applied sciences

MDPI

Article

An Integrated FTA-FMEA Model for Risk Analysis of Engineering Systems: A Case Study of Subsea Blowout Preventers

Mahmood Shafiee [1], Evenye Enjema [1,*] and Athanasios Kolios [2]

[1] Department of Energy and Power, Cranfield University, College Road, Bedfordshire MK 43 0AL, UK; m.shafiee@cranfield.ac.uk

[2] Department of Naval Architecture, Ocean & Marine Engineering, University of Strathclyde, 100 Montrose Street, Glasgow G4 0LZ, UK; athanasios.kolios@strath.ac.uk

* Correspondence: e.m.enjema@cranfield.ac.uk; Tel.: +44-1234-750111

Received: 3 February 2019; Accepted: 15 March 2019; Published: 21 March 2019

Abstract: Engineering systems such as energy production facilities, aviation systems, maritime vessels, etc. continue to grow in size and complexity. This growth has made the identification, quantification and mitigation of risks associated with the failure of such systems so complicated. To solve this problem, several advanced techniques such as Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), Reliability-Block Diagram (RBD), Reliability-Centered Maintenance (RCM), Monte-Carlo Simulation (MCS), Markov Analysis (MA) and Bayesian Networks (BN) have been developed in the literature. In order to improve the strengths and eliminate the drawbacks of classical techniques, some hybrid models have been recently developed. In this paper, an integrated FTA and FMEA model is proposed for risk analysis of safety-critical systems. Minimal cut sets derived from the fault trees are weighted based on Birnbaum's measure of importance and then the weights are used to revise Risk Priority Numbers (RPNs) obtained from the use of traditional FMEA techniques. The proposed model is applied to a Blowout Preventer (BOP) system operating under erratic and extreme conditions in a subsea oil and gas field. Though those failures caused by kill valves and hydraulic lines remain among the top risks in the BOP system, significant differences are revealed in risk rankings when the results from the hybrid approach are compared with those obtained from the classical risk analysis methods.

Keywords: Fault Tree Analysis (FTA); Failure Mode and Effects Analysis (FMEA); blowout preventer (BOP); risk analysis; minimal cut set; Birnbaum's measure

1. Introduction

A system is considered complex if it comprises of several interacting components whose series/parallel breakdown is impossible and the overall task cannot be obtained by the summation of individual components' activities [1]. Regardless of the degree of intricacy of the complex system under study, some components are deemed critical, relative to others, regarding the safety and functionality of the entire system. Due to the increasing complexity of engineering systems, the identification and evaluation of risks associated with the failure of individual components is usually the starting point for efficient reliability and safety analysis. For this purpose, several advanced techniques such as Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), Reliability Block Diagram (RBD), Reliability-Centered Maintenance (RCM), Monte-Carlo Simulation (MCS), Markov Analysis (MA) and Bayesian Networks (BN) have been developed in the literature [2–4].

FTA is a 'top down' Boolean logic tool commonly used to identify possible causes for potential operating hazards or an undesired event. FMEA is another risk analysis technique that is extensively

used across different industries, such as aerospace, automotive, energy, transport, etc. for determining failure modes and corresponding effects on system performance. The successful application of both the FTA and FMEA techniques has increased their adoption in several reliability and safety engineering analyses studies. However, due to inherent limitations of each technique, coupled with the growing complexity of engineering systems, the use of hybrid models has become very popular in recent years.

Integrated FTA and FMEA has been employed coherently and concurrently to enhance and complement each other in several reliability applications. Forward integration (i.e., FMEA to FTA) and backward integration (i.e., FTA to FMEA) have been proposed, with divers' advantages associated with each integration direction [5,6]. Lutz & Woodhouse [7] also propounded a bi-directional intertwine of both techniques and used it to certify safety-critical software, paving the way for numerous studies on integrating the software domains of both tools. The combination has successfully been applied in civil aerospace and automotive domains. To effectively achieve a set reliability goal, ensure thoroughness and completeness of analysis, and improve quality of analysis without compromise on overall safety, it is necessary to redefine the underlying criteria governing techniques in a combinatorial framework. In Xiao et al. [8], only the occurrence (O) of a failure is taken into consideration because the complex system under consideration was non-repairable. Equal importance was given to all minimal cut sets in terms of their effect on system performance, which caused the severity (S) of failure for all the system components to be same.

By using the minimal cut sets theory and Birnbaum's measure of importance, this paper aims to develop a modified FMEA approach in the backward integration with FTA tool for the identification, evaluation and prioritization of failure risks in safety-critical systems. In order to appropriately identify and rank components according to their criticality, a weight will be assigned to the Risk Priority Number (RPN) associated with each component's failure mode. This weight represents the importance of the component in overall system functionality. A case study of a subsea Blowout Preventer (BOP) is presented to illustrate the applicability of the proposed model.

The rest of the paper continues with a background review of risk analysis techniques in Section 2, followed by a full presentation of our proposed FTA-FMEA methodology in Section 3. Section 4 presents the case study and Section 5 concludes our paper.

2. Research Background

2.1. Fault Tree Analysis (FTA)

FTA is a deductive technique for identifying, evaluating, and modeling the interrelationship between events leading to a failure or an undesired state [9]. It is a scientifically sound and proven technique that models complex system interactions in an easy-to-read visual model. Containing qualitative (cut sets) and quantitative (probabilities) sides, the structured, repetitive and methodical construction process results in layers, levels and branches. Once a logical and systematic picture of all immediate and basic causes leading to top event are identified, undesired events are clearly depicted. Though FTA employs Boolean logic to combine a series of lower-level events causing an undesired state of a system, the technique is static and incapable of examining multiple failures [10]. It also is unintuitive and lacks the ability to properly account for dynamic interactions between components. These and many other drawbacks make FTA limited in modeling dynamic complex systems.

