IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 6, 2021, accepted March 24, 2021, date of publication March 30, 2021, date of current version April 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3069807

A Novel Approach Based on Stochastic Hybrid Fault Tree to Compare Alternative Flare Gas Recovery Systems

SOHEYL MOHEB KHODAYEE[1], FERDINANDO CHIACCHIO[1], AND YIANNIS PAPADOPOULOS[2]

[1]Department of Electrical, Electronics and Computer Engineering, University of Catania, 95124 Catania, Italy
[2]Department of Computer Science and Technology, University of Hull, Hull HU6 7RX, U.K.

Corresponding author: Ferdinando Chiacchio (chiacchio@dmi.unict.it)

This work was supported by European Union Horizon 2020 (EU H2020) Project under Grant 101017258–SESAME.

ABSTRACT Flaring has always been an inseparable part of oil production and exploration. Previously, waste gas collected from different parts of facilities was released for safety or operational reasons and combusted on top of a flare stack since there was not the possibility to treat or use this type of gas. Concerns about global warming led to several initiatives for reducing flaring or even eliminating combustion. Treating flare gas was made possible by the introduction of flare gas recovery systems that have become increasingly obligatory. Most solutions add a flare gas recovery system to an existing flare system. In a typical scenario, after analyzing the existing facility and collecting the necessary data, alternative designs are proposed and criteria are determined to make a choice between the proposed alternatives. In this paper two designs of a gas control system are proposed, and reliability was chosen as the deciding factor. Using repairable dynamic fault trees, the failure models of the two designs have been implemented. Afterwards, a novel hybrid technique, the Stochastic Hybrid Fault Tree Automaton, is used to model the working conditions in which the system operates, with the aim to achieve a more realistic assessment and evaluate the disaster likelihood associated to these failures. It is shown that the latter enables a richer analysis where the effects of failure can be better assessed. This is important for correct choice between design alternatives because, as shown in the case study, the results of the two analyses can lead to contrasting conclusions of the solution to adopt. Further investigations have been carried out focusing on the safety sub-systems and on the basic events in each design. The Importance Measure analysis revealed that some of the components were responsible for most of the critical failures, thus locating some areas of possible design improvement.

INDEX TERMS Model-based dependability analysis, dynamic reliability, importance measure, stochastic hybrid automaton, Monte Carlo simulation.

LIST OF ACRONYMS

BE	: Basic Event
CCIR	: Collection, compression and injection/reinjection
DFT	: Dynamic Fault Tree
EPC	: Engineering, Procurement and Construction
FEED	: Front End Engineering Design to provide basic designs
FGRS	: Flare Gas Recovery System
GCP	: Gas with Critical Pressure
GCS	: Gas Control System
HAZOP	: Hazard Operability
HDFT	: Hybrid DFT
LSV	: Liquid Seal Vessel
MTTF	: Mean Time to Fail
MDBA	: Model-based dependability analysis
OREDA	: Offshore Reliability Data Handbook
PPMS	: Positive Pressure Maintaining System
ROR	: Rate of Return
RDFT	: Repairable Dynamic Fault Tree
SHyFTA	: Stochastic Hybrid Fault Tree Automatons
TE	: Top Event

The associate editor coordinating the review of this manuscript and approving it for publication was Yu Liu.

I. INTRODUCTION

One of the major trends in the current scientific works is towards bringing together both financial benefits from exploiting terrestrial resources while trying to keep intact the natural balance that governs the environment. Extracting oil and gas has been a massively profitable industry but its effects on the environment are not negligible and manifest themselves throughout different aspects of environmental measurements because of the inevitable safety measures that release waste gas into the atmosphere.

Flaring was introduced to moderate these effects but has turned into a major concern itself. High-pressure gas in this process is burnt-off in at appropriate height into the low-pressure atmosphere, at the stack top, with a visible flame. With an efficient combustion, requiring an appropriate mixture of fuel with air, the main products are water vapor and CO2, but depending on the combination of the waste gas it can contain toxins such as benzene, carbonyl sulfide (COS) or Nitrogen oxide (NOx) or methane (CH4), as found in [1]. Nevertheless, many negative effects of flaring process have been found analyzing the groundwater samples of Delta State Nigeria in [2] which revealed a correlation with a poor water quality. Negative effects on the atmosphere and broadly on human health were also reported in [3] which reviewed the impacts of flaring on the soil.

On the other hand, the economic aspects linked to the improvement of the flaring processes can represent an important opportunity. In fact, as recalled in [3], the United Nations Framework Convention on Climate Change (UNFCCC) has stated that gas flaring can be registered as a Clean Development Mechanism (CDM) for greenhouse emissions reduction if valid technological expedients are taken to prevent the negative impacts. Some economics related to the flaring industry have been analyzed in [4] and in [5] that evaluated the equivalent US dollars of annually gas flared or vented with a value of about $30.6 billion which is equivalent to one-quarter of the United States' or 30% of European Union's gas consumption. As discussed in [3] the most used methodology in gas flaring for CDM projects is AM0009, i.e. recovery and utilization of vented or flared gas.

Adding a Flare Gas Recovery System (FGRS) has become a well-practiced solution in the existing fields to avoid massive wastes, making a profit and reducing effects on the environment. An FGRS can be, depending on the requirements and conditions of each field, composed of different technologies, as discussed in papers like [4]–[10], of which the most utilized are: a) Collection, Compression and Injection/Reinjection (CCIR); b) Gas-To-Liquid (GTL); c) Electricity generation; as well as other less discussed methods, such as Gas-To-Ethylene (GTE). These technologies are installed on gas header route [11] before the flare tower, as shown in Figure 1, between the knockout vessel and liquid seal, and pull flare gas from the header whenever flow is detected. In this way, a great portion of flare gas is recycled to better use rather than being combusted in the flare tower, leading to significant reduction in greenhouse gas emission to the atmosphere. Figure 1shows a simplified Piping & Instrumentation Diagram of such a system. It should be noted that a recovery system is, in most cases, being added to an existing flare system which is considered a development project.

In any development project there is going to be some basic steps to follow: 1) Conceptual design, 2) Feasibility study, 3) Front End Engineering Design to provide basic designs (FEED engineering), 4) bidding phase by EPC (Engineering, Procurement and Construction) companies, and 5) execution of EPC, or project management by the winning EPC company.

The feasibility study of such projects is carried out using simulation software, like Aspen HYSYS for oil and gas industries, that helps to predict important parameters, like the production of electricity or barrels of a product for GTL method, as well as other economic parameters of a project, like the rate of return, capital investment, return on investment and annual profit. This information is used to compare different proposed design solutions for a specific site and, thus, evaluate the relative benefits of different investment proposals [4], [6], [8]–[10], [12]–[18].

During the next step in the process, a FEED dossier is presented to EPC companies. To conduct EPC bidding, after a full understanding of the conceptual designs and correcting the possible flaws in them, one should consider moving to more detailed design and consider alternatives. At this point, and, having secured the economic feasibility and benefits of the concept, dependability becomes very important as the concept is refined to technical proposals. As shown in [19], the parameters referring to system dependability [20] are very relevant in safety critical systems [21] in the oil and gas industry [22]–[25] where significant hazards exist. On one hand, reliability, availability, safety, security, and survivability are inherently important and they must be designed and assured; on the other hand, exploring how to incorporate these properties in a design, will increase the detail of a proposed technical solution and improve the accuracy of the previous predictions regarding the efficiency and economic benefits of the system.

Model-based dependability analysis (MDBA) seems to offer mechanisms to manage and reduce the complexity of activities required to perform the dependability assessment of safety critical systems [26], [27] with tools and techniques that can be effective both in a preliminary design phase as well as during the lifecycle of a system, if a revamp modification of a plant is required [28]–[30]. Among the modelling tools of MDBA and RAMS (Reliability, Availability, Maintenance & Safety), high-level formalisms like FMEA [31], Markov Process [32], Fuzzy Petri Nets [33], Monte Carlo Simulation or Bayesian Networks [34] play an important role in the analysis of safety and risks of industrial processes.

Among them, Fault Tree Analysis [29] is of certain interest because of its intuitiveness and the wide variety of support from the research community that, during the last three decades, has driven the conception of powerful extensions of the methodology. This methodology has been object of

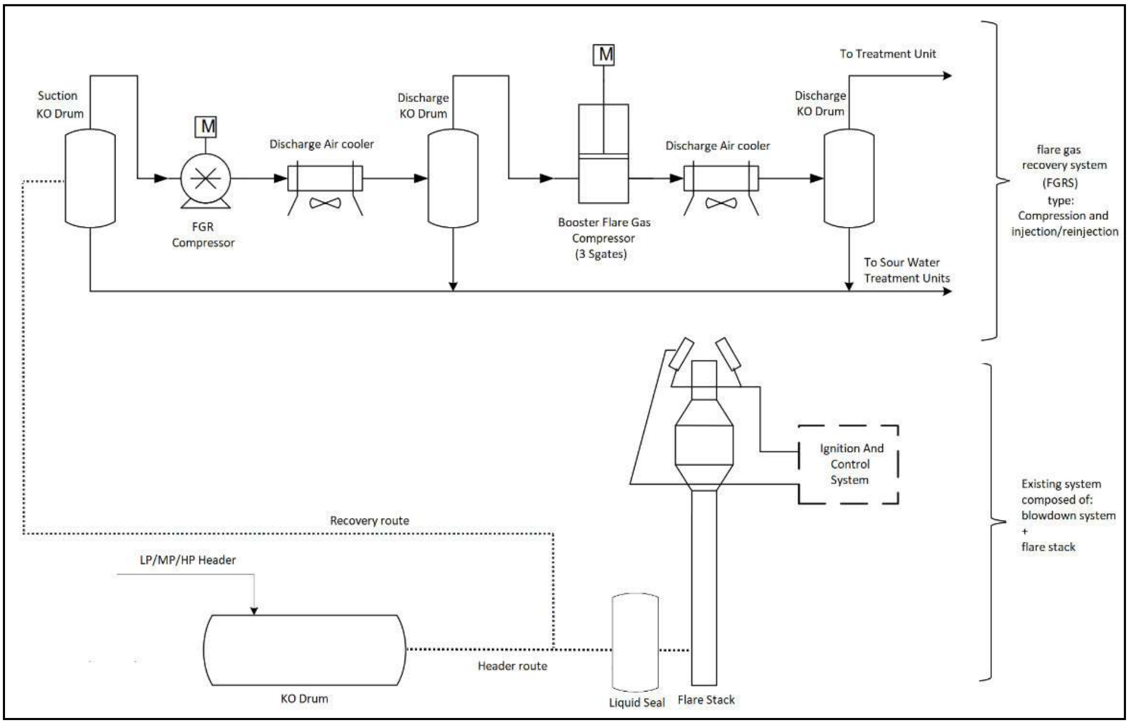


FIGURE 1. Piping & instrumentation diagram of the south pars field development phase 2 and 3.

numerous extensions: Fuzzy Fault Tree has been conceived to tackle the scarcity of data from the field process [35]; Dynamic Fault Tree (DFT) to include temporal dependencies [36] among the system components [37]; or when the physical process cannot trivially be neglected (or considered as static, i.e. normal operative working conditions), then Stochastic Hybrid Fault Tree Automatons (SHyFTA) [38] can model and predict dependability more accurately [39]. The application of hybrid approaches for the probability analysis of safety and risk of hazardous industries is a significantly hot topic of literature and, as stated in [40], they are becoming more meaningful because can combine both qualitative and quantitative knowledge.

Although literature presents works on the dependability analysis of flare gas recovery systems [41], [42] and on the simulation of the working conditions [43], [44], to the authors' knowledge, the combination of these two matters has never been studied. Especially, the studies have only been conducted for the FGRS itself and not for the corresponding systems, one of which being a gas control system (GCS). It is essential to install a GCS to control the flow of the gas in a correct proportion to the flare stack or to the FGRS depending on the capacity of the recovery components.

Expanding on this earlier research, this paper focuses on proposing an improved methodology for the selection of design proposals case for FGRS that exploits the benefits of simulation and MBDA. The case study is focused on the development of the South Pars plant phase 2 and 3 [45], [46], where the main objective will be to compare two different GCS alternatives with respect to dependability attributes. The process of gas flaring is described for both the two alternative GCS design solutions of the FGRS system of South Pars phase 2 and 3 and used to propose DFT models for the two solutions. Based on these two DFT models results are discussed which point to a preferred design. Afterwards, to improve the accuracy of the dependability analysis, the conversion of the DFTs into the equivalent Hybrid Dynamic Fault Trees (HDFT) is proposed. In fact, this latter is able to consider not only the failure dependencies among the system components, but, via simulation, the temporal dynamics of the safety mechanisms which come in place to mitigate the effects of dynamic changes of physical conditions. As it is shown, this feature will be used to evaluate the probability of critical disasters that can occur during certain operational scenarios characterized by the unavailability of certain safety components and by an altered status of the gas pressure flowing in the system. This modelling represents a second important novelty with respect to the state of the art because the results obtained prove that the hybrid model gives evidences and insights that would not emerge using Dynamic Fault Tree.

