Lukman Irshad
School of Mechanical,
Industrial and Manufacturing Engineering,
Oregon State University,
Corvallis, OR 97331
e-mail: mohammoh@oregonstate.edu

Daniel Hulse
School of Mechanical,
Industrial and Manufacturing Engineering,
Oregon State University,
Corvallis, OR 97331
e-mail: hulsed@oregonstate.edu

H. Onan Demirel[1]
School of Mechanical,
Industrial and Manufacturing Engineering,
Oregon State University,
Corvallis, OR 97331
e-mail: onan.demirel@oregonstate.edu

Irem Y. Tumer
School of Mechanical,
Industrial and Manufacturing Engineering,
Oregon State University,
Corvallis, OR 97331
e-mail: irem.tumer@oregonstate.edu

David C. Jensen
Department of Mechanical Engineering,
University of Arkansas,
Fayetteville, AR 72701
e-mail: dcjensen@uark.edu

Quantifying the Combined Effects of Human Errors and Component Failures

While a majority of accidents and malfunctions in complex engineered systems are attributed to human error, a closer inspection would reveal that such mishaps often emerge as a result of complex interactions between the human- and component-related vulnerabilities. To fully understand and mitigate potential risks, the effects of such interactions between component failures and human errors (in addition to their independent effects) need to be considered early. Specifically, to facilitate risk-based design, severity of such failures need to be quantified early in the design process to determine overall risk and prioritize the most important hazards. However, existing risk assessment methods either quantify the risk of component failures or human errors in isolation or are only applicable during later design stages. This work intends to overcome this limitation by introducing an expected cost model to the Human Error and Functional Failure Reasoning (HEFFR) framework to facilitate the quantification of the effects of human error and component failures acting in tandem. This approach will allow designers to assess the risk of hazards emerging from human- and component-related failures occurring in combination and identify worst-case fault scenarios. A coolant tank case study is used to demonstrate this approach. The results show that the proposed approach can help designers quantify the effects of human error and component failures acting alone and in tandem, identify worst-case scenarios, and improve human-product interactions. However, the underlying likelihood and cost models are subject to uncertainties which may affect the assessments.
[DOI: 10.1115/1.4050402]

Keywords: design theory and methodology, risk-based design, human-in-the-loop-design, risk assessment, human reliability assessment, systems design

1 Introduction

While the rate of component failure related incidents has decreased significantly in the past few decades [1], the rate of human error-related incidents has not decreased at the same pace [1]. Consequently, a majority of accidents and performance losses in complex engineered systems are attributed to human errors [2]. For instance, around 80% of accidents in high-hazard industries, such as offshore drilling and aviation, are attributed to human errors [3,4]. However, a closer look would reveal that component malfunctions and poor design often act in tandem with human fallibilities to produce the resulting mishaps [5]. Hence, to prevent potential hazards, it is vital to understand how the interactions between component- and human-related fallibilities affect the system in addition to how they affect the system independently. Furthermore, it is important to mitigate these hazards early in the design process—before costly design commitments are made—to prevent costly late-stage design changes and rework [6]. One way to approach this problem is to quantify the risk of the independent and interaction effects of component failures and human errors early in the design stages to identify potential hazardous fault scenarios and prioritize them so that appropriate mitigation strategies can be built into the design early on.

Traditionally, engineers have used Probabilistic Risk Assessment (PRA) to assess potential risk by quantifying the probability and severity of failures [7]. The risk of component failures and human errors is assessed separately using component failure assessment techniques and human reliability assessment methods later in the design stages [7]. Methods such as Fault Tree Analysis (FTA) [8], Event Tree Analysis (ETA) [9], and Failure Modes and Effects Analysis (FMEA) [10] are used to quantify the risk and severity of component failures. Human reliability assessment techniques such as Systematic Human Error Reduction and Prediction Approach (SHERPA) [11] and Technique for Human Error Rate Prediction (THERP) [12] are used to quantify the risk and severity of human errors. While these approaches can be used to identify hazardous scenarios involving component failures or human errors independently, they are not capable of identifying the combined effects of human errors and component failures because none of these methods allow the detailed assessment of component failures and human errors in combination. Also, these are not optimal to be used at the early design stages since they require detailed system/component models. Similarly, early design stage quantitative risk assessment methods such as COBRA (Conceptual Object-Based Risk Analysis) [13], Risk in Early Design (RED) Method [14], and Conceptual Stress and Conceptual Strength Interference Theory (CSCSIT) [15] only assess the risk of component failures, giving minimal insight relating to human errors. In summary, existing risk assessment methods are limited because they either assess human error and component faults in isolation or are only applicable during the later design stages.

Recent research has introduced the Human Error and Functional Failure Reasoning (HEFFR) Framework to assess the effects of human errors and component failures in combination in the early

[1]Corresponding author.

This paper is based on a paper presented at the 2020 ASME International Design Engineering Technical Conferences.

Contributed by the Design Automation Committee of ASME for publication in the Journal of Mechanical Design. Manuscript received October 27, 2020; final manuscript received February 24, 2021; published online May 3, 2021. Assoc. Editor: Michel-Alexandre Cardin.

design phase [16,17]. The framework takes inputs from an automated scenario generation technique that generates fault scenarios using all possible combinations of human-induced and non-human-induced component behaviors to identify the resulting functional failures, human errors, and their propagation paths [18]. This approach enables designers to generate a large number of potential fault scenarios that result in critical functions failing. However, as of yet, the HEFFR framework does not quantify the risk of resulting failures, limiting the designers' ability to identify and mitigate high-risk scenarios.