2.2. Failure Mode and Effects Analysis (FMEA)

FMEA is a highly structured approach through which all potential failure modes of a system and their effects can be identified, evaluated, and prioritized. The technique can result in cost/time-savings when employed during early design stages by exposing probable operational challenges and eliminating cascading failures. In this technique, the risk score for each failure mode is obtained by

multiplying the individual scores for three risk factors of severity (S), occurrence (O), and detectability (D). This composite risk is called "Risk Priority Number (RPN)" and is calculated by:

$$RPN = S \times O \times D \quad (1)$$

where the risk factors S, O and D are rated on a scale 1–10 for each failure mode using the guidelines presented in reference [11]. Therefore, the RPN values for different failure modes will range between 1 and 1000. Engineers should assign a threshold RPN value to classify failure modes. For instance, in the current FMEA technique, precautions are taken for all failure modes whose RPN values exceed 100. Thus, a failure mode with RPN = 100 is considered as 'corrective action required', whereas another failure mode with RPN = 98 is classed as 'consider corrective action'.

The general principle governing the multiplication of risk factors to obtain RPNs and prioritization of failure modes has been largely criticized [12]. For example, the three risk factors S, O and D are assumed to have the same importance; or various combinations of S, O and D may produce an identical RPN value, whereas the risk implication may be totally different and may result in high-risk events going unnoticed; etc. Extensive work has been done in the recent years to improve the FMEA process (see, e.g., references [13–15]). According to a detailed literature review performed by [16], Artificial Intelligence (AI), fuzzy rule-based systems, Grey theory, and Multi-Criteria Decision Analysis (MCDA) models such as Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP) are the most prominent methods used for overcoming the FMEA limitations. Furthermore, the cost-based FMEA models pioneered by Gilchrist [17] have also gained popularity.

2.3. FTA and FMEA

Recently, applying both the FTA and FMEA techniques either simultaneously or in succession has been proven to be complementary, effective and increasingly popular. Employed systematically, an integrated FTA-FMEA technique can provide a thorough evaluation of system safety concerns [18]. FTA yields a comprehensive breakdown of faults leading to the undesired top event, whilst FMEA furnishes the exact fashion in which these faults exists and their direct effects on the top event, making the combination appropriate for safety and reliability analyses.

The backward integration of both tools seemingly provides stronger advantages, though many researchers argue advantages depend on the specific application [9]. Khaiyum and Kumaraswamy [19] carried out FTA in parallel and FMEA sequentially, to analyze and diagnose the different causes of failures in a gas leak detection system. Limitations of the individual techniques were however not explored. Bluvband et al. [20] in a unified bouncing approach considered multiple point failures through interaction matrices, a major enhancement to the traditional FMEA. The interaction between the techniques grows in complexity, requiring in-depth knowledge of the tools and particularly of the system under study.

Employing the combination of FTA and FEMA for identifying critical components and reliability analysis of highly complex systems has received little attention. Zhai et al. [21] combined three methods of critical component identification, namely reliability prediction, FMEA and FTA in a reliability tolerance design program for light-emitting diode (LED). Liu et al. [5] used the combination of FTA and FMEA techniques to identify critical components in the manufacturing processes of a photovoltaic power station in the bi-directional fashion, revising minimal cut sets and continually refining them. Though software usage is incorporated, the process remains long and complex. As clearly seen, these methodologies are not without limitations. Therefore, there still exists a crucial need to manage different criteria of risk analysis techniques in a combinatorial framework to efficiently furnish and complement each other, and be pertinent to specific safety and reliability requirements. In order to tap maximum benefits of an FTA-FMEA integration, minimal cut set theory will be used in this study.

Weights (w) are assigned to RPN values in the FMEA technique to incorporate the importance of each component in the system. Therefore, the weighted RNP value is calculated by Equation (2), that is,

$$\text{WRPN} = w \times \text{S} \times \text{O} \times \text{D} \tag{2}$$

where as shown, w is factored into traditional RPN values to prioritize failure modes and thereafter critical components. These weights are vital as they are representative of the importance of minimal cut sets and hence all components are represented by the latter. The FTA methodology is selected for this purpose, as it readily provides and ranks minimal cut sets in terms of importance to system performance. Subsequent breakdown of minimal cut sets allows all components to be analyzed in FMEA worksheets. Simplicity and ease of use are introduced through underlying theory that links both techniques and the complex system under consideration, and is streamlined to component level. The criticality of components is then calculated, not based on RPN but on the weighted RPN. The details of the methodology are presented in the next Section.

3. Proposed Methodology

To integrate both the FTA and FMEA techniques for the purposes of identifying, evaluating and prioritizing failure modes, a methodology is proposed based on the minimal cut sets theory and Birnbaum's measure of importance. In the backward integration framework, as shown in Figure 1, components of the complex system under consideration are de-coupled by means of the FTA technique. The undesired top event is identified based on the reliability requirements of the complex system and initial itemization of components emanates from the fault trees. Results provide information to subsequently adjust the FMEA criteria. With root nodes in the fault tree forming the base for system function in the failure mode table, probability, severity and detectability measures are modified based on the set reliability goal. The steps of the proposed methodology are explained below:

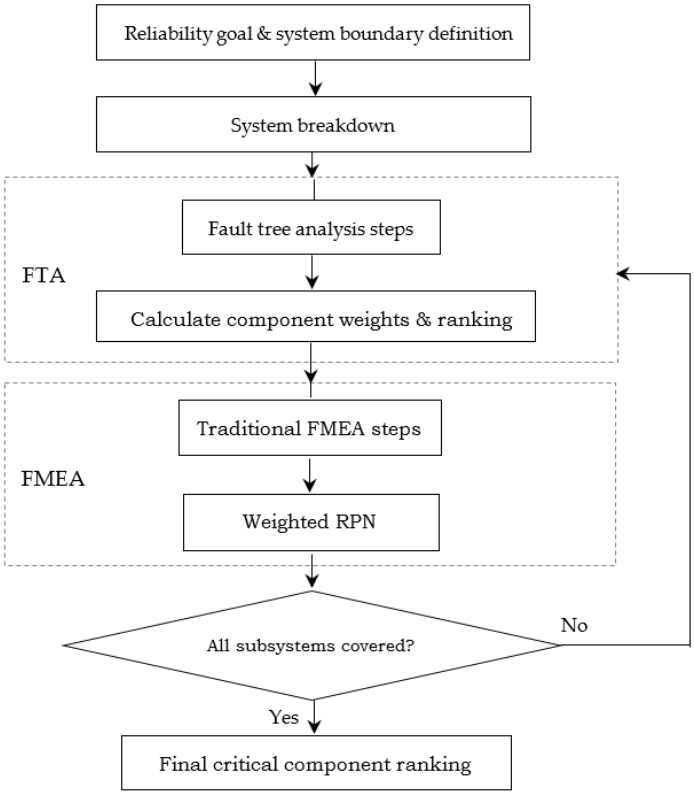

Figure 1. FTA-FMEA integration framework.

3.1. Reliability Goal and System Boundary Definition

As a preliminary step in reliability assessment, particularly for complex systems, establishing generic reliability requirements of the system under consideration acts as a reference for further verification and validation. More so, the scope and element boundaries of the system require elucidation as complexity by definition may depict considerably large systems, interacting with several other elements.

3.2. System Breakdown

As stated by Kolowrocki [1], it is nearly impossible to model a complex system using the traditional reliability analysis methods. The logical approach for this purpose is to subdivide the system into smaller units and employ probabilistic techniques to calculate overall reliability, based on reliability of the subsystems. Once the scope and boundaries are defined, clarity on further categorization of the system under consideration is facilitated, particularly for any expert or analyst with considerable knowledge.

3.3. FTA Steps

This phase includes slight modifications to the traditional FTA steps. The top event is defined and all immediate causes are identified. Again, secondary level events are specified and all root causes down to basic level are identified. The fault tree diagram is built and different fault combinations leading to top event are presented. At this stage, several fault trees may become necessary, dependent on the complexity of the system under consideration. For this reason, utilization of software applications for building and analyzing fault trees can facilitate the process. Finally, minimal cut sets are obtained and their importance weights are evaluated. Assuming w is an independent function variable representing the importance of ith minimal cut set in the fault tree structure, we have:

$$w_i = F(X_i),\ i = 1, 2 \tag{3}$$

where X_i represents the importance of the ith minimal cut set and $F(X_i)$ is a function with independent variable X_i. By substituting Equation (3) in Equation (2), we have:

$$WRPN_i = F(X_i) \times S_i \times O_i \times D_i, \cdots i = 1, 2 \tag{4}$$

Quantitative perspectives on dominant contributors to the top event can be provided by calculating the importance measure of the components in the system. Several methods such as Fussell-Vesely, Birnbaum, etc. have been developed in the literature for this purpose [22]. Though Fussell-Vesely is the most commonly used approach, it does not necessarily identify all minimal cut sets in a complex system. Birnbaum's measure is hence selected and used in this study as modification and versatility based on system application is possible. Hence, the importance of the ith minimal cut set is given by:

$$X_i = \delta hp / \delta p_i = h(1_i, p^{(i)}) - h(0_i, p^{(i)}) \tag{5}$$

where $h(1_i, p^{(i)})$ presents the probability that the system fails when component i fails and $h(0_i, p^{(i)})$ presents the probability that the system fails when component i is working. w_i is a value between zero and one, i.e., $w_i \in [0,1]$, and thus it will have little impact on RPN values which are integer numbers between 1 and 1000. Based on the assessment catalogue proposed by Pickard et al. [23], Table 1 is created to magnify individual importance indices and map them to corresponding domain functions $F(X_i)$.

Table 1. Ranking criteria for the weights.

X_i (w_i)	F (X_i)
1 (0.000001)	1
10 (0.00001)	2
100 (0.0001)	3
1000 (0.001)	4
5000 (0.005)	5
10000 (0.01)	6
50000 (0.05)	7
100000 (0.1)	8
500000 (0.1)	9
1000000 (1)	10

3.4. FMEA Steps

Aside from typical FMEA steps that are detailed and explained in reference [11], the additional tasks that should be implemented at this stage include revising traditional RPN values and ranking components based on the weighted RPNs. Experts brainstorm and report the results as in the traditional FMEA process. In this case, the minimal cut sets that were obtained from the fault trees aid the failure mode identification process. The weights are multiplied with RPNs obtained from the traditional FMEA procedure. It must be noted that minimal cut sets may include one or more components which should be assigned relative importance, as multiple failures are not considered. Components with highest RPNs may not necessarily possess highest WRPNs in this methodology, hence added criteria for ranking. An integrated FTA-FMEA worksheet carrying all necessary data from the traditional FTA and FMEA approaches is shown in Table 2, ending with suggested preventive actions.

Table 2. An integrated FTA-FMEA worksheet.

System:					Report No.											
Component:					Prepared by:											
Team:					Date:											
FTA					FMEA											
MCS	Component/ subsystem	X_i	$F(X_i)$		Fail. mode	Fail. cause	Fail. effect	Ctrl. Mech.	S	O	D	RPN	Priority	WRPN	New priority	Action required

The traditional approaches of both FTA and FMEA techniques are revisited though all relevant software advances. This is to provide the basis for criteria amelioration at every stage. Certain assumptions are considered with this methodology:

- Failure modes in FMEA are a direct result of the faults identified in the FTA process and the failure causes are assumed to be mutually independent.
- In the FMEA method, only the most critical failure modes are considered. Double or multiple failure modes inclusion, though representing a major improvement to traditional FMEA, would be important only when the assessment's aim is beyond the scope of this work such as risk identification and further quantitative analysis.
- The complex system under consideration should be coherent and modular with each module relevant to system functioning, with the FTA possessing only *AND* and *OR* gates.