Summarizing, the main objectives of this paper are to:

- Discuss two different design solutions for improving the gas flaring process of the plant of South Pars;

- Model the corresponding Dynamic and Hybrid Fault Trees of the two different design solutions;

- Perform a Monte Carlo simulation of the two models by using a Matlab
texttextregistered-based software library [47];

- Analyse and compare the difference between the DFT and the HDFT results, to demonstrate that the latter provide further information for determining the most suitable design solution.

This paper is organized as follows. Section 2 presents the problem statement and the methodology adopted. To this end the FGRS system functions are described, the design alternative of the FEED dossiers illustrated, and the Fault Tree methodologies are summarized. Section 3 presents the case study describing the process performed by the FGRS solutions, and the corresponding DFT models. Furthermore, and this is a significant departure from earlier work, we describe a transformation from the DFT to HDFT by means of the SHyFTA formalism, and using we model the physical process of the gas flaring. In section 4 the result of the hybrid stochastic automata simulation is discussed, while conclusions are drawn in section 5.

II. PROBLEM STATEMENT & METHODOLOGY

To provide the necessary background, first we discuss the South Pars plant, phase 2 and 3 [45], [46]. The development of this plant was comprised of two major sub-projects: (1) Selection of the FGRS and (2) Selection of a GCS. The first sub-project, discussed in [9], established that CCIR technology is the most economical choice for the FGRS because of the lower capital investment and higher ROR (Rate of Return) compared to GTL or electricity production.

When installing an FGRS into an existing field, necessary changes are required on the existing system [11]. Changes include adding a pre-process/pre-flaring system called Gas Control System (GCS), second sub-project, which spreads throughout header route and recovery route (Figure 1) that directs gas in proper portions to the flare stack and to FGRS. Without one, a safe operation to keep piping and FGRS intact would not be possible. Since adding a GCS into an existing field is considered a development project, it is composed of the main 5 steps of every development project.

FEED is conducted after completion of Conceptual Design or Feasibility Study and before EPC phase. This phase is meant to bring up the technical issues and make an estimation of the costs of the project which will be handed over to the EPC engineers in the bidding phase [48].

EPC contractors will receive the FEED package to approve the basic designs and see, based on the cost estimates, if they can deliver the project execution [49]. Since EPC contractors will be fully responsible for the delivery of the projects, they will be required to approve the FEED package at the time of bidding which brings additional challenges and responsibilities to the EPC contractors [49]. To approve the FEED package, a complete understanding of the basic designs and verification of their function is required such as process simulation and other calculations in a short period of time. If the designs present a flaw, EPC engineers need to propose proper alterations. Moreover, if FEED package has suggested multiple alternatives to be installed, EPC contractor must choose the best alternative [50] based on the requirements that are imposed by the project owner.

In this paper, the idea is to use some attribute of dependability as metric to perform the differential analysis of two designs. Therefore, after studying the proposed designs for inherent flaws and approving them, when finalized P&IDs are available, dependability assessment is required to compare both the systems. Dependability analysis can represent one of the most critical activities for the comparison of the two alternatives [51] because it gives much information about the system, including the unreliability, the likelihood of a disaster occurrence, the critical components and so on.

In the systems under evaluation, a disaster may happen if the GCS does not perform on demand, causing highly expensive components to get damaged and as a result, there is a complete shut-down of the system. According to IEC60050-191, the reliability of a product (system) is the probability that the product (system) will perform its intended function for a specified time-period when operating under normal (or stated) environmental conditions [51]. Therefore, in order to provide a reliability assessment that copes with the final objective of the feasibility study, the idea is to focus on critical failures with no turn-backs, namely those stops that can involve big financial loss. In fact, a higher reliability turns in other favorable benefits for the lifecycle operations of the system, including less downtimes, the reduction of maintenance costs and an increasing of the overall profits.

In this paper, the methodology used for analyzing and quantifying the system failures of the two alternative plants is the Dynamic Fault Tree (DFT) analysis. Every failure that can cause a total stop of the system operations needs to be identified and analyzed in order to design a model that can describe the components and the corresponding process dependencies which bring to the critical failure. The failure and repair rates of the systems have been taken from OREDA [52], a source of reliability dada, which provides a database of failure rates of components used in offshore engineering from their normal steady-state operating life time period.

Afterwards, a more thorough investigation has been performed by simulating the system working conditions of different operating scenarios that depend on the gas pressure. This has been achieved by modelling the system and its processes with the Stochastic Hybrid Fault Tree Automaton (SHyFTA) methodology [38] able to account for both the deterministic and of the stochastic features of a system. The physics of the operating working conditions have been simulated starting from the data of the gas pressure taken by the DCS system of a similar plant. Thus, the models have been designed and simulated using the SHyFTOO library [53] a Monte Carlo software solver working under the Matlab® environment able to solve both DFT and SHyFTA, here referred also as Hybrid DFT (HDFT).

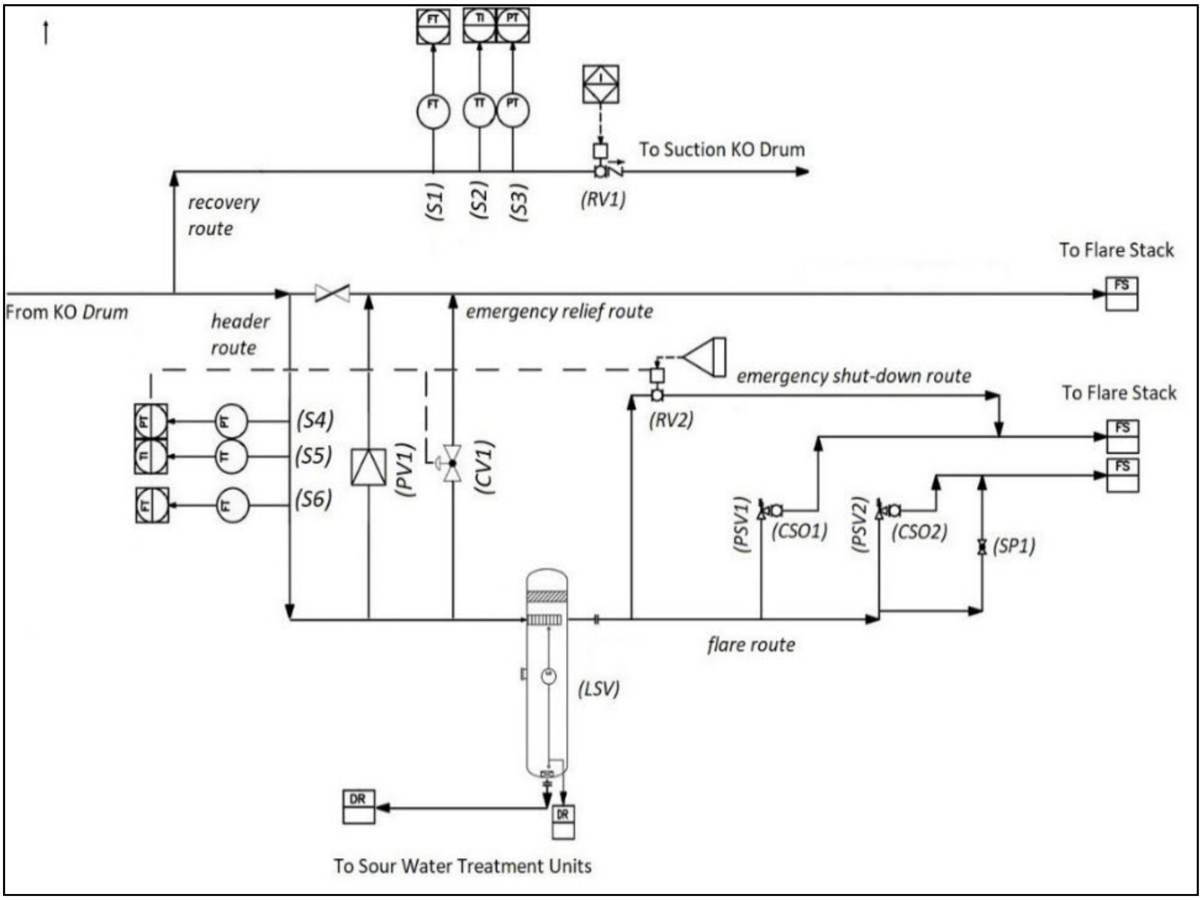


FIGURE 2. GCS1 – after revision by EPC contractor.

In the next two subsections, the system design alternatives and the dynamic and hybrid fault tree methodologies are summarized.

A. SYSTEM DESCRIPTION & DESIGN ALTERNATIVES

Approval of the provided FEED dossiers by EPC contractors consists of considering different scenarios of gas behavior, usually performed using HAZOP, to see how the systems will react and handle the situations (e.g., when gas with high pressure enters, what will each GCS do to protect FGRS, piping and even its own components). In this way, certain conclusions about the necessity of making changes in the existing P&IDs can be drawn with an acceptable degree of certainty. Of the two proposed alternatives in FEED dossier are shown in Figure 2 and Figure 3.

The existing facility (Figure 1) consists only of the flare system and a FGRS has to be added. In the existing flare system, the ensemble of the (i) 3-phase separator, (ii) LSV and (iii) flare stack, in this order, constitutes the blowdown system [6]. The FGRS will be located upstream of the flare between the 3-phase separator (Knock-Out (KO) drum) and the LSV. It will be working in parallel with the existing flare system and both may be continuously operational depending on the circumstances of the gas pressure. FGRS includes a compressor that pulls flare gas from header route into recovery section whenever flow is detected [11]. The principal potential safety risk in integrating an FGRS is from ingression of air into the flare header route that is introduced by compressor suction [44]. The pressure in header route must remain positive to prevent flashback from the flare stack which in turn prevents a flammable gas mixture being flashed off inside the system from flare pilots.

In the GCS1 of Figure 2 there is a LSV before the flare stack which might be the same LSV that already exists in the flare system; but, due to the adaption requirements [11], a new one is installed according to the FGRS capacity.

The LSV provides maintained positive pressure in header route by providing a back pressure using a predetermined height of water inside it that, according to FGRS capacity, does not let the gas pass through, unless the gas pressure exceeds back pressure. Also, it does not let the gas pass in the reverse direction, which helps in preventing flashbacks.

Since operating problems exist for LSV, [44], that may include plugging or choking, vibration, suction pressure instability, cyclic flare flame puffing which requires proper attention to the asymmetry of internals, in the GCS2 of Figure 3 sensors and a valve replace the LSV.

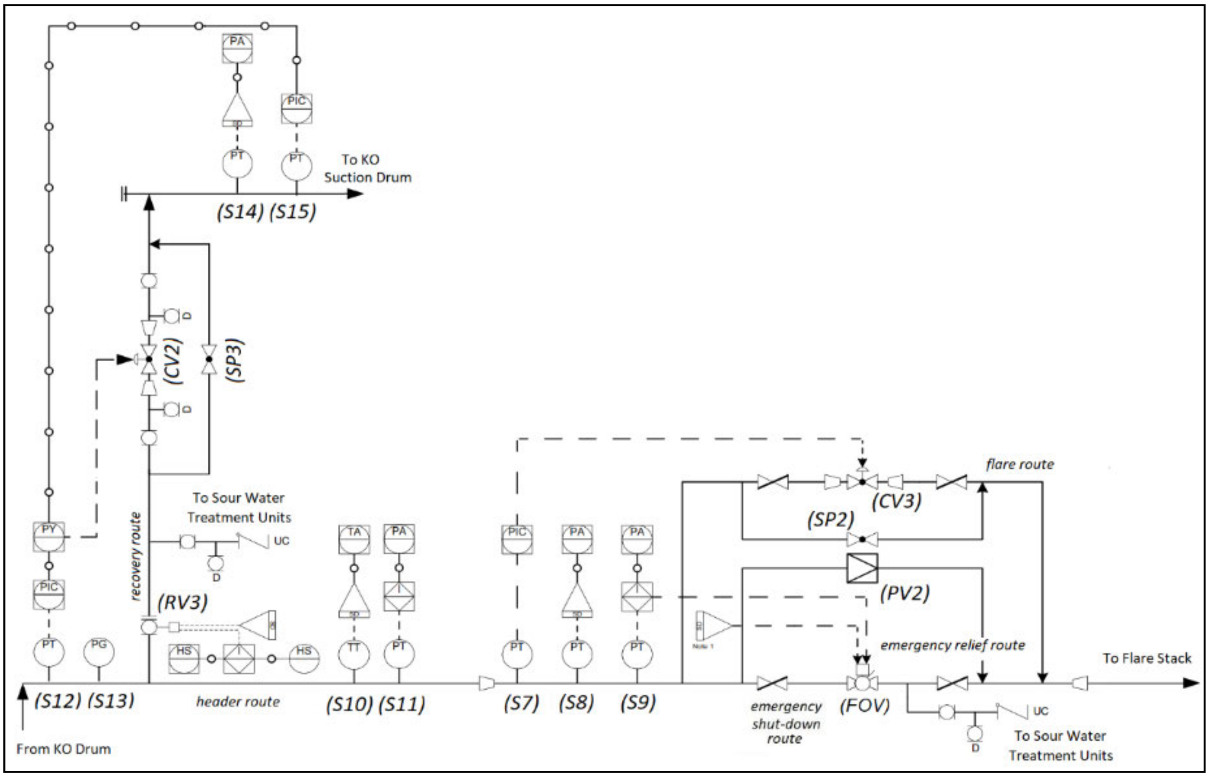


FIGURE 3. GCS2 – after revision by EPC contractor.

