).

PFD values for selected devices are listed in Table 2.

The total average PFD value of FTD, calculated by formula (2) based on the values taken from Table 2, is as follows:

$$\text{PFDCO} = 0.10018 \cdot 10^{-3} \tag{4}$$

Thus, based on the PFDCO value given in (4) and the relationship between PFD and SIL rate in Table 3, the proposed CMDs-based FSC with the selected hardware meets the calculated SIL3 rate and the selected 1-out-of-1 (1oo1) logic control architecture. The actuators of both CMDs-based FTDs are selected as normally closed, considering the possibility of FSC failure.

Software of control of the proposed functional safety system

A CMDs-based FSC designed for the nitrogen purge process operates as follows: after the process cycle set by the absorbent bed technologist is completed, the SCADA operator starts the bed cleaning process. At this stage, the KK21 valve of the FSC in the inlet gas line of the system is closed. By opening the valves in all beds of the PSA unit, gas is transferred to the corresponding capacities, purging the system of gas. As a next step, the controller of the CMDs-based FSC opens the KK20 conical valve of the nitrogen purge system. The signal from the FTA1 sensor is processed by the controller to measure whether sufficient nitrogen has entered the PSA unit. If the nitrogen flow to the system is cut off during maintenance mode, the controller's program generates an emergency signal in the form of sound and light and closes KK20 and KK21 valves.

Even if the operator acknowledges the emergency condition by pressing the "Ok" button in the dialog window displaying the emergency message about the lack of nitrogen flow, the command to open the KK10 valve is not executed. This is because the KK21 valve of the FSC is installed closer to the entrance of the PSA unit than the KK10 valve. The unit is allowed to start up only after the nitrogen purge valve is cleared and nitrogen flow is restored.

Programming of the HIMA modular controller system is done with SILworX software. Technological process data for the program and intermediate data of the program are determined according to the algorithm. These data for the nitrogen purge system are given in Table 4.

Table 4. Program data

Tabela 4. Dane programu

Type of parameter	Signal name	Type of Signal/Data
Technological process data	AzotFTA1	AI/word
Technological process data	KK20OPND	AI/word
Technological process data	KK20CLSD	AI/word
Technological process data	KK20OPN	AO/word
Technological process data	KK20CLS	AO/word
Technological process data	KK21OPND	AI/word
Technological process data	KK21CLSD	AI/word
Technological process data	KK21CLS	AO/word
Technological process data	KK21OPN	AO/word
Technological process data	AlarmSirena	AO/word
Technological process data	AlarmLight	AO/word
Intermediate data of the program	AzotONOFF	word

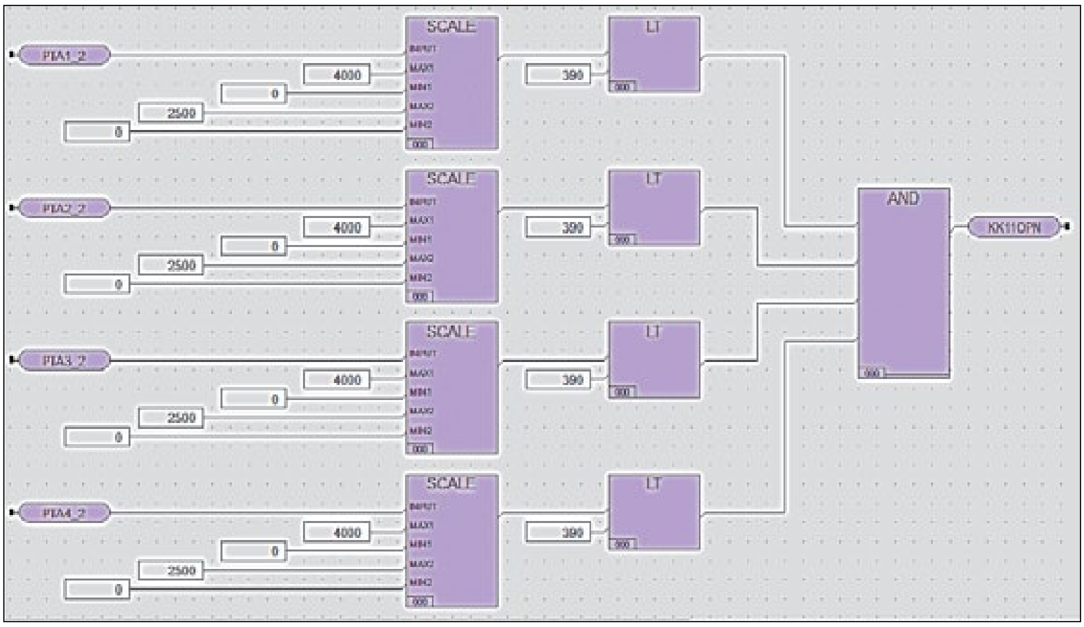


Figure 4. Program for FSC for the absorbent bed valve failure case (II part)