In the next section, a case study is presented to illustrate the application of the proposed model in an industrial context.

4. Case Study

Blowout Preventers (BOPs) are considered the last line of defense in any drilling or workover oil and gas operations. In an array of stacked valves (see Figure 2), where one or more lower level non-critical components can result in a common undesired event, FTA is a suitable tool as it identifies

minimal cut sets and minimal path sets of common-cause failure (CCF). This is particularly important for BOP systems, as in an assembly with parallel connections, wherein CCF is a major characteristic [24]. FTA has been so far employed in several BOP reliability analyses (see, e.g., references [25–28]), proving to be convenient for identifying failure modes within the BOP stack. Fowler and Roche [29] used both FTA and FMEA for reliability analysis of the device and its hydraulic control system. They employed the inductive bottom-up approach to determine consequences of part malfunction and to link undesired events to their causes, the deductive supplement. FMEA was again extended to include criticality and applied to the entire system in a study conducted by American Bureau of Shipping (ABS) and ABSG Consulting Inc. for the Bureau of Safety and Environmental Enforcement (BSEE) [30]. A BOP reliability analysis model was recently developed by employing the software package Norsys Netica (https://www.norsys.com/netica.html) to aid in identification, evaluation, and prioritization of failure risks [31].

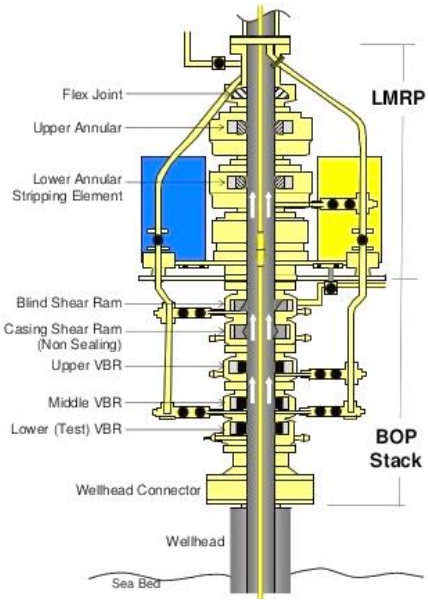

Figure 2. Typical BOP stack and components.

For complex systems such as BOP in which interdependencies between sub-components are complicated, combined (hybrid) techniques are worthwhile. Identifying critical components in a system with over seven (7) main subsystems, housing about 600 individual components may be the starting point for more detailed qualitative and quantitative analyses. The proposed integration methodology is explained step by step as follows:

1. Reliability goal and system boundary definition

- Identification of critical components within the system: As a large specialized and mechanical valve assembly that is used to seal wells against kicks or blowouts during drilling or work-over operations, a critical component will be the one whose failure will lead to the failure of the entire system or a major part of it.
- Setting overall reliability requirements for the system: Safety Integrity Level (SIL) requirements are widely accepted for the basis of operation and design of Safety Instrumented Systems. For BOP systems, the IEC 61508 requirements for the safety integrated functions are applied [32].
- Defining system specifications: The BOP system considered in this study is a type of class VI configuration with 4 rams and dual annular. Main subsystems (from the upper annular

preventer to the wellhead connector) make up components under investigation, ignoring surface controls, panels and accumulators as shown in Figure 2.

2. System Breakdown Physical and functional categorization of components is achieved as part of the requirements for FTA and FMEA. Major components of the BOP as identified in the literature include: control system (pods, accumulators, auto-shear system), ram preventers (pipe, blind-shear and/or casing-shear preventers), annular preventers (lower and upper), connectors (wellhead and Lower Marine Riser Package (LMRP)) and kill/choke system (valves and lines).
3. FTA Steps The undesired top event for a BOP is a blowout once a kick cannot be killed. This forms the apex, upon which the fault tree is built and shown in Figure 3, alongside the immediate top-level basic events. Analyses at this stage were aided by a professional software called FaultTree+^{TM} [33], requiring overall structural and functional knowledge about the system. All cut sets were determined and the weights were calculated by Equations (4) and (5). The minimal cut sets and gate summary of the BOP's fault tree are extensive and not thoroughly presented here. Table 3 gives the results obtained for some components and presents the cut sets with associated rankings calculated from Table 1, to demonstrate applicability.
4. FMEA Steps An FMEA standard procedure is followed at this stage. In this case, however, a detailed FMEA study is conducted on BOP system using the severity, occurrence and detectability ratings reported in reference [34]. The methodology used ten-point scales for severity rating (see Table 4), occurrence rating (see Table 5), and detectability rating (see Table 6) to represent the risk priorities of the BOP failures.

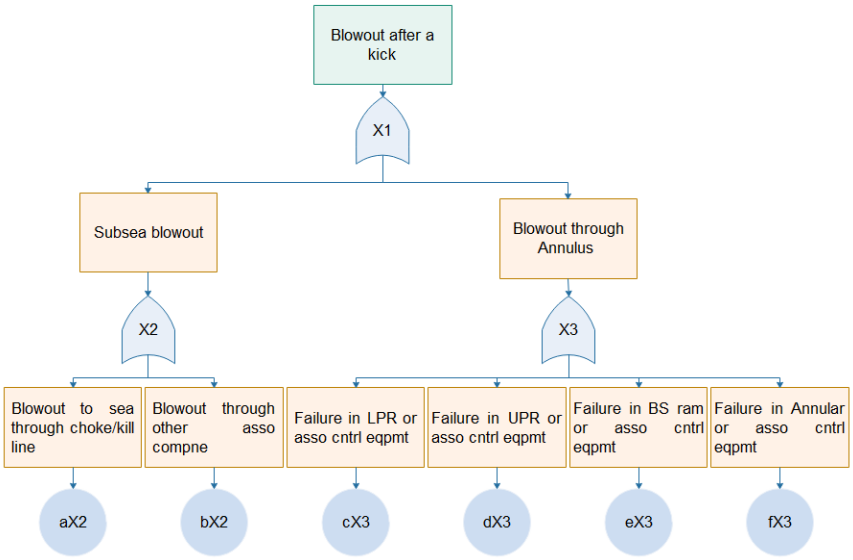

Figure 3. Top level of fault tree.