To make the next sections easier to follow, Table 1 represents symbols, abbreviations, failure and repair rates of each component. Configurations of GCSs and their components are represented in Figure 2 for GCS1 and Figure 3 for GCS2. The corresponding branches of the DFT are represented in Figure 4 for GCS1 and in Figure 5 for GCS2.

B. DYNAMIC AND HYBRID FAULT TREES

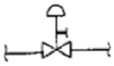
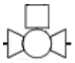
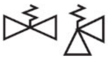
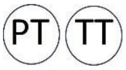
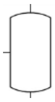
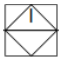
Fault Tree Analysis (FTA) is a popular technique of RAMS engineering (Reliability, Availability, Maintenance & Safety) used in the industrial and hazard industry field, like aerospace, nuclear power, chemical processes, pharmaceutical and petrochemical, to perform the dependability analysis of fault-tolerant systems and identify the most critical events.

The graphical representation of a Fault Tree (FT) is a diagram constituted by a Top Event (TE), the Basic Events (BEs) and logic gates. Following a TOP-DOWN approach, the construction of a FT is realized identifying the sequence of events bringing to the occurrence of the TE. The TE is the undesired scenario of the fault tree, whereas BEs are the leaves of the FT and represent the elementary events of a process, generally linked with the failure of the system components, that cannot be further decomposed. Gates are used to interconnect logically the BEs and/or other intermediary events that depend on the output of other lower-level gates. The original formulation of FT analysis – known also as Static Fault Tree (SFT) – is characterized by two main Boolean logic gates, the OR and the AND. The main flaw of SFT technique is that the OR and the AND gates are static in nature, thus unable to describe common failure scenarios that arise when temporal and complex inter-dependencies held among the components of a system (e.g., stand-by systems, load-sharing policies, automatic safe mechanisms, etc.) [54].

To increase the modelling capabilities of SFT, [37] introduced new gates that are at the basis of the methodology known as Dynamic Fault Tree (DFT) analysis. In particular, the PAND, SPARE, SEQ and FDEP gates allow to model temporal sequences of dependent events, spare allocation policies, components degradation and failure/repair dependencies. The qualitative analysis of a FT allows the finding of the minimal cut sets (or sequences in a DFT) of the system component failures [55] that bring to the occurrence of the TE. Minimal cut sets and sequences are used to assess the structural vulnerability of a system. Intuitively, the longer the cut set/sequence, the less vulnerable the system is to that combination of events.

Moreover, numerous cut set/sequences mean that the system is characterized by a high vulnerability. But, another interesting aspect of FT analysis is the possibility to solve the model quantitatively, if the probability density function of the time to fail of the BEs are known. For instance, for a generic component characterized by random failures, the corresponding pdf to adopt is the exponential distribution that is characterized by one parameter, named Mean Time to Fail (MTTF). In practice, MTTFs are provided by the components

TABLE 1. Symbols, failure and repair rates of the components.

Name	Abb.	Symbol	Failure type	Failure rate (hours)	Repair rate (hours)
Control valve	CV		Close, open, regulate	26.5e-6	1/119
Rotary valve	RV		Close, open	90.84e-6	1/61
Pin valve	PV		Buckle, close	27.74e-6	1/119
Fast opening valve	FOV		Close, open	33.76e-6	1/113
Pressure safety valve	PSV			36.32e-6	1/16
Spare Globe valve	SP		Close, open	23.70e-6	1/119
Process sensor	S		Detect	10.39e-6	1/135
Liquid seal vessel	LSV		Plugged, choked	11.22e-6	1/120.4
Programmable logic controller	PLC		Send signal	-	-
Car sealed open Valve	CSO		Provide constant flow	-	-

manufacturer, although literature presents several databases collecting the most used industrial equipment.

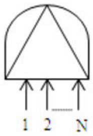
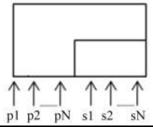
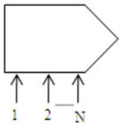
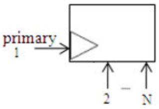
The quantitative resolution of a Fault Tree depends on the complexity of the model [54], [56]. If SFTs can be easily solved with the Boolean algebra tools, the same cannot be said for DFTs that need to be converted into a different mathematical model like ATS, SAN, BDMP, CTMC, ICMC and so forth [57]. Among all, the class of repairable DFTs (RDFT) is the most cumbersome because restoration and dynamic gate logics enable temporal and circular inter-dependencies that are not caught by any of the previous mathematical tools. Table 2 resumes the main gates of a DFT model as taken by [53].

Nowadays, Monte Carlo simulation is the best option for solving such models which can offer a good trade-off between precision and accuracy, (i.e., accuracy improves with the number of iterations that causes an increasing of the time of computation) [58]. In point of fact, the simulation approach has further favored the conception of advanced methodologies to improve the realism of a model. In recent papers, Stochastic Hybrid Automaton models have been used to analyze complex dependable systems like nuclear [39] and renewable power plants [19], [58], [59]. In particular, the latter have been analyzed adopting a Fault Tree-like methodology, known as Stochastic Hybrid Fault Tree Automaton (SHyFTA) or Hybrid DFT.

Nowadays, Monte Carlo simulation is the best option for solving such models which can offer a good trade-off between precision and accuracy, (i.e., accuracy improves with the number of iterations that causes an increasing of the time of computation) [58]. In point of fact, the simulation approach has further favored the conception of advanced methodologies to improve the realism of a model. In recent papers, Stochastic Hybrid Automaton models have been used to analyze complex dependable systems like nuclear [39] and renewable power plants [19], [58], [59]. In particular, the latter have been analyzed adopting a Fault Tree-like methodology, known as Stochastic Hybrid Fault Tree Automaton (SHyFTA) or Hybrid DFT.

As said, the main benefit of SHyFTA is to improve the realism of a model. To this end, SHyFTA methodology allows to implement a hybrid model able to couple the deterministic and the stochastic behaviour of a system process by means of the Hybrid Basic Events [57]. In this way, a change of the physical process is reflected in the stochastic model and vice-versa. In a SHyFTA model, the deterministic process of a system can be described with any mathematical formalism (like algebraic of differential equations of a process), whereas the stochastic process is implemented by means of RDFT. This modelling formalism is not as easy as SFT or DFT; therefore, in order to simplify the modeling of such artifacts, a Matlab® software library called SHyFTOO has been

TABLE 2. Gates supported by a DFT Model.

Name	Symbol	Description (with N input)	Repairable Behaviour
PAND		It behaves like an AND Gate, but it triggers only if the events occur from left-to-right order.	Assume that the PAND has failed. If the i-1th input gets repaired and afterwards it fails again, the PAND gate does not trigger because the ttf(i-1th) > ttf (ith).
SPARE		It triggers only if the failed primary inputs cannot be replaced by an equal number of spare inputs. Moreover, spare inputs can be shared with other SPARE Gates	If a primary input gets restored, the corresponding shared input which was substituting it gets available again and can be used in other SPARE gates.
SEQ		It forces the inputs to occur from the left to the right order and triggers if all the inputs occur. It can model the gradual degradation of a system.	If the ith input is repaired, the inputs at its right - e.g. (i+j)th , j=i+1,…,N - get restored.
FDEP		The output of the gate is dummy. It forces the failure of the inputs (2,…,N) if the primary fails.	Restoration of the inputs (2,..,N) are inhibited as long the primary is failed (another possible logic is to allow restoration of inputs (2,..,N) although primary is still failed)

developed and freely distributed [47]. Since the alternative design solutions proposed in this paper are complex industrial equipment, the most appropriate dependability model technique is the repairable DFT that will be simulated with SHyFTOO. Moreover, the implementation of a SHyFTA model will be proposed by coupling the DFT with variable operational scenarios (i.e., different profile of gas pressure). To develop the fault tree models, in the next section the function of the systems is presented.

III. CASE STUDY MODELING

The objective of a GCS is to prevent disasters, namely those type of events that can affect the whole operations and cause severe damages to the system. Generally, disasters have another important consequence as they force a prolonged shut down of the entire plant before it is restored. In order to make a dependability assessment with Fault Trees, faults in the form of a top event need to be detected so that the probability occurrence can be computed.

In this study, the Top Event has been identified considering the objectives of the GCS. One thing that needs to be mentioned about the modelling approach taken in this paper is that failures which do not cause a stop in the system function have not been considered. Therefore, whenever the failure of a group of components would lead to a disaster, a Top Event is formed. To describe the system functions we need to explain how it behaves for several levels of gas pressure and Table 3 and Table 4 resume the main failure scenarios respectively for the system design solution GCS1 and GCS2.

Some parts of the system play an active role in preventing the occurrence of a disaster. These are system's reaction to each gas pressure so that the flow is regulated in a way to avoid damages to the system.

One of the main critical subsystems of the proposed alternatives is the Positive Pressure Maintaining System (PPMS) that assures to maintain a positive pressure in the header route. In GCS1, the most prominent feature of this subsystem is the LSV which is a very costly component to maintain. It leaks and gets out of calibration very easily, although – on the other hand – its failure could only cause the FGRS not to run at its full capacity. In other words, the failure of this component does not make the system stop and it does not cause damages to the other components.

In GCS2, the same task is undertaken by CV3 & SP2 and their related sensors which are far easier to maintain since they fail far less regularly and their function is not based on a predetermined water height, but a smart collaboration of sensors and valves keeps the positive pressure.

Despite this important difference between GCS1 and GCS2, the decision of choosing the best alternative will be based on the capability of each alternative to prevent disasters. In other words, how well does an alternative keep the system continuously functioning.

A. PROCESS AND FAILURE MODEL OF GCS1

Figure 4 shows the Dynamic Fault Tree model of the GCS1 design solution of Figure 2, whereas Table 3 resumes a breakdown relating the gas pressure scenarios and the subsystems of the GCS1 which play an active role for preventing possible disasters.

1) SYSTEM FUNCTION DURING HIGH PRESSURE (TABLE 3#COLUMN 6)

Branch #01 – responsible for preventing LSV and piping damage – models the system safeguard when gas with high pressure enters in the system. In this case, PSV1, PSV2 and their spare SP1 (represented by CSP1 and CSP2 in fault tree)

TABLE 3. GCS1 way of functioning of the branches sub-systems during each gas pressure.

Sub-systems (fault-tree branches)	Gas pressure behavior								
	1	2	3	4	5	6	7	8	9
	Very low	Normalization from very low	Low	Normalization from low	Normal	High	Normalization from high	Very high	Normalization from very high
#01	-		-			D1 (LSV, pipe damage)	#02	-	
#02						#01 OR #03	D2 (Flash back)		
#03						D1 (LSV, pipe damage)	#02		
#04						-		D1 (LSV, pipe damage)	-
#05								-	D2 (Flashback)
#06	D1 (FGRS damage)	*				D1 (FGRS damage)	*	D1 (FGRS damage)	*

TABLE 4. GCS2 way of functioning of the branches sub-systems during each gas pressure.

Sub-systems (fault tree branches)	Gas pressure behavior								
	1	2	3	4	5	6	7	8	9
	Very low	Normalization from very low	Low	Normalization from low	Normal	High	Normalization from high	Very high	Normalization from very high
#01	D1 (pipe damage)	-	-			D1 (pipe damage)	-	-	-
#02	-	D2 (Flash back)				-	D2 (Flashback)		
#03		-					-	D1(pipe damage)	
#04								-	D2 (Flash back)
#05	D1 (FGRS damage)					D1 (FGRS damage)		D1(pipe damage)	-
#06	-	*				-	*	-	*

are responsible for automatically releasing gas and preventing high pressure build-up in LSV.

At the same time, at least 2 out of 3 Sensors (VOR2:3) sense the High pressure and open RV2 to release the extra gas. If the sensors do not sense a drop in pressure, it means that RV2 has failed to open and they send a signal to open CV1, and hence (AND3) in the fault tree. The failure of all these components during high pressure causes LSV or pipe

TABLE 5. Notes referring to the system design functioning of Table 3 and Table 4.

GCS1	GCS2	Notes
Yes	Yes	(*) means **activation** of a branch during flow of gas with certain pressure. This means in case of unavailability of the respective branch, there will be an undesired event (failure) but there will be no disasters (no component damage).
Yes	Yes	(D1 and D2) Also mean activation but in case of unavailability, there will be a **disaster**.
Yes	Yes	D1 means a **disaster** when gas is reaching a **certain pressure**. It means the component has failed first and then gas has reached a critical pressure
Yes	Yes	D2 means a **disaster** when gas is **being normalized** from a certain pressure. It means during a critical pressure the component has failed and then gas pressure normalized while the component was still being repaired (unavailable).
Yes	Yes	Branch activation indicates the activation of all the components (gates) existing in that branch.
Yes	No	#02 is a fraction of #01 and #03 in the fault tree and in column 7, only this fraction of #01 and #03 needs to be available otherwise there will be a disaster (flashback)
Yes	No	Cell (#02,6) means that the function of OR1 in fault tree needs to be taken into consideration in that scenario

damage (Table 3, Row#01, Col6). It must be noted that during high pressure, when RV1 is closed, the PLC also sends an automatic signal to open RV2.