Rysunek 4. Program systemu bezpieczeństwa funkcjonalnego dla przypadku awarii zaworu strefy absorpcyjnej (część II)

The control program of the CMDs-based FSC of the nitrogen cleaning process is shown in Figure 4. As regards the programming language, when designing a program for CMDs-based FTDs, the main program module must be selected from FBD and LAD languages. Functions and functional blocks controlled from the main program can be written in one or more of the languages regulated by section 3 of the IEC61131 standard. A CMDs-based FSC designed for valve failure in absorbent beds operates as follows: In the event of a control failure in the downstream valve of the appropriate absorbent bed during the absorbent bed process, transfer is made to the out-of-order absorbent bed. If there is also a fault in the corresponding valves, the CMDs-based Functional Safety Circuit prevents the available pressure in the PSA section from exceeding the emergency limit by closing the KK11 conical cut-off valve in the CMDs-based FSC inlet line of the PSA section. The pressure relief valves PSV12/1–PSV12/4 and PSV13/1–PSV13/4 open due to the pressure at the inlets and vent the current gas in the PSA compartment. In the event of a failure of the valves of the PSA unit, the pressure in the system on the corresponding line increases, and this increase is transmitted to the HIMA modular controller system by the pressure transmitters (pressure switches) PTA1/2–PTA4/2 of the CMDs-based FSC. When the pressure transmitters (pressure switches) reach the emergency limit set by the technologist, they generate a signal corresponding to the logic “1”, and the HIMA modular controller system closes the KK11 valve according to the given comparison operation and notifies the engineering staff by generating a sound and light emergency signal. Thus, CMDs-based FSC prevents gas from entering the system and provides pressure release. If the pressure in all absorbent beds returns to normal value, the KK11 valve is opened. Technological process data for the program and intermediate data of the program are determined according to the algorithm. Data for the crash prevention program in case of valve failure are given in Table 5.

Table 5. Program data

Tabela 5. Dane programu

Type of parameter	Signal name	Type of Signal/Data
Technological process data	PTA1_2	AI/word
Technological process data	PTA2_2	AI/word
Technological process data	PTA3_2	AI/word
Technological process data	PTA4_2	AI/word
Technological process data	KK11CLSD	AI/word
Technological process data	KK11OPND	AI/word
Technological process data	KK11CLS	DO/bit
Technological process data	KK11OPN	DO/bit
Technological process data	AlarmSirena	AO/word
Technological process data	AlarmLight	AO/word
Technological process data	AlarmLight	AO/word
Intermediate data of the program	AzotONOFF	word

Conclusion

The potential risks of accidents in the PSA section of the hydrogen production unit of the oil refinery have been evaluated, leading to the development of a Functional Safety Circuit aimed at preventing accidents and mitigating their effects. The FSC designed for the nitrogen purge system that prevents the formation of potentially explosive gas mixtures with hydrogen when oxygen enters the system during system maintenance is proposed. Another FSC has been developed specifically to prevent pressure increase in the system during the failure of the valves in the PSA section, ensuring the isolation of the gas inlet of the PSA section, and restoring the system to the previous safe state by releasing the excess gas to the air.

The SIL rating was determined for both Functional Safety Circuits based on the Risk Analysis Diagram, the selected logical control architecture of the FSC, and the selection of equipment that satisfies the SIL rating. Components of the controller system of FSCs, essential for ensuring safe and efficient operation of the PSA unit, were selected to comply with SIL3, and dedicated the software was developed accordingly.

Reference

Brau J.-F., 2013. Production of Hydrogen for Oil Refining by Thermal Gasification of Biomass: Process Design, Integration and Evaluation. *Chalmers University of Technology, Göteborg*. DOI: 10.13140/RG.2.1.2599.6402.

Centre for Chemical Process Safety (CCPS), 2010. Guidelines for Safe Process Operations and Maintenance. *John Wiley & Sons Inc., New York*.

Chen W.-H., Lu Ch.-Y., Tran K.-Q., Lin Y.-L., Naqvi S.R., 2020. A new design of catalytic tube reactor for hydrogen production from ethanol steam reforming. *Fuel*, 281, 118746. DOI 10.1016/j.fuel.2020.118746.

Cruz-Campa H.J., Cruz-Gómez M.J., 2010: Determine sis and SIL using HAZOPS. *Process Safety Progress*, 29(1): 22–31. DOI: 10.1002/prs.10293.

da Cruz F.E., de Oliveira Junior S., 2008. Petroleum Refinery Hydrogen Production Unit: Exergy and Production Cost Evaluation. *Chalmers University of Technology, Göteborg. International Journal of Thermodynamics*, 11(4). DOI: 10.5541/ijot.227.

Goble W.M., 2010. Control Systems Safety Evaluation & Reliability. 3rd Edition. *International Society of Automation*.