Table 3. Weights and rankings of some BOP components.

Minimal Cut Set	Associated Component(s)	Importance Weight	Ranking
B0	Wellhead connector	1	10
D001; D002	Pod 1 (blue pod)	0.106	8
	Pod 2 (yellow pod)	0.106	8
B00000; B0000; B00	Lower pipe ram	0.00001	2
	Upper pipe ram	0.000053	2
	Blinds shear ram	0.233	8

Table 4. Severity ratings of a failure for BOP.

Severity Rating	Significance	Personnel	Environment	Downtime
1	Does not affect BOP functionality; no impact on safety and environment	No impact	No impact	No downtime, repair can be done while drilling continues.
2	Does not affect BOP functionality but needs to be corrected; no impact on safety and environment.	No impact	No impact	No downtime, repair can be done at next opportunity, drilling continues.
3	Partial loss of BOP function; no loss of well control	No impact	No impact	Downtime of less than a shift, stop drilling, intervene and repair.
4	Partial loss of BOP function; no loss of well control.	No impact	No impact	Downtime between a shift and 24 h, stop drilling, intervene and repair.
5	Partial loss of BOP primary function if not corrected immediately.	No impact	No impact	Downtime between 1 and 7 days—stop drilling, intervene and repair (surface only).
6	Partial loss of BOP primary function if not corrected immediately.	Minor injury no recordable lost time	Minor external subsea leak (e.g., choke & kill (C&K0 Connector leak)	Downtime between 8 and 21 days—stop drilling, intervene and repair (surface only).
7	Loss of BOP primary function.	Minor Injury; some lost time	Significant external subsea leak (e.g., major connector leak)	Pulling LMRP only
8	Loss of BOP primary function.	Serious Injury; significant lost time.	<1000 barrels	Pulling LMRP/BOP stack
9	Loss of BOP primary function.	Single Fatality; multiple serious injuries	>1000 barrels	Shut down of operations; drilling stopped and major regulatory implications; changes to drilling schedule >3 months.
10	Loss of BOP primary function.	Multiple fatalities and injuries	>10,000 barrels and severe environmental damage over a large area.	Shut down of operations; drilling stopped and major regulatory implications; total loss of asset.

Table 5. Occurrence ratings of a failure for BOP.

Occurrence Rating	Frequency/Rig Year	Occurrence
1	<1 event every 100 rig years	Less than 1% chance every 10 years of operation
2	<1 event every 10 rig years to 1 event every 100 rig years	Less than once every 10 years to 10% chance every 10 years of operation
3	<1 event every 5 rig years to 1 event every 10 rig years	Less than once every 5 years to once every 10 years
4	<1 event every 2 rig years to 1 event every 5 rig years	Less than once every 2 years to once every 5 years
5	<1 event/rig yr. to 1 event every 2 rig years	Less than once a year to once every 2 years
6	<2 events/rig yr. to 1 event/yr.	Less than twice a year to once a year
7	<4 events/rig yr. to 2 events /yr.	Less than once a quarter to twice a year
8	<10 events/rig yr. to 4 events /rig yr.	Less than once a month to once a quarter
9	<50 events/rig yr. to 10 events /rig yr.	Less than once a week to once a month
10	>50+ events/rig yr.	Once a week or more often

Table 6. Detectability ratings of a failure for BOP.

Detection Rating	Detection	Likelihood of Detection
1	Almost certain	Very high probability of detection (>90% probability of detection) by design controls (redundant or independent self-diagnostic capability, independent alarms) will certainly detect failures
2	Very high	High probability of detection (50 to 90% of detection) by design controls (single device self-diagnostic capability, single alarms, visual monitoring, leak monitoring, loss of fluid etc.) will certainly detect failures
3	High	Probability of detection via weekly on-stream tests/inspections will provide immediate detection of the failure
4	Moderately high	Probability of detection via monthly on-stream tests/inspections will provide immediate detection of the failure
5	Moderate	Probability of detection via quarterly on-stream tests/inspections will provide immediate detection of the failure
6	Low	Can only be detected during routine inspections/tests while the BOP is pulled from the well
7–8	Very low	Can only be detected during major PMs while the BOP is pulled from the well
9	Remote	Can only be detected and/or corrected during major overhaul or rebuilding-type activities
10	Absolute uncertainty	Currently no design controls or maintenance techniques in place

Weighted RPNs are then calculated by multiplying the traditional RPN values with the weight factor, resulting in weighted RPN values to become between 1 and 10,000. Comparatively, components requiring greater corrective action and implicitly considered to be critical based on the traditional FMEA approach differ from those obtained by the proposed FTA-FMEA technique. Table 7 demonstrates this for a cross section of components and reveals that control pods may require more attention after blind shear rams as opposed to pipe rams in the traditional FMEA ranking system.

Table 7. A comparison between the results obtained from the traditional FMEA technique with those obtained by the proposed method.

Component	RPN from Traditional FMEA	Weighted RPN from FTA-FMEA Approach
Wellhead connector	40	400
Blue Pod	35	280
Yellow pod	35	280
Lower pipe ram	70	140
Upper pipe ram	76	152
Blind shear ram	80	640

Figure 4 provides a clear comparison between the traditional RPN values and the weighted RPN values.

Though some components such as the kill valves still remain at top priority in RPN rankings with the proposed technique, a clear disparity in rankings and hence in the criticality of components is depicted in others such as the connectors (wellhead and LMRP). Choke valves are ranked at the same level with casing shear rams and are higher than blind shear rams and accumulators.