Branch #03 (responsible for preventing LSV and piping damage when LSV is chocked) shows the case where LSV is chocked and the route is closed for the gas to pass. In a very low, low and normal pressure, all of the gas is being processed and the branch doesn't need to get activated but when a high pressure gas enters the system, the extra gas needs to be emitted to the flaring stack and (2:3 of the) sensors 4, 5, 6 will send a signal to open RV2 and naturally will not sense a drop in pressure because gas is not passing through LSV to pass through RV2. As a result, these sensors will send a signal to open CV1 so that extra gas is released. During high pressure, branch #03 needs to be available which means both CV1 and LSV need to be available. Availability of LSV means that it is not choked and is operating normally. If LSV is plugged and CV1 is failed, a high-pressure gas entering in the system will cause a disaster (Table 3, Row#03, Col6).

Branch #04 and **Branch #05**: when LSV is chocked, very high pressure may also start to flow. But when very high pressure enters in the system, no matter if LSV is chocked or not, another group of valves will be activated to put LSV completely out of system.

In the case of branch #02 one needs to consider that it represents the function of CV1 which is a part of #01 or #03.

When gas is reaching a high pressure, the sole function of #02 will not suffice to prevent a disaster. Cell (Table 3, Row#02, Col6) refers to the function of OR1 in the fault tree.

In other words, when gas is reaching a high pressure, if LSV is choked the function of AND5 is the determiner and if LSV is running normally, then the function of AND 4 is the determiner.

Branch #06 (responsible for preventing FGRS damage) states that during the flow of high-pressure gas, 2 out of 3 sensors (1, 2, 3) and 2 out of 3 sensors (4, 5, 6) will send a signal to close RV1 and block the route to FGRS to prevent damages to it. In case of failure a disaster will happen (Table 3, Row#06, Col6).

2) SYSTEM FUNCTION DURING NORMALIZATION FROM HIGH PRESSURE (TABLE 3#COLUMN 7)

When high pressure starts to normalize, then all of the activated components need get deactivated again. In case of deactivation failure, there will not be a disaster because LSV automatically prevents a reverse flow and there will be no flashback.

But, during this scenario it is only important that branch #02 is available whether LSV is plugged, or running normally because the route of CV1 does not pass through LSV and a flashback is not automatically prevented; in fact, in case of malfunction during pressure normalization, a disaster (flashback) can occur. So, whether we are discussing **Branch #01** (LSV performing normally) or **Branch #03** (LSV plugged), during normalization only the malfunction of **Branch #02** can lead to a disaster. Hence Table 3 contains a reference to **Branch #02** in Row#01, Col7 and Row#03, Col7. Moreover,

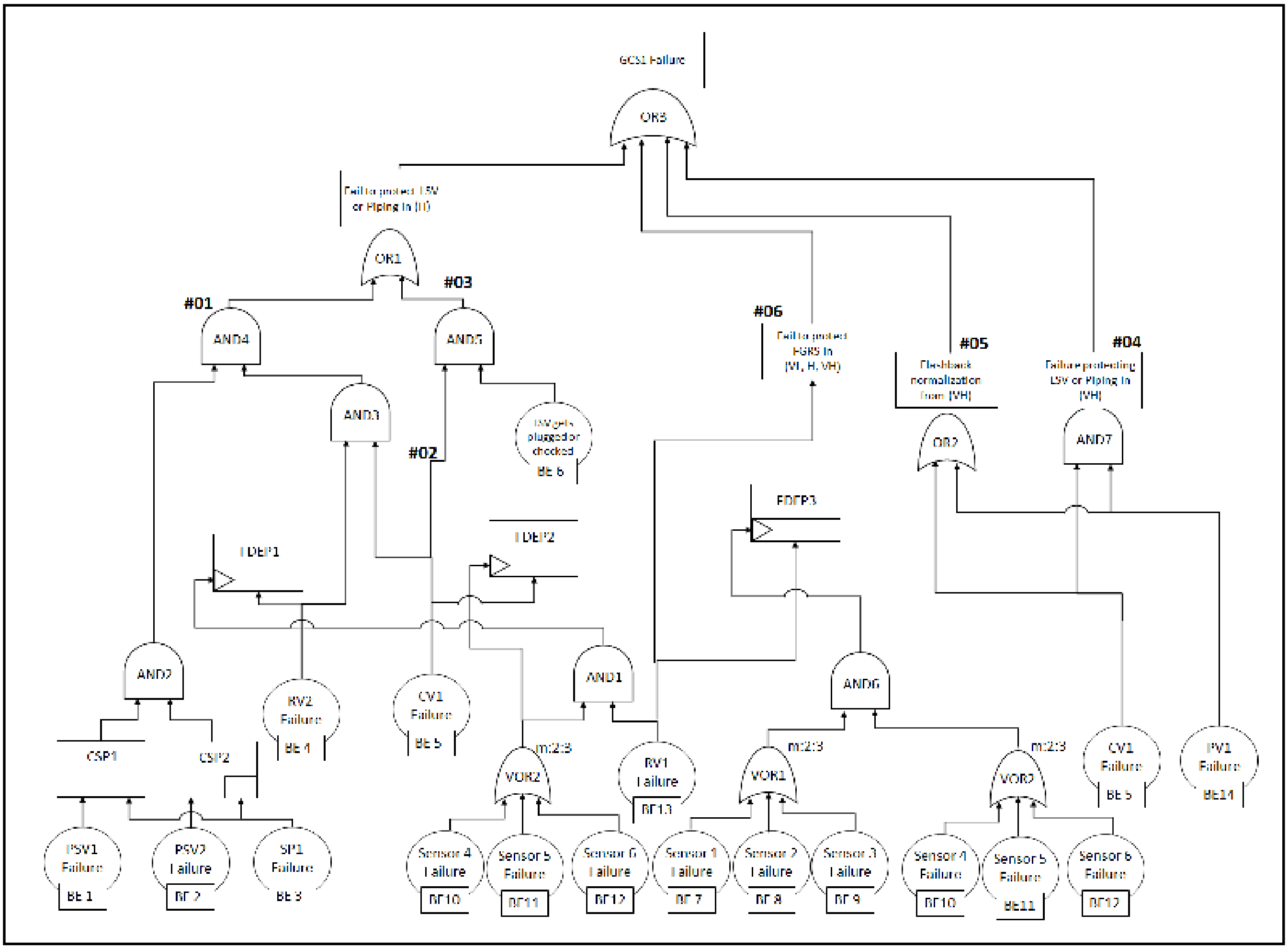


FIGURE 4. **GCS1 DFT Model.**

the cells (Table 3, Row#02, Col7) refers to a flashback scenario.

In this scenario, also **Branch #06** needs to get activated. In this case, RV1 – that was closed during high pressure – needs to open again for the FGRS to start processing again. In case of failure, there will not be a disaster but just a financial loss (Table 3, Row#06, Col7).

3) SYSTEM FUNCTION DURING VERY LOW PRESSURE AND NORMALIZATION (TABLE 3#COLUMN1, COLUMN2)

Branch #06 handles this scenario and during very low pressure the only part of the system that may get damaged is the FGRS. This part will undergo a stress because it must compress the gas at a very low pressure to make it proper for being processed. In this case 2 out of 3 sensors (1, 2, 3) should close RV1 to block the route to FGRS. Failure in doing so will lead to a disaster (Table 3, Row#06, Col1). During normalization RV1 needs to get opened but failure in this task will only lead to financial loss and not a disaster since there will be no damages to the components (Table 3, Row#06, Col2).

4) SYSTEM FUNCTION DURING VERY HIGH PRESSURE AND NORMALIZATION (TABLE 3#COLUMN8, COLUMN9)

This scenario is handled by **Branch #04** and **Branch #05**. During very high pressure, sensors send a signal to open CV1 and PV1 opens automatically so that gas does not pass through LSV and prevent damages to it. If both the valves fail, then there will be a disaster, as modelled with the AND7 in the fault tree and (Table 3. Row#04, Col8). During normalization of gas pressure if any of the two valves remain open there will be a disaster (flashback) as described by the OR2 (Table 3, Row#05, Col9).

The adoption of the FDEP gates in the fault tree model is motivated by the following reasons:

i. FDEP 1: a failure of at least 2 out of 3 sensors in VOR2 and the failure of RV1 – modelling the absence of the automatic signal to open RV2 – will lead to RV2 failure.

ii. FDEP 2: a failure in the abovementioned sensors will lead to the failure of CV1.

iii. FDEP 3: a failure of at least 2 out of 3 of the sensors in VOR 1 and VOR 2 will lead to the failure of RV1.

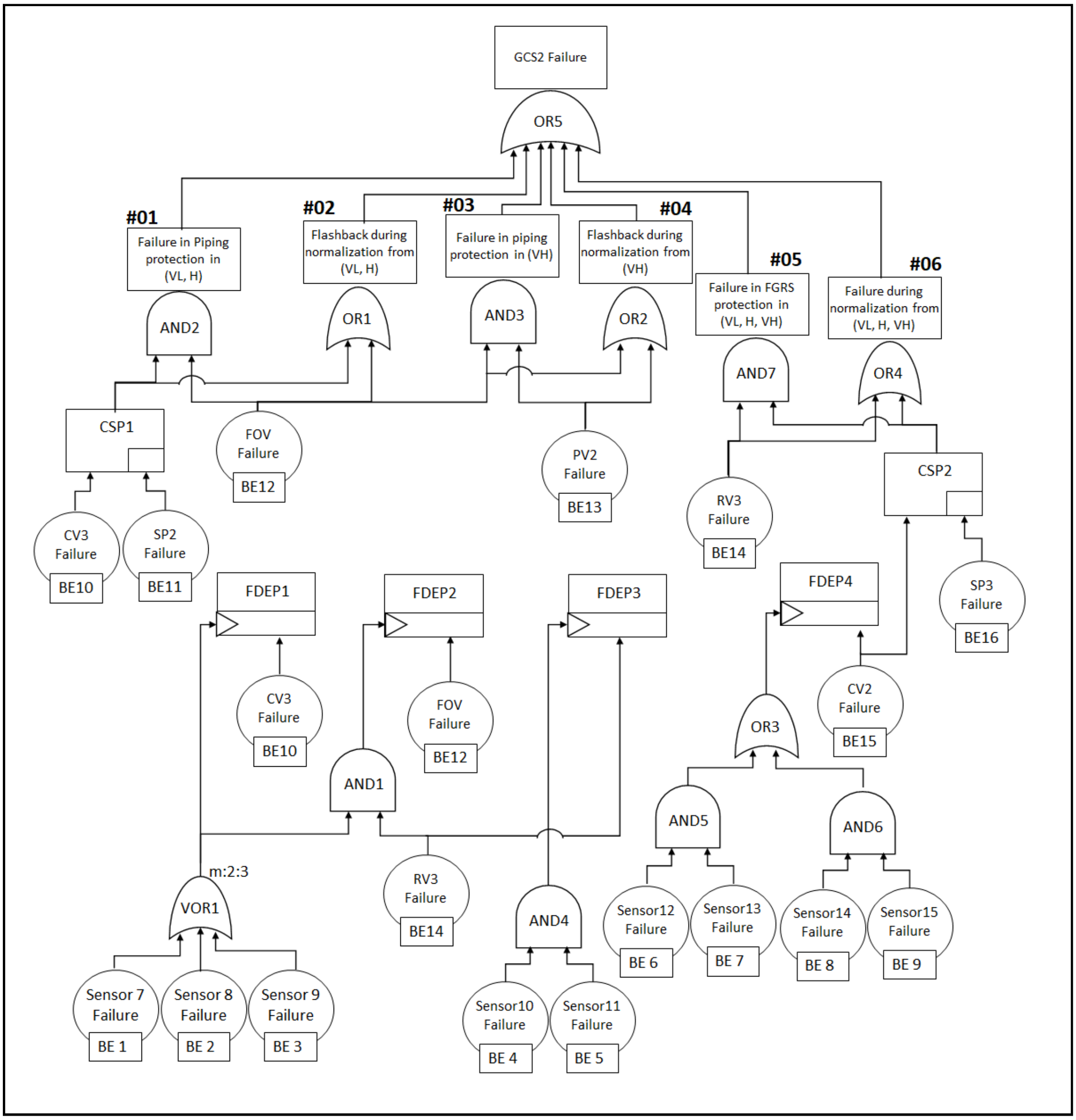


FIGURE 5. GCS2 DFT Model.

B. PROCESS AND FAILURE MODEL OF GCS2

Figure 5 shows the Dynamic Fault Tree model of the GCS2 design solution of Figure 3, whereas Table 4 resumes a breakdown relating the gas pressure scenarios and the subsystems of the GCS2 which play an active role for preventing possible disasters.