Great Britain. Health and Safety Executive, Out of Control, 2003. Why control systems go wrong and how to prevent failure. *HSE Books*.

Hauge S., Håbrekke S., Lundteigen M.A., 2010. Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection. *SINTEF Technology and Society, Norway*.

Hyatt N., 2003. Guidelines for Process Hazards Analysis (PHA, HAZOP), Hazards Identification, and Risk Analysis. 1st Edition. *CRC Press LLC*.

IEC 60812, Analysis techniques for system reliability-Procedure for failure modes and effects analysis (FMEA).

Kuo W., 2000. Optimal reliability design: fundamentals and applications. *Cambridge University Press*.

Mehdiyeva A.M., 2023. Types of accidents, their causes and prevention measures. Actual problems of modern science. *Proceedings of the IV International Scientific and Practical Conference, Boston, USA*, 441–444.

Mehdiyeva A.M., Quliyeva S.V., 2022. Control mechanism to manage quality of energy conversions. Science. Engineering. Technology. *Polytechnical bulletin, JSC "Publishing house-South"*, 1: 19–24.

Mehdiyeva A.M., Sardarova I.Z., Quliyeva S.V., 2022. Methods for Increasing Accuracy in the Process of Information Exchange and Processing. Novel Research Aspects in Mathematical and Computer Science. *BP International*, 4(11): 108–122.

Nolan D.P., 2014. Handbook of fire and explosion protection engineering principles: for oil, gas, chemical and related facilities. 3rd Edition. *William Andrew*.

Penelas A. de J., Pires J.C.M., 2021. HAZOP Analysis in Terms of Safety Operations Processes for Oil Production Units: A Case Study. *Applied Sciences*, 11(21): 10210. DOI: 10.3390/app112110210.

Pulster E.L., 2015. Assessment of Public Health Risks Associated with Petrochemical Emissions Surrounding an Oil Refinery. *USF Tampa Graduate Theses and Dissertations*.

Ramachandran R., Menon R.K., 1998. An overview of industrial uses of hydrogen. *International Journal of Hydrogen Energy*, 23(7): 593–598. DOI: 10.1016/S0360-3199(97)00112-2.

Rausand M., 2005. Preliminary hazard analysis. *Norwegian University of Science and Technology*.

Rausand M., 2011. Risk Assessment Theory, Methods, and Applications. 1st Edition. *Wiley & Sons, Inc., New York*.

Smith D.J., 2011. Reliability, Maintainability and Risk: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems. 8th Edition. *Butterworht-Heinemann*.

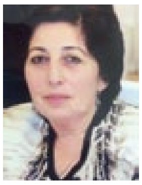
Stinn M., Vance J., 2018. Selecting valves for pressure swing adsorption. *Revamps*, 31–35.

Thomson J., 2013. Refineries and Associated Plant: Three Accident Case Studies. *Safety in Engineering Ltd, New York*.

Walters N., Ross B., 2011. Predicting and mitigating the risk of catastrophic incidents. *A Hart Energy Publication, USA*.

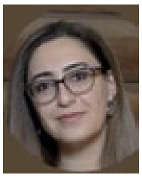
Wilson J.S. (ed.), 2005. Sensor Technology Handbook. *Elsevier Inc*. DOI: 10.1016/B978-0-7506-7729-5.X5040-X.

Farid Haji AGAYEV, Ph.D.
Associate Professor; Dean of the Faculty
of Information Technologies and Control
Azerbaijan State Oil and Industry University
16/21 Azadliq Ave., AZ1010 Baku, Azerbaijan
E-mail: *farid.agayev@asoiu.edu.az*

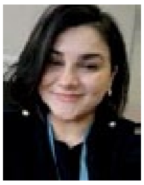


Almaz Mobil MEHDIYEVA, Ph.D.
Associate Professor at the Department of Electronics
and Automation
Azerbaijan State Oil and Industry University
20 Azadlig Ave., AZ1010 Baku, Azerbaijan
E-mail: *almaz.mehdiyeva@asoiu.edu.az*

Qadir Arzu GAFAROV, M.Sc.
Teacher at the Department of Electronics
and Automation
Azerbaijan State Oil and Industry University
16/21 Azadliq Ave, AZ1010 Baku, Azerbaijan
E-mail: *qadir.gafarov@asoiu.edu.az*



Sevinj Vaqif BAKHSHALIYEVA, M.Sc.
Teacher at the Department of Electronics
and Automation
Azerbaijan State Oil and Industry University
16/21 Azadliq Ave., AZ1010 Baku, Azerbaijan
E-mail: *sevinj.quliyeba@asoiu.edu.az*



Natella Vusal SHIRINZADE M.Sc.
Instrumentation and Automation Engineer
Technip Energies Italy S.p.A.
Viale Castello della Magliana, 68-00148 Roma
E-mail: *shnatella15628@sabah.edu.az*