Comprehensive analyses of the system produce results that may significantly alter corrective measures and criticality priorities for the BOP and any complex system in general. Whilst FMEA focuses on causal effects, taking into consideration all possible failures but not necessarily component interdependencies, FTA considers the latter but avoids minute components and their effects on overall system failure. The integration of the techniques is proven to produce more robust prioritization of system risks as greater failure severity may not necessarily mean greater criticality. This phenomenon becomes explicit when weighted RPNs for BOP under two different operating conditions, namely deep-water and shallow-water, are compared. Six experts are consulted to provide their opinion on the severity, occurrence and detectability of various failure modes, and a Multi-Criteria Decision Analysis (MCDA) method based on Weighted Sum Model (WSM) is used to aggregate the experts' opinions (see Tables 8–10). Though FMEA requires the experts to brainstorm on every aspect of FMEA process, ambiguity is avoided by disseminating similar FMEA worksheets to experts, containing the specific components/subsystems as previously established and their single associated undesired failure mode. Judgement is elicited mainly on the severity, occurrence and detectability ratings of failure modes.

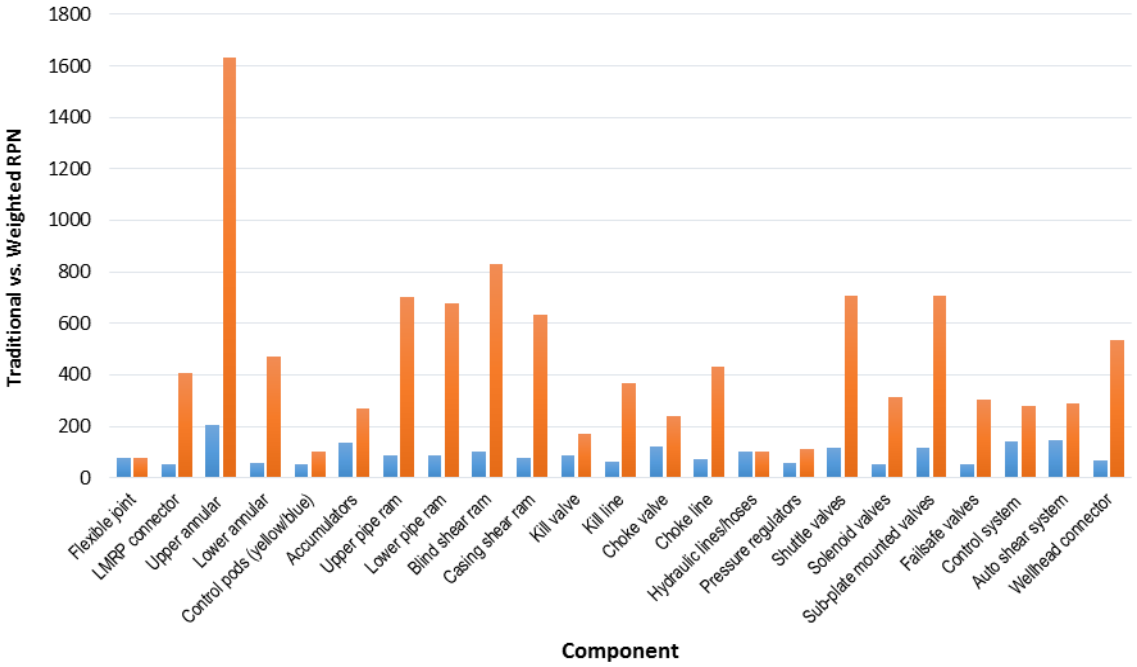

Figure 4. RPN values obtained from the traditional FMEA technique (■) versus weighted RPN values obtained by the propose method (■).

Table 8. Weighting criteria for the group of experts.

Constitution	Classification	Score
Occupation	Field expert (Engineer)	4
	Senior academia	3
	Junior academia	2
	Technician	1
Experience	Above 30 years	4
	20–29	3
	10–19	2
	0–9	1
Education	PhD	4
	MSc	3
	BSc	2
	HND	1

Table 9. Expert weighting.

Expert	Occupation	Experience	Education	Weight Factor	Weight Score
1	Engineer = 4	[0–9] = 1	PhD = 4	4 + 1 + 4 = 9	0.16
2	Engineer = 4	[10–19] = 2	PhD = 4	4 + 2 + 4 = 10	0.18
3	Engineer = 4	[10–19] = 2	PhD = 4	4 + 2 + 4 = 10	0.18
4	Junior academia = 2	[10–19] = 2	MSc = 3	2 + 2 + 3 = 7	0.13
5	Senior academia = 3	[20–29] = 3	PhD = 4	3 + 3 + 4 = 10	0.18
6	Senior academia = 3	[20–29] = 3	PhD = 4	3 + 3 + 4 = 10	0.18
				Total = 56	**Total = 1**

Table 10. Final aggregation for RPNs (example of the blind shear ram component).

Expert	RPN	Weight Score	Weighting
1	60	0.16	$60 \times 0.16 = 9.6$
2	70	0.18	$70 \times 0.18 = 12.6$
3	192	0.18	$192 \times 0.18 = 34.56$
4	96	0.13	$96 \times 0.13 = 12.48$
5	84	0.18	$84 \times 0.18 = 15.12$
6	70	0.18	$70 \times 0.18 = 12.6$
			Total = 96.96 ≈ 97

As expected, RPN values for all BOP components in deep waters are larger than those in shallow waters, however, significant differences exist between ranking priorities in deep and shallow waters, as shown in Figure 5. The robustness of the technique is proven as components such as the wellhead connector and casing shear ram gain significant priority leaps in deep water, in compliance with research and regulatory standards.