1) SYSTEM FUNCTION DURING VERY LOW AND HIGH PRESSURE AND NORMALIZATION (TABLE4# COLUMNS 1, 2, 6, 7)

FGRS is vulnerable to very low, high and very high pressure. So, the system must block the recovery route to prevent FGRS damage and provide extra capacity for emission to prevent piping damage. The case of very high pressure will be discussed in the next section.

One of the main differences between GCS1 and GCS2 is that in GCS1, LSV automatically prevents the disaster of 'flashback' during normalization because of its inner design. But, in GCS2 if one of the valves in this section is left open during normalization, it can lead to a flashback disaster.

Looking at the rows of Table 4, it is clear that when gas pressure reaches to a very low or high pressure, **Branch #01** and **Branch #05** need to get activated, whereas **Branch #02** and **Branch #06** have to manage the normalization from these pressures. In case of unavailability of these branches there will be disasters (component damages) except that for **Branch #06** whose unavailability (not opening the recovery route during safe pressures) only leads to financial loss (Table 4, Row#06, Col2; Row#06, Col7; Row#06, Col9).

When gas reaches a very low or high pressure, the recovery route must be blocked. This task is undertaken by RV3, CV2 and its spare SP3. Moreover, PLC compares the pressure at the entrance of the system and of the FGRS, using respectively the measures taken by sensors 12 and 13 (for the entrance of the system), and the sensors 14 and 15 (for the FGRS). In these cases, **Branch #05**, sensors 10 and 11 send a signal to close RV3; moreover, the pair of sensors 12 and 13 compare the pressure at the entrance of the system and at the entrance of the FGRS using sensors 14 and 15. In case of a significant difference, they will send a signal to close CV2 or – in case of its unavailability – to the spare valve SP3. The failure of all three of these valves (as modelled by the AND7) leads to a disaster (Table 4, Row#05, Col1; Row#05, Col6).

Also, the route to flaring must open to emit all the gas that enter into the system, since it is not being processed. This is undertaken by activating **Branch #01**. Specifically, 2 out of the 3 sensors (7, 8, 9) send a signal to open CV3, or in case of its failure, to the spare SP2. If they do not sense a drop in pressure, they will send a signal to open FOV. Failure of all these components (see AND2) leads to a disaster (Table 4, Row#01, Col1).

When the gas start to normalize from these pressures, the recovery route must open so that gas start to be processed again. If any of the functioning valves in this route remain closed, then gas will not be processed (OR4). As mentioned before this will not lead to a disaster. At the same time, the route to flaring must get closed again and if any of the valves remain open (OR1), then there will be a disaster (Table 4, Row#02, Col2; Row#02, Col7).

2) SYSTEM FUNCTION DURING VERY HIGH PRESSURE AND NORMALIZATION (TABLE3#COLUMN8, COLUMN9)

During the flow of very high pressure and its normalization the same components described in 3.2.1 need to open and get closed (**Branch #05** and **Branch #06** in fault tree).

But the route to flaring needs to open to its full capacity (**Branch#03**) since the pressure is very high. As a result, FOV is opened by signals from sensors and PV2 buckles automatically. Failure of both of these components (AND3) leads to a disaster (Table 4, Row#03, Col8). During normalization from very high, both these valves need to close so that there is no flashback. If anyone of these two valves remain open (OR2), there will be a disaster (Table 4, Row#04, Col9).

It must be noted that during very high pressure, when RV3 closes, PLC also sends an automatic signal to open FOV so that this components function does not only rely on the sensors.

3) SYSTEM FUNCTION DURING VERY HIGH PRESSURE AND NORMALIZATION (TABLE4#COLUMN8, COLUMN9)

During the flow of very high pressure and its normalization the same components described in 3.2.1 need to open and get closed (**Branch #05** and **Branch #06** in fault tree).

But the route to flaring needs to open to its full capacity (**Branch#03**) since the pressure is very high. As a result, FOV is opened by signals from sensors and PV2 buckles automatically. Failure of both of these components (AND3) leads to a disaster (Table 4, Row#03, Col8). During normalization from very high, both these valves need to close so that there is no flashback. If anyone of these two valves remain open (OR2), there will be a disaster (Table 4, Row#04, Col9).

It must be noted that during very high pressure, when RV3 closes, PLC also sends an automatic signal to open FOV so that this components function does not only rely on the sensors.

Moreover, the adoption of the FDEP gates in the fault tree model is motivated by the following reasons:

i) FDEP1: CV3 will fail in case of unavailability of at least 2 out of 3 of sensors in VOR1.
ii) FDEP2: FOV will fail in case of unavailability of the abovementioned sensors and also if RV3 fails to close and PLC will send an automatic signal during very high pressure.
iii) FDEP3: RV3 will fail in case of unavailability of sensors input of AND4.
iv) FDEP4: CV2 will fail in case of unavailability of sensors input of AND5 or AND6.

C. IMPLEMENTATION OF HYBRID DFTS

In the previous sections, Tables 3 and 4, it was discussed that two different kinds of disasters, ‘D1’ and ‘D2’, can happen if the sub-systems identified within their branches are unavailable and some gas pressure scenarios occur. Therefore, a more precise model should take into account also the temporal dependencies between the unavailability of the components that guarantee the activation of the safety mechanisms and the physical conditions happening in the system process. This latter cannot be described by a traditional DFT, therefore also the results that can be achieved with this type of modelling are not the most suitable. In fact – as it will be also shown in the simulation campaign section – DFTs overestimate the probability of failure or – in other words – they compute the system unreliability without being able to distinguish between a fault from a fault that can bring to a disaster.

Therefore, in the case study described, it is important to consider whether gas with critical pressure (GCP) has flowed into a section when a safety component has become unavailable. With reference to Table 3 and 4, the following statements can be pointed out:

- Disaster (D1) occurs when there is a sensitive element (like FGRS or any) the route to which is open in normal pressure. When gas pressure is getting critical, the component in charge to protect the sensitive element should redirect the flow of gas such that the sensitive element remains intact. But, if this component fails and is not repaired before GCP starts to flow, it means that this component will not be able to protect the sensitive element that will get damaged.
- Disaster (D2) occurs in the situation that involve the relief routes that allow GCP to be emitted outside the system. When GCP starts to flow, the components of the relief routes

TABLE 6. Disaster VS Gas behavior VS Time axis.

<table>
<tr><td></td><td colspan="6"><b>Time axis →</b></td></tr>
<tr><td><b>Gas behavior</b></td><td colspan="2">Before the flow of GCP</td><td colspan="2">Gas with <b>critical pressure (GCP)</b> is flowing</td><td colspan="2">GCP is normalizing</td></tr>
<tr><td><b>Component's situation</b></td><td>Gets damaged and repaired before GCP starts to flow</td><td colspan="2">Gets damaged and is being repaired When GCP starts to flow</td><td colspan="2">Gets damaged and gets repaired after the pressure normalizes</td><td>Gets damaged and repaired during a non-critical gas pressure</td></tr>
<tr><td><b>Disaster</b></td><td></td><td colspan="2">D1</td><td colspan="2">D2</td><td></td></tr>
</table>

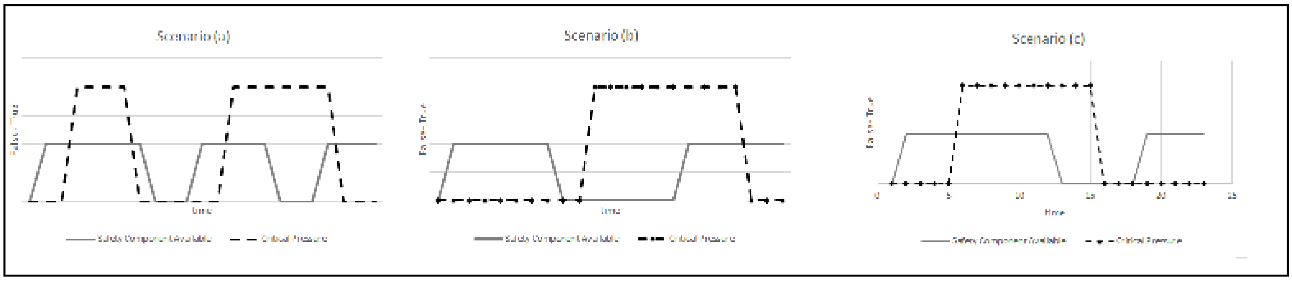


FIGURE 6. Disaster diagram with respect to the occurrence of GCP and availability of protecting components.

open. If GCP starts to normalize, this component should close otherwise there will be a flashback.

Table 6 depicts, according to the temporal dependencies, the order of gas flow with a critical pressure and the components failure (unavailability of a branch). To develop the Hybrid branches, it is required to consider the temporal priority relation between GCP and the unavailability of the safety components. Figure 6 shows three scenarios that can explain the temporal dependencies of Table 5.

- Scenario (a) will not lead to a disaster but only to regular failures because safety components are available during critical pressure.
- Scenario (b) will lead to a disaster in case of unavailability for a component that protects sensitive elements from disaster of type D1. In this case, there is a disaster if the failure of the protecting components happens before GCP starts to flow and its restoration happens after GCP flow, because GCP has flown into the sensitive element.
- Scenario (c) will lead to a disaster in case of unavailability for a component that protects sensitive elements from disaster of type D2. In this case, GCP starts to flow and the protecting components opens correctly to emit the extra volume; afterwards when GCP normalizes, the protecting component should close immediately to avoid air ingression and explosion. If the protecting component gets unavailable (the valve fails to close) before GCP starts to normalize, this will lead to the disaster, regardless if the protecting components is restored afterwards.
- All the other scenarios will not bring to a disaster.

Based on the previous considerations, stochastic hybrid branches can be developed using PAND gates. For each protecting sub-system (or component), it will be added a PAND gate that model the disaster D1 and D2 and added in the branches of the previous DFT.

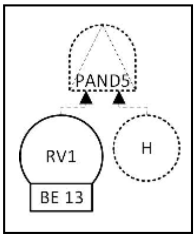


FIGURE 7. Example of PAND for state of D1.

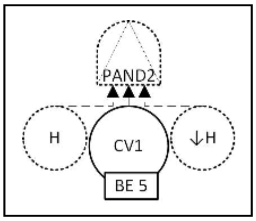


FIGURE 8. Example of PAND for state of D2.

For example, as shown in Figure 7, the RV1 is a component that protects from the D1 disaster in GCS1. If RV1 fails and is being repaired when GCP starts to flow (high pressure gas), there will be a disaster with a damage of the FGRS. Therefore, to model it in this temporal order, a PAND gate can be used as follows.

For a disaster of type D2, we can analyse the example of the CV1. In this case, the temporal dependency has to follow the ordered sequence in which a high pressure occurs (H),

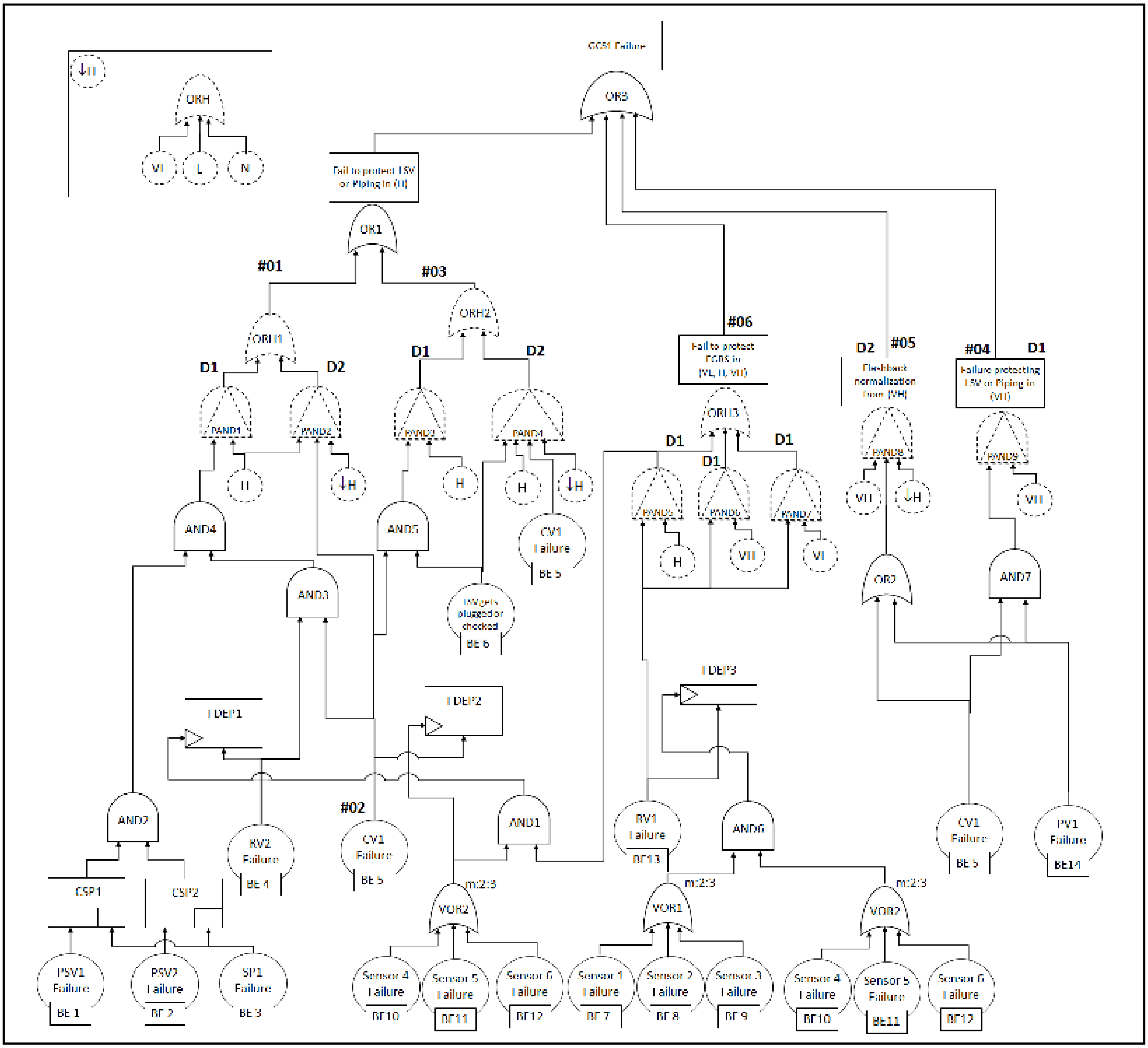


FIGURE 9. GCS1. Hybrid DFT.