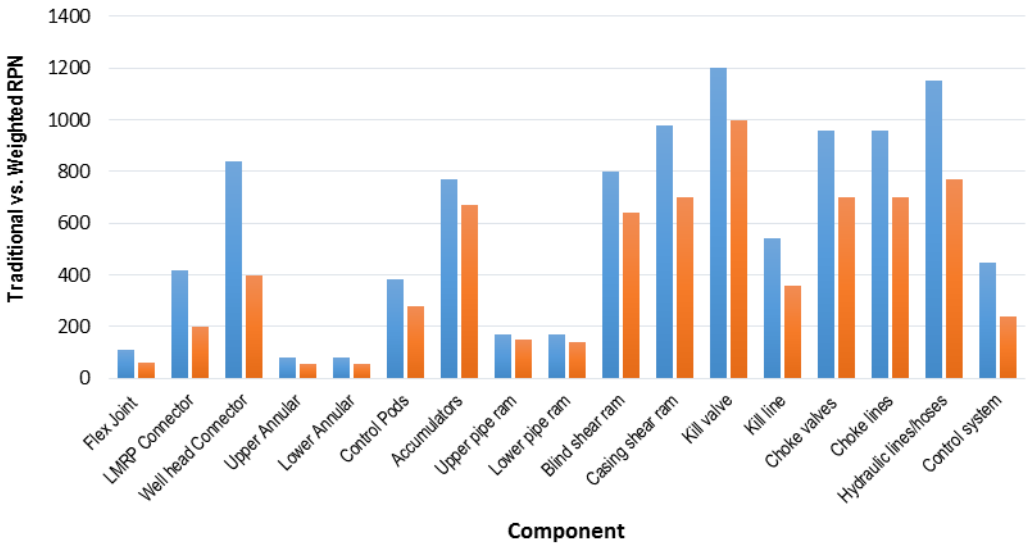

Figure 5. Weighted RPN values for shallow-water (■) and deep-water (■) cases.

5. Conclusions

This paper presented an integrated methodology of fault tree analysis (FTA) and failure mode and effects analysis (FMEA) in a manner that provides a modified, systematic and structured approach for identifying, evaluating and prioritizing the risks associated with different components in a complex system. The synergy of complementary techniques is harnessed by modifying criteria, hence increasing efficiency in analysis. By using the proposed technique, it is possible to gain insights about any complex system which otherwise might be overlooked. The basis for corrective action is improved in

a computationally sound manner. The application of the proposed methodology was demonstrated with a critical subsea oil and gas system known as Blowout Preventer (BOP).

The results of the study proved the benefits of the proposed FTA-FMEA methodology and combinatorial risk analysis techniques in general. Components that may be overlooked based on the traditional FMEA technique were brought to the limelight for consideration. More so, the priority rankings were improved significantly. Minute changes in ranking order may have huge implications, particularly for a safety-critical system such as BOP. Aside being essential for further quantitative research, component priority can significantly alter maintenance and testing policies. As shown in Table 7 and Figure 4, some components such as the kill valves remained at top priority in RPN rankings with the proposed technique. However, a clear disparity in rankings was observed for some components such as the connectors (wellhead and LMRP). Choke valves were ranked at the same level with casing shear rams and were higher than blind shear rams and accumulators.

Future research can be directed towards the effects of double and multiple failures, the comparative difference obtained when different importance measures are used, and linking the software interphases of the proposed integration scheme. Also, the normed design of subsea accumulators for actuation and control of BOPs may sometimes not be safe (see reference [35]). Thus, consideration of the actuation of the BOP and its design in reliability analysis can be an interesting subject for research.

Author Contributions: E.E. performed the analysis and wrote the initial manuscript draft. M.S. reviewed the initial manuscript, made contributions to its structure and responded the reviewers' comments. Both M.S. and A.K. supervised the work.

Funding: This work was supported by Commonwealth Scholarship Commission.

Conflicts of Interest: The authors declare no conflict of interest. This research received no external funding.

Acronyms

D	detectability of a failure
h(1i, p(i))	probability that the system fails when component i fails
h(0i, p(i))	probability that the system fails when component i is working
O	occurrence of a failure
RPN	risk-priority-number
S	severity of a failure
w_{i}	importance of ith component in the system
WRPN	weighted RPN
X_i	importance of the ith minimal cut set in the fault tree structure

References

1. Kolowrocki, K. *Reliability of Large and Complex Systems*, 2nd ed.; Elsevier: London, UK, 2014.
2. Moubray, J. *Reliability-Centered Maintenance*, 2nd ed.; Butterworth-Heinemann: Oxford, UK, 1999.
3. Chen, S.; Qi, Z.; Chen, D.; Guo, L.; Peng, W. Investigation of Bayesian network for reliability analysis and fault diagnosis of complex systems with real case applications. *Adv. Mech. Eng.* **2017**, *9*, 1–12. [CrossRef]
4. Shafiee, M.; Animah, I.; Alkali, B.; Baglee, D. Decision support methods and applications in the upstream oil and gas sector. *J. Pet. Sci. Eng.* **2019**, *173*, 1173–1186. [CrossRef]
5. Liu, C.-T.; Hwang, S.-L.; Lin, I.-K. Safety analysis of combined FMEA and FTA with computer software assistance—take Photovoltaic plant for example. *IFAC Proc. Vol.* **2013**, *46*, 2151–2155. [CrossRef]
6. Hong, Z.; Binbin, L. Integrated analysis of software FMEA and FTA. In Proceedings of the International Conference on Information Technology and Computer Science, Kiev, Ukraine, 25–26 July 2009.
7. Lutz, R.R.; Woodhouse, R.M. Bi-directional analysis for certification of safety-critical software. In Proceedings of the International Software Assurance Certification Conference (ISACC), Chantilly, VA, USA, 28 February–2 March 1999; pp. 1–9.
8. Xiao, N.; Huang, H.-Z.; Li, Y.; He, L.; Jin, T. Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. *Eng. Fail. Anal.* **2011**, *18*, 1162–1170. [CrossRef]