CV1 fails and finally the GCP starts normalizing (↓H) before CV1 has been repaired. The PAND2 gate of Figure 8 can model exactly this circumstance using.

Based on the statements above, the Hybrid Fault Tree models of GCS1 and GCS2 are respectively presented in Figure 9 and Figure 10. With the hybrid modelling, the working conditions of the gas pressure can be modelled and the dependability assessment results more accurate.

IV. SIMULATION CAMPAIGN & RESULTS

This section resumes the main results of this paper. The simulation campaigns have been performed using SHyFTOO under the version of Matlab R2018 with a standard desktop workstation having the following characteristics: 16 GB Ram, Intel® Core ^{TM} I7-4790 CPU @ 3.6 GHz, x64 Windows 10.

For each model, the simulation campaigns have been set in order to run 10000 iterations with a mission time of 8760 hours, corresponding to one year at 24-7 service.

Whereas the DFT can be simulated just by coding the corresponding fault tree of Figure 4 and Figure 5, using the parameters of the Table 1, some further modelling operations are needed to carry out the Hybrid DFT simulation. In fact, this latter requires the physical conditions (e.g., gas pressure) of the system process during a year of operation. In order to do that, a historical data series of the system gas pressure was

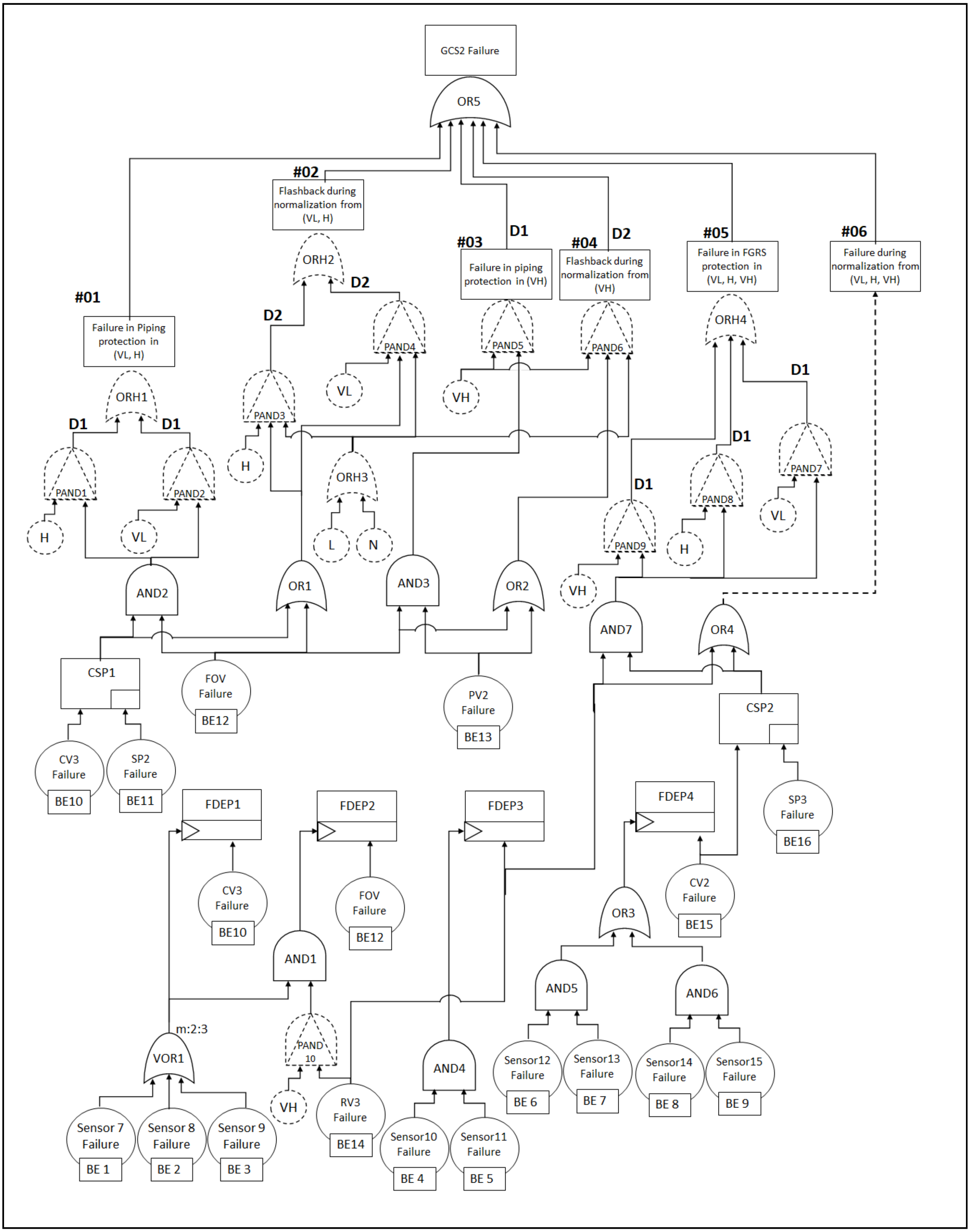


FIGURE 10. **GCS2. Hybrid DFT.**

TABLE 7. Gas pressure condition.

Gas Pressure Condition	Percentage %
Very Low	26.87
Low	20.46
Normal	27.91
High	16.71
Very High	8.03

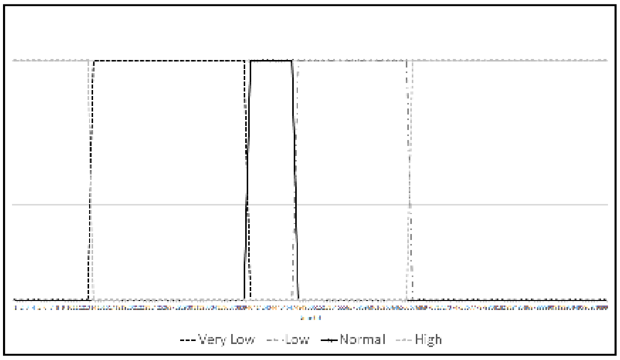


FIGURE 11. Example of fabricated gas pressure condition in the system (100 hours).

gathered from the site by the FEED engineers from the existing field. Table 7 depicts the characteristics of this historical data series which has been used as a pattern for fabricating random samples of input for the Monte Carlo Simulation. For instance, as shown, a very low pressure is revealed for about the 26.87% of the total, whereas the very high only for the 8,03%. In this way, it is possible to configure the SHyFTA model so as to simulate the pressure change during a year of operation for every realization of the Monte Carlo simulation.

Figure 11 shows an example extracted from a random sample of 100 hours, where it is possible to notice the alternation of a pattern (low – very low – normal – high – very low) gas pressure.

A. GCS1 AND GCS2 COMPARISON

Figure 12 allows to compare the unreliability of the system design for the GCS1 and the GCS2 solutions, respectively modelled with the Dynamic Fault Trees of Figure 4 and 5. As said, this modelling takes into account the failures of a system but it is not able to distinguish a fault from a fault that – due to the physical operational conditions – can bring to a disaster. In the DFT modeling, results shown in Figure 12 demonstrate that, under this viewpoint, the GCS1 design looks a bit more reliable than solution GCS2.

But, different conclusions can be drawn analyzing the simulation results of the Hybrid Dynamic Fault Trees of Figure 9 and 10 that have been used to model the disaster scenarios.

As shown in Figure 13, in this case, three trends can be depicted. In fact, the HDFT of GCS2 provides results not only for the cumulated probability of a disaster occurrence, but also for regular faults that, in the HDFT models of GCS2, is due by a failure in branch#06 which, as said in the previous sections, will never turn in a disaster. As can be seen, the green trend (triangle indicator) of Figure 13 combines the cumulated probability of GCS2 disasters with the faults generated from branch #06. But, when the effect of branch #06 is eliminated, and only disasters are considered, it is possible to notice a huge drop (blue trend with cross indicator), meaning that GCS2 performs considerably better than GCS1 against disasters.

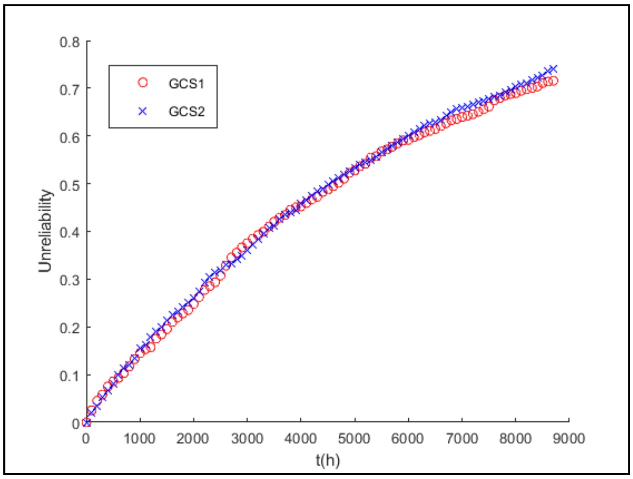


FIGURE 12. Comparison of the system unreliability for GCS1 and GCS2 design.

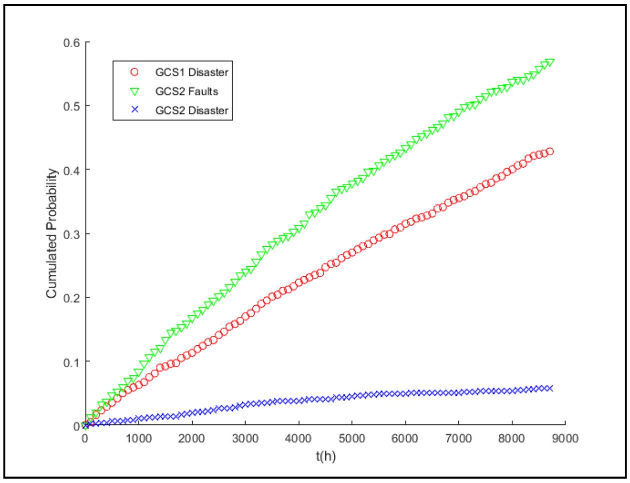


FIGURE 13. Comparison of cumulated probability of disaster occurrence for GCS1 and GCS2 design.

From the previous results, the following considerations can be pointed out:

- For both the GCS1 and GCS2 designs, the HDFT provides lower values of Top Event occurrence than the DFT models. This represents a first important result because it demonstrates that, with a more realistic model representation able to account for the gas pressure operative conditions, the safety sub-systems protecting the FGRS have a greater capability than what was calculated by the DFT models.

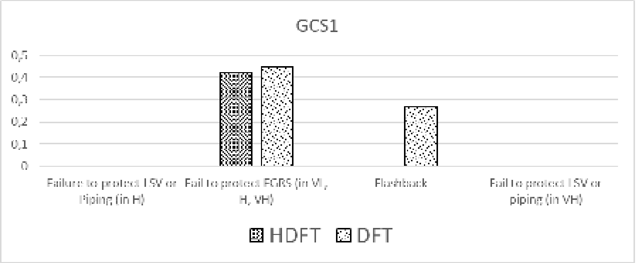


FIGURE 14. Contribution of each branch to the top event of the GCS1 design solution.

- The second important consideration is that, in contrast with the DFT model results, GCS2 is far better because this system design improves tremendously the capability to protect the FGRS against disasters. Figure 13 shows that GCS2 is better at protecting the system against damages although, in terms of regular faults during the mission time GCS1 is still better.

B. SUB-SYSTEMS ANALYSIS

To better understand the system dependencies and identify the critical sub-systems, the unreliability of each branch for both the DFT and the HDFT models has been studied, as shown in Figures 14 and 15. What can be gathered from this analysis is that GCS1 is weaker in protecting FGRS, whereas GCS2 struggles in protecting the system against flashbacks.