9. Han, X.; Zhang, J. A combined analysis method of FMEA and FTA for improving the safety analysis quality of safety-critical software. In Proceedings of the IEEE International Conference on Granular Computing, Beijing, China, 13–15 December 2013.
10. Sinnamon, R.M.; Andrews, J.D. Improving efficiency in qualitative fault tree. *Qual. Reliab. Eng. Int.* **1997**, *13*, 293–298. [CrossRef]
11. Shafiee, M.; Dinmohammadi, F. An FMEA-based risk assessment approach for wind turbine systems: A comparative study of onshore and offshore. *Energies* **2014**, *7*, 619–642. [CrossRef]
12. Dinmohammadi, F.; Shafiee, M. A fuzzy-FMEA risk assessment approach for offshore wind turbines. *Int. J. Progn. Health Manag.* **2013**, *4*, 59–68.
13. Franceschini, F.; Galetto, M. A new approach for evaluation of risk priorities of failure modes in FMEA. *Int. J. Prod. Res.* **2001**, *39*, 2991–3002. [CrossRef]
14. Chang, D.-S.; Sun, K.-L.P. Applying DEA to enhance assessment capability of FMEA. *Int. J. Qual. Reliab. Manag.* **2009**, *26*, 629–643. [CrossRef]
15. Vahdani, B.; Salimi, M.; Charkhchian, M. A new FMEA method by integrating fuzzy belief structure and TOPSIS to improve risk evaluation process. *Int. J. Adv. Manuf. Technol.* **2015**, *77*, 357–367. [CrossRef]
16. Liu, H.-C.; Liu, L.; Liu, N. Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert Syst. Appl.* **2013**, *40*, 828–838. [CrossRef]
17. Gilchrist, W. Modelling failure modes and effect analysis. *Int. J. Qual. Reliab. Manag.* **1993**, *10*, 16–23. [CrossRef]
18. Whiteley, M.; Dunnett, S.; Jackson, L. Failure Mode and Effect Analysis, and Fault Tree Analysis of Polymer Electrolyte Membrane Fuel Cells. *Int. J. Hydrog. Energy* **2016**, *41*, 1187–1202. [CrossRef]
19. Khaiyum, S.; Kumaraswamy, Y. An effective method for the identification of potential failure modes of a system by integrating FTA and FMEA. *Adv. Intell. Systs. Comput.* **2014**, *248*, 679–686.
20. Bluvband, Z.; Polak, R.; Grabov, P. Bouncing failure analysis (BFA): The unified FTA-FMEA methodology. In Proceedings of the Annual Reliability and Maintainability Symposium, Alexandria, VA, USA, 24–27 January 2005; pp. 463–466.
21. Zhai, G.; Zhou, Y.; Ye, X.; Hu, B. A method of multi-objective reliability tolerance design for electronic circuits. *Chin. J. Aeronaut.* **2013**, *26*, 161–170. [CrossRef]
22. Meng, F.C. Relationships of Fussell–Vesely and Birnbaum importance to structural importance in coherent systems. *Reliab. Eng. Syst. Saf.* **2000**, *67*, 55–60. [CrossRef]
23. Pickard, K.; Müller, P.; Bertsche, B. Multiple failure mode and effects analysis—An approach to risk assessment of multiple failures with FMEA. In Proceedings of the Annual Reliability and Maintainability Symposium, Alexandria, VA, USA, 24–27 January 2005; pp. 457–462.
24. Cai, B.; Liu, Y.; Liu, Z.; Tian, X.; Zhang, Y.; Liu, J. Performance evaluation of subsea blowout preventer systems with common-cause failures. *J. Pet. Sci. Eng.* **2012**, *90–91*, 18–25. [CrossRef]
25. Holand, P.; Rausand, M. Reliability of subsea BOP systems. *Reliab. Eng.* **1987**, *19*, 263–275. [CrossRef]
26. Holand, P.; Awan, H. Reliability of Deepwater Subsea BOP Systems and Well. Report No. ES 201252/02. 2012. Available online: www.bsee.gov (accessed on 18 August 2018).
27. Enjema, E.; Shafiee, M.; Kolios, A. A study on the reliability of oil and gas Blowout Preventer (BOP) technologies under deep-water erratic conditions. In *Safety and Reliability—Theory and Applications*; CRC Press, Taylor & Francis Group: Portoroz, Slovenia, 2017; p. 346.
28. Enjema, E. Reliability Performance Analysis of Complex Teachnical Systems under Extreme Loading Conditions with Application to Subsea Blowout Preventer. Ph.D. Thesis, Cranfield University, Cranfield, UK, 2018.
29. Fowler, J.H.; Roche, J.R. System safety analysis of well-control equipment. *SPE Drill. Completion* **1994**, *9*, 193–198. [CrossRef]
30. Bureau of Safety and Environmental Enforcement (BSEE). Blowout Preventer (BOP) Failure Mode Effect Criticality Analysis (FMECA), 2013. Available online: www.bsee.gov (accessed on 18 August 2018).
31. Enjema, E.; Shafiee, M.; Kolios, A. An integrated framework for Blowout preventer configuration selection in deep and ultra-deep water offshore fields. In *Safety and Reliability—Safe Societies in a Changing World*; CRC Press, Taylor & Francis Group: Trondheim, Norway, 2018; pp. 2007–2012.

32. International Electrotechnical Commission. IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. 2010. Available online: https://www.iec.ch/functionalsafety/standards/page2.htm (accessed on 18 August 2018).
33. Isograph's Fault Tree Analysis Software. FaultTree+. Available online: https://www.isograph.com/software/reliability-workbench/fault-tree-analysis-software/?gclid=EAIaIQobChMIuJfmq6jt4AIVSCtBh04xAGvEAAYASAAEgLWy_D_BwE (accessed on 18 August 2018).
34. Pinker, R. Improved Method for Reliability Assessment of Safety-Critical Systems: An Application Example of BOP Systems. Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2012.
35. Cipollone, R.; Fatigati, F.; Di Battista, D.; Allara, P.; Carini, N. On the rapid discharge of subsea accumulators: Remarks on the normed design method and proposal of improvement. *Energy Sci. Eng.* **2018**, *6*, 239–252. [CrossRef]