More specifically, as shown in Figure 14, the DFT of GCS1 shows that the contribution to system unreliability during mission time of the Fail to Protect FGRS is ∼0.446 whereas Flashback contributes for ∼0.27. Also, in the case of the HDFT, it can be noticed that the main contribution to the system failure is given by the Fail to protect the FGRS (∼0.422).

For the GCS2 design, similar considerations can be pointed out by analysing the results of Figure 16. Flashbacks are the main failure causes in the three branches#02, #04 and #06. Their contributions are respectively ∼0.164, ∼0,313 and ∼0.432.

In this case, this sum is higher than the Top Event unreliability of the GCS2 (∼0.745) because the failure of the FOV is input for both Flashback during normalization (from VL, H) and Flashback during normalization (from VH); therefore, to find the Top Event unreliability, the sum of the previous three contributions has to be subtracted with the probability of the FOV unreliability (∼0.163). On the other hand, the HDFT remarks an increased criticality (around ∼0.512) of the Failure during normalization (from VL, H, VH) with respect to the DFT model, whereas the other branches are considerably reduced. It must be noticed that this event does not bring to a disaster.

C. IMPORTANCE MEASURE ANALYSIS

To improve the accuracy of the investigation, an Importance Measure analysis of the basic components of the systems has been carried out. This type of analysis is an essential tip for the designers to become aware of the components flaws and be able to propose valid alternatives.

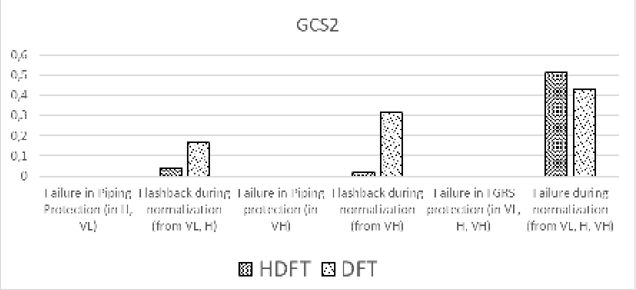


FIGURE 15. Contribution of each branch to the top event of the GCS2 design solution.

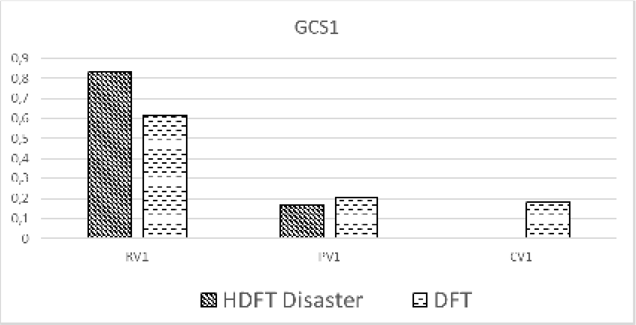


FIGURE 16. Importance measure analysis for the GCS1 design solution.

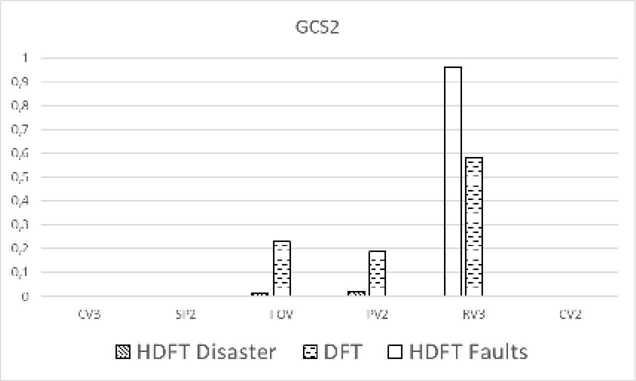


FIGURE 17. Importance measure analysis for the GCS2 design solution.

For the GCS1, the results shown in Figure 16 reveal that the weakness in protecting FGRS, identified from Figure 14, is mainly due to the unreliability of the RV1 (both in the DFT and HDFT modelling). This can be explained by its placement in the conceptual design of GCS1 (see Figure 2). The logical suggestion to correct the weakness in protecting FGRS would be to add another rotary valve, or any other proper type of valve on the way to FGRS, so that if one of them fails to close when gas pressure is getting critical, the other would be able to respond.

As pointed out from Figure 15, the main issue of the GCS2 design is the possibility of flashback. This evidence is further proven by the Importance Measure analysis shown in Figure 17 that identifies the components which require to be strengthened in order to avoid flashback (FOV, PV2 and RV3).

Therefore, to improve the system safety, it would be possible to install a pressure safety valves after each of these components. In fact, a safety valve is designed to automatically close when the pressure has dropped to a normal level [60]. It opens automatically as well when the pressure rises above a certain limit.

Another possible solution would be to inject sweep gas, gathered from the network of recovery units, to maintain a positive pressure in the header route until the problem can be fixed by manpower.

V. CONCLUSION

This paper presented the dependability analysis for the conceptual design of Flare Gas Recovery System to install into an existing plant, performed during the EPC bidding phase. At this stage, after the qualitative study of the proposed Gas Control System design solutions, for the EPC company to bid it is necessary to perform a series of simulations to assess the reliability of the systems so as to be able to judge each proposed alternative by evaluating their capability to maintain a consistent operation and prevention of vital component from fault and disasters.

The process operated by a Gas Control System is complex since it reacts to each operational scenario. Besides this fact, temporal dependencies between failures, repairs and restorations of each component and working conditions must be considered. For this reason, engineers and risk technicians must be able to identify the most dangerous risk scenarios and model the system functions accordingly.

Model-based dependability analysis offers tools and techniques that assist risk engineers to perform the dependability assessment of safety critical systems. Among the modelling tools of model-based dependability analysis, Stochastic Hybrid Fault Tree Automaton (known also as Hybrid Dynamic Fault Tree) looks the most promising methodology as it can effectively model the complex process operated by a safety critical system, being able to couple the deterministic and the stochastic processes of a system.

In this paper, the comparison of two design solutions of the Flare Gas Recovery Systems has been performed studying the reliability and the probability of a disaster occurrence. To achieve these goals, the two systems have been simulated using Dynamic Fault Trees and Hybrid Dynamic Fault Trees models. It was shown that the former type of modelling can provide results that cannot distinguish between failures and disasters. In fact, although disasters depend on the failure behaviour of the system, they occur only under certain gas pressure conditions that Dynamic Fault Tree cannot model. To tackle the limitation of Dynamic Fault Trees, in this study the gas pressure scenarios that lead to a disaster have been analysed and modelled with Hybrid Dynamic Fault Trees. This represents an important novelty with respect to previous studies.

The models and the simulations have been developed using SHyFTOO library, a Monte-Carlo simulation-based library compatible with Simulink toolbox, a powerful environment in which stochastic and physical traits of a system can be modeled.

The adoption of the Hybrid Dynamic Fault Tree allowed to understand that the two design solutions of the Flare Gas Recovery Systems presented by the EPC company perform in a different manner against regular failure and disasters; in particular, it was possible to understand that the solution that performs better against regular failures presents, on the other hand, a higher probability of handling non appropriately an abnormal gas pressure condition which can lead to a disaster. This demonstrates that the EPC company must also investigate the implications of such events and eventually analyse further improvements to strengthen the system and the components which require more attention. Therefore, to increase the knowledge of the systems, this research has presented also an Importance Measure analysis that can be used by the EPC engineers as a pointer of areas where improvements must be pursued.

The main limitation of the proposed research is the lack of information – at the component level – of the gas pressure condition during the operations. As said, the simulation of the physical process has been modelled starting from the aggregated data provided by the FEED engineers which have been used to randomize the working conditions along one year of operations. Therefore, in future research, the idea that has been pointed out together with the FEED engineers is to improve the model of the physical process so as to describe more precisely the working conditions of the various sections of the plant and have a more realistic idea of the gas pressure conditions at the components level. In this way, the main limitation of this current study can be overcome, and more precise results can be achieved.

REFERENCES

[1] O. S. Ismail and G. E. Umukoro, "Global impact of gas flaring," *Energy Power Eng.*, vol. 4, no. 4, Jan. 2012, doi: 10.4236/epe.2012.44039.

[2] K. Emumejaye, "Effects of gas flaring on surface and ground water in irri town and environs, Niger-Delta, Nigeria," *IOSR J. Environ. Sci., Toxicol. Food Technol.*, vol. 1, no. 5, pp. 29–33, 2012, doi: 10.9790/2402-0152933.

[3] M. Soltanieh, A. Zohrabian, M. J. Gholipour, and E. Kalnay, "A review of global gas flaring and venting and impact on the environment: Case study of Iran," *Int. J. Greenhouse Gas Control*, vol. 49, pp. 488–509, Jun. 2016, doi: 10.1016/j.ijggc.2016.02.010.

[4] E. Ojijiagwo, C. F. Oduoza, and N. Emekwuru, "Economics of gas to wire technology applied in gas flare management," *Eng. Sci. Technol., Int. J.*, vol. 19, no. 4, pp. 2109–2118, Dec. 2016, doi: 10.1016/j.jestch.2016.09.012.

[5] E. A. Emam, "GAS flaring in industry: An overview," *Petroleum Coal*, vol. 57, no. 5, pp. 532–555, 2015.

[6] G. Comodi, M. Renzi, and M. Rossi, "Energy efficiency improvement in oil refineries through flare gas recovery technique to meet the emission trading targets," *Energy*, vol. 109, pp. 1–12, Aug. 2016, doi: 10.1016/j.energy.2016.04.080.

[7] E. Emam, "Gas flaring reduction: Perspective environmental and economical," *Int. J. Sci. Res. Sci., Eng. Technol.*, vol. 2, pp. 240–251, 2016.

[8] M. R. Rahimpour and S. M. Jokar, "Feasibility of flare gas reformation to practical energy in Farashband gas refinery: No gas flaring," *J. Hazardous Mater.*, vols. 209–210, pp. 204–217, Mar. 2012, doi: 10.1016/j.jhazmat.2012.01.017.

[9] M. R. Rahimpour, Z. Jamshidnejad, S. M. Jokar, G. Karimi, A. Ghorbani, and A. H. Mohammadi, "A comparative study of three different methods for flare gas recovery of Asalooye gas refinery," *J. Natural Gas Sci. Eng.*, vol. 4, pp. 17–28, Jan. 2012, doi: 10.1016/j.jngse.2011.10.001.

[10] M. Zolfaghari, V. Pirouzfar, and H. Sakhaeinia, "Technical characterization and economic evaluation of recovery of flare gas in various gas-processing plants," *Energy*, vol. 124, pp. 481–491, Apr. 2017, doi: 10.1016/j.energy.2017.02.084.

[11] P. W. Fisher and D. Brennan, "Minimize flaring with flare gas recovery," *Hydrocarb. Process.*, vol. 6, no. 81, pp. 83–85, 2002.

[12] J. P. Allamaraju and R. Mukherjee, "Successful implementation of flare gas recovery systems in Gasco plants," in *Proc. Soc. Pet. Eng. Abu Dhabi Int. Pet. Exhib. Conf.*, Jan. 2016 Art. no. SPE-183248-MS, doi: 10.2118/183248-MS.

[13] E. Barekat-Rezaei, M. Farzaneh-Gord, A. Arjomand, M. Jannatabadi, M. Ahmadi, and W.-M. Yan, "Thermo–economical evaluation of producing liquefied natural gas and natural gas liquids from flare gases," *Energies*, vol. 11, no. 7, p. 1868, Jul. 2018, doi: 10.3390/en11071868.

[14] A. Hajizadeh, M. Mohamadi-Baghmolaei, R. Azin, S. Osfouri, and I. Heydari, "Technical and economic evaluation of flare gas recovery in a giant gas refinery," *Chem. Eng. Res. Des.*, vol. 131, pp. 506–519, Mar. 2018, doi: 10.1016/j.cherd.2017.11.026.

[15] A. Y. Ibrahim, A. O. Ghallab, M. A. Gadalla, S. S. Makary, and F. H. Ashour, "Technical and economical/financial feasibility analyses of flared gas recovery in Egypt from oil and gas industry from international/national oil companies' perspectives," *Clean Technol. Environ. Policy*, vol. 19, no. 5, pp. 1423–1436, Jul. 2017, doi: 10.1007/s10098-017-1340-2.

[16] M. R. Johnson and A. R. Coderre, "Opportunities for CO_2 equivalent emissions reductions via flare and vent mitigation: A case study for Alberta, Canada," *Int. J. Greenhouse Gas Control*, vol. 8, pp. 121–131, May 2012, doi: 10.1016/j.ijggc.2012.02.004.

[17] K. Kabirifar and M. Mojtahedi, "The impact of engineering, procurement and construction (EPC) phases on project performance: A case of large-scale residential construction project," *Buildings*, vol. 9, no. 1, p. 15, Jan. 2019, doi: 10.3390/buildings9010015.

[18] O. Zadakbar, A. Vatani, and K. Karimpour, "Flare gas recovery in oil and gas refineries," *Oil Gas Sci. Technol. Revue de l'IFP*, vol. 63, no. 6, pp. 705–711, Nov. 2008, doi: 10.2516/ogst:2008023.

[19] F. Chiacchio, F. Famoso, D. D'Urso, and L. Cedola, "Performance and economic assessment of a grid-connected photovoltaic power plant with a storage system: A comparison between the north and the south of Italy," *Energies*, vol. 12, no. 12, p. 2356, Jun. 2019, doi: 10.3390/en12122356.

[20] A. Avizienis, J. C. Laprie, and B. Randell, *Fundamental Concepts of Dependability*. University of Newcastle upon Tyne, Computing Science, 2001, pp. 7–12.

[21] G. Buja, S. Castellan, R. Menis, and A. Zuccollo, "Dependability of safety-critical systems," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, vol. 3, Dec. 2004, pp. 1561–1566, doi: 10.1109/icit.2004.1490799.

[22] M. Alauddin, F. Khan, S. Imtiaz, and S. Ahmed, "A probabilistic risk assessment of offshore flaring systems using Bayesian network," in *Advances in Industrial Safety*. Singapore: Springer, 2020, pp. 121–131.

[23] I. N. Karelin, "Improving the design reliability of petroleum pipeline components on repair," *Chem. Petroleum Eng.*, vol. 41, nos. 9–10, pp. 560–564, Sep. 2005, doi: 10.1007/s10556-006-0019-z.

[24] F. Eljack and M.-K. Kazi, "Process safety and abnormal situation management," *Current Opinion Chem. Eng.*, vol. 14, pp. 35–41, Nov. 2016, doi: 10.1016/j.coche.2016.07.004.

[25] H. Huang, C. Zhu, W. Zhang, S. Hao, S. Zhang, J. Leng, and Y. Wei, "Design and analysis of the multifunctional oil-injection equipment for deep-sea hydraulic systems," *IEEE Access*, vol. 8, pp. 143679–143691, 2020.

[26] J. I. Aizpurua and E. Muxika, "Model-based design of dependable systems: Limitations and evolution of analysis and verification approaches," *Int. J. Adv. Secur.*, vol. 6, no. 1, pp. 16–31, 2015.

[27] S. Sharvia, S. Kabir, M. Walker, and Y. Papadopoulos, "Model-based dependability analysis: State-of-the-art, challenges, and future outlook," in *Software Quality Assurance: Large Scale and Complex Software-Intensive Systems*, I. Mistrik, R. Soley, N. Ali, J. Grundy, and B. Tekinerdogan, Eds. Amsterdam, The Netherlands: Elsevier, 2016, pp. 251–278.

[28] H. S. and D. Phillips, "Reliability and risk analysis—Failure modes and effects analysis," in *Proc. MTS Dyn. Positioning Conf.*, 1997, pp. 1–13.

[29] S. Kabir, "An overview of fault tree analysis and its application in model based dependability analysis," *Expert Syst. Appl.*, vol. 77, pp. 114–135, Jul. 2017, doi: 10.1016/j.eswa.2017.01.058.

[30] A. Vicenzutti, R. Menis, and G. Sulligoi, "All-electric ship-integrated power systems: Dependable design based on fault tree analysis and dynamic modeling," *IEEE Trans. Transport. Electrific.*, vol. 5, no. 3, pp. 812–827, Sep. 2019, doi: 10.1109/TTE.2019.2920334.

[31] H. Zheng and Y. Tang, "A novel failure mode and effects analysis model using triangular distribution-based basic probability assignment in the evidence theory," *IEEE Access*, vol. 8, pp. 66813–66827, 2020.

[32] Y. Zhou, C. Lin, Y. Liu, and H. Xu, "Analytical study on the reliability of redundancy architecture for flight control computer based on homogeneous Markov process," *IEEE Access*, vol. 6, pp. 2169–3536, 2018.

[33] L. Wang, W. Dai, J. Ai, W. Duan, and Y. Zhao, "Reliability evaluation for manufacturing system based on dynamic adaptive fuzzy reasoning Petri net," *IEEE Access*, vol. 8, pp. 167276–167287, 2020.

[34] X. Yang, Y. Yang, Y. Liu, and Z. Deng, "A reliability assessment approach for electric power systems considering wind power uncertainty," *IEEE Access*, vol. 8, pp. 12467–12478, 2020.

[35] S. Kabir, T. K. Geok, M. Kumar, M. Yazdi, and F. Hossain, "A method for temporal fault tree analysis using intuitionistic fuzzy set and expert elicitation," *IEEE Access*, vol. 8, pp. 980–996, 2020.

[36] M. Walker, L. Bottaci, and Y. Papadopoulos, "Compositional temporal fault tree analysis," in *Proc. 26th Int. Conf. (SAFECOMP)*, in Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 4680. Nuremberg, Germany: Springer, Sep. 2007, pp. 106–119, doi: 10.1007/978-3-540-75101-4_12.

[37] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Trans. Rel.*, vol. 41, no. 3, pp. 363–377, Sep. 1992.

[38] F. Chiacchio, D. D'Urso, L. Compagno, M. Pennisi, F. Pappalardo, and G. Manno, "SHyFTA, a stochastic hybrid fault tree automaton for the modelling and simulation of dynamic reliability problems," *Expert Syst. Appl.*, vol. 47, pp. 42–57, Apr. 2016, doi: 10.1016/j.eswa.2015.10.046.

[39] G. Babykina, N. Brinzei, J.-F. Aubry, and G. Deleuze, "Modeling and simulation of a controlled steam generator in the context of dynamic reliability using a stochastic hybrid automaton," *Rel. Eng. Syst. Saf.*, vol. 152, pp. 115–136, Aug. 2016, doi: 10.1016/j.ress.2016.03.009.

[40] F. Khan, S. Rathnayaka, and S. Ahmed, "Methods and models in process safety and risk management: Past, present and future," *Process Saf. Environ. Protection*, vol. 98, pp. 116–147, Nov. 2015, doi: 10.1016/j.psep.2015.07.005.

[41] M. T. Berrouane and Z. Lounis, "Safety assessment of flare system by fault tree analysis," *J. Chem. Technol. Metall.*, vol. 51, no. 2, pp. 229–234, 2016.

[42] S. Kabir, M. Taleb-Berrouane, and Y. Papadopoulos, "Dynamic reliability assessment of flare systems by combining fault tree analysis and Bayesian networks," *Energy Sour. A, Recovery, Utilization, Environ. Effects*, pp. 1–18, Sep. 2019, doi: 10.1080/15567036.2019.1670287.

[43] B. O. Evbuomwan, V. Aimikhe, and J. Y. Datong, "Simulation and evaluation of a flare gas recovery unit for refineries," *Eur. J. Adv. Eng. Technol.*, vol. 5, no. 10, pp. 775–781, 2018.

[44] M. E. Sangsaraki and E. Anajafi, "Design criteria and simulation of flare gas recovery system," in *Proc. Int. Conf. Chem., Food Environ. Eng.*, Jan. 2015, pp. 11–12, doi: 10.17758/iaast.a0115008.

[45] K. H. Fard and M. Shafiee, "Recovering gas flares from the 12th gas phase of the south pars gas refinery," *Adv. J. Chem. A*, vol. 3, no. 1, pp. 49–57, 2020, doi: 10.33945/sami/ajca.2020.1.6.

[46] P. Glénat, J. L. Peytavy, N. Holland-Jones, and M. Grainger, "South-pars phases 2 and 3: The Kinetic Hydrate Inhibitor (KHI) experience applied at field start-up," in *Proc. Abu Dhabi Int. Conf. Exhib.*, 2004, Art. no. SPE-88751-MS, doi: 10.2118/88751-MS.

[47] F. Chiacchio, J. I. Aizpurua, L. Compagno, S. M. Khodayee, and D. D'Urso, "Modelling and resolution of dynamic reliability problems by the coupling of simulink and the stochastic hybrid fault tree object oriented (SHyFTOO) library," *Information*, vol. 10, no. 9, p. 283, Sep. 2019, doi: 10.3390/info10090283.

[48] *Project Lifecycle Engineering*, Chiyoda, Kanagawa, Japan, 2017.

[49] S. K. Srivastava, O. Takeidinne, and H. Singh, "FEED endorsement—A challenge to EPC contractor's engineering team," presented at the Abu Dhabi Int. Petroleum Conf. Exhib., 2012.

[50] S. K. Srivastava and O. Takeidinne, "Feed endorsement—A challenge to EPC contractor's engineering team," in *Proc. Soc. Petroleum Eng. Abu Dhabi Int. Petroleum Exhib. Conf. (ADIPEC), Sustain. Energy Growth, People, Responsibility, Innov.*, vol. 1, Nov. 2012, pp. 301–311, doi: 10.2118/158941-MS.

[51] D. N. P. Murthy, M. Rausand, and S. Virtanen, "Investment in new product reliability," *Rel. Eng. Syst. Saf.*, vol. 94, no. 10, pp. 1593–1600, Oct. 2009, doi: 10.1016/j.ress.2009.02.031.

[52] *OREDA: Offshore Reliability Data Handbook*, OREDA, Oslo, Norway, 2002.

[53] F. Chiacchio, J. I. Aizpurua, L. Compagno, and D. D'Urso, "SHyFTOO, an object-oriented Monte Carlo simulation library for the modeling of stochastic hybrid fault tree automaton," *Expert Syst. Appl.*, vol. 146, May 2020, Art. no. 113139, doi: 10.1016/j.eswa.2019.113139.

[54] F. Chiacchio, L. Compagno, D. D'Urso, G. Manno, and N. Trapani, "Dynamic fault trees resolution: A conscious trade-off between analytical and simulative approaches," *Rel. Eng. Syst. Saf.*, vol. 96, no. 11, pp. 1515–1526, Nov. 2011, doi: 10.1016/j.ress.2011.06.014.

[55] Z. Tang and J. B. Dugan, "Minimal cut set/sequence generation for dynamic fault trees," in *Proc. Annu. Symp. Rel. Maintainability (RAMS)*, 2004, pp. 207–213, doi: 10.1109/rams.2004.1285449.

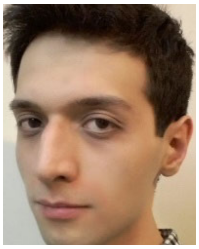
[56] J. Faulin, A. A. J. Perez, S. S. M. Alsina, and J. Ramirez-Marquez, *Simulation Methods for Reliability and Availability of Complex Systems* (Springer Series in Reliability Engineering), J. Faulin, Ed. Springer, 2010, pp. 1–9. [Online]. Available: https://www.springer.com/gp/book/9781848822122

[57] F. Chiacchio, D. D'Urso, G. Manno, and L. Compagno, "Stochastic hybrid automaton model of a multi-state system with aging: Reliability assessment and design consequences," *Rel. Eng. Syst. Saf.*, vol. 149, pp. 1–13, May 2016.

[58] F. Chiacchio, D. D'Urso, F. Famoso, S. Brusca, J. I. Aizpurua, and V. M. Catterson, "On the use of dynamic reliability for an accurate modelling of renewable power plants," *Energy*, vol. 151, pp. 605–621, May 2018, doi: 10.1016/j.energy.2018.03.101.

[59] F. Famoso, S. Brusca, D. D'Urso, A. Galvagno, and F. Chiacchio, "A novel hybrid model for the estimation of energy conversion in a wind farm combining wake effects and stochastic dependability," *Appl. Energy*, vol. 280, Dec. 2020, Art. no. 115967, doi: 10.1016/j.apenergy.2020.115967.

[60] D. J. Breaux, "Safety valve closure system," U.S. Patent WO 1996 012 087, Oct. 1994. [Online]. Available: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO1996012087



SOHEYL MOHEB KHODAYEE received the M.Sc. degree in industrial engineering from Islamic Azad University South Tehran Branch.

He has a strong knowledge on hazardous processes for oil industry by his multiple collaboration with several private companies. His research interests include dependability assessment, stochastic hybrid automaton, dynamic systems, shock-degradation models, simulation, machine learning, and risk-based integrity assessment and management.

FERDINANDO CHIACCHIO received the Laurea and Ph.D. degrees from the University of Catania, in 2005 and 2010, respectively. He is currently a Researcher with the Department of Electrical Electronic and Computer Engineering, University of Catania. His research interests include reliability, performability, dependability of complex systems for hazardous industrial plants and renewable power plants, Industry 4.0, supply chain management, and blockchain applications for the industrial field.

YIANNIS PAPADOPOULOS is currently a Professor and a Leader of the Dependable Systems Research Group with the University of Hull. He pioneered the HiP-HOPS MBSA method and contributed to the EAST-ADL automotive design language, working with Volvo, Honda, Continental, Honeywell, and DNV-GL, among others. He is actively involved in two technical committees of IFAC (TC 1.3 & 5.1). His awards and honors include the Frew Fellowship (Australian Academy of Science), the I. I. Rabi Prize (APS), the European Frequency and Time Forum Award, the Carl Zeiss Research Award, the William F. Meggers Award, and the Adolph Lomb Medal (OSA).