In this paper, we address this limitation by developing a cost and probability model to quantify the relative impact (and thus priority) of critical event scenarios [19]. To calculate the likelihood of occurrence of critical events, we consider both component failure and human error probabilities, using traditional reliability engineering principles to estimate component failure probabilities and the Human Error Assessment and Reduction Technique (HEART) [20] to estimate human error probabilities. To quantify the relative importance and priority of failures, we adapt the expected cost of resilience metric developed in Ref. [21], which defines expected cost as the multiplication of the modeled probability and cost of the scenario. We then demonstrate and study the use of these metrics in HEFFR using a liquid coolant tank case study. The goal of using these metrics in HEFFR is to identify highest priority scenarios that include component failures, human errors, or combinations of both and enable the use of failure costs in design trade studies to motivate design. One could then use this assessment to identify critical points of human intervention and use this information to motivate design of the physical system (e.g., components), electronic system (e.g., control logic and interfaces), and human system (e.g., best practices and training materials). However, models of risk in these systems have implications to how best to account for risks in the design process and may additionally be subject to model and parameter uncertainties. Thus, the results of this demonstration are additionally used to understand the benefits and limitations of using risk metrics in human-component fault modeling.

2 Background

This section provides a background about the methods used in this paper. First, we discuss the HEFFR framework and the automated scenario generation technique. Then, we explore the methods used to quantify the probability of failure and human error to build the foundation for the likelihood of occurrence calculation. Finally, we explain the theoretical basis for using expected cost in risk quantification.

2.1 Human Error and Functional Failure Reasoning. The HEFFR [16,17] framework was developed to assess the system-level effects of component failures and human errors acting in combination during the early design stages. As shown in Fig. 1, the HEFFR framework extends the Functional Failure Identification and Propagation (FFIP) [22] framework (highlighted by a dotted box in Fig. 1) by introducing the modules Action Sequence Graphs (ASG), action classifications, and action simulation to represent the human aspects of the failure assessment. FFIP uses a functional model, which is created by decomposing the system using the functional basis for engineering design [23] method and a configuration flow graph to represent the generic components fulfilling each function. HEFFR uses ASGs to represent human-product interactions through a graph that captures the human actions that need to be performed to interact with each component that require human interactions in the order that they are executed.

The HEFFR framework uses component behavior models and action classifications to simulate faults. The component behavior model defines all possible behavior modes of each component in the configuration flow graph. The action classifications describe all possible nominal and faulty states of each human action in the ASGs. The framework takes fault scenarios as inputs to produce

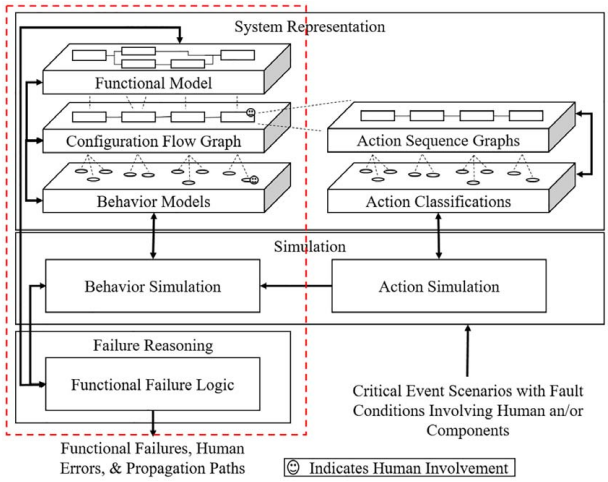

Fig. 1 The architecture of human error and functional failure reasoning framework [18]

functional failures, human errors, and their propagation paths as outputs. Based on the input scenario, the action simulation determines the state (nominal or faulty) of each action in the ASGs, which are then used to identify the human-induced behavior of components with human interaction. The behavior simulation tracks the behaviors (human-induced and non-human-induced) of components using the configuration flow graph. Finally, the functional failure logic determines the functional health using the functional model and the behaviors modeled in the behavior simulation. The simulation is time-based, where each time-step is a discrete system state. More details on how to model a system and simulate faults using HEFFR can be found in Ref. [16].

As a follow up to HEFFR, an automated scenario generation technique [18] was developed to generate a majority of the potential fault scenarios so that designers do not need to identify scenarios manually. The technique uses a modified depth-first search to traverse through all possible combinations of human-induced and non-human-induced component behaviors to generate scenarios that can result in systems' critical functions failing. The algorithm also generates all possible human action state combinations that can result in human-induced behaviors to identify the system-level impact of human interactions. In the tree search, each branch is a scenario, and each level in a branch is viewed as a time-step. A user-defined number limits the maximum number of time-steps (or levels in a branch). When a new event is introduced in a time-step, no more events are introduced for a user-defined number of time-steps to assess the cascading effects of failures. The events in each time-step are considered to be independent unless they are allowed to propagate. The algorithm performs a HEFFR assessment at each time-step to determine if the critical functions have failed. When the critical functions have failed, the results are recorded, and the next scenario is generated. Scenarios are generated until all possible combinations of behavior modes are executed at each time-step. More details on the automated scenario generation are available in Ref. [18].

HEFFR simulations outputs the input scenarios (HEFFR input at each time-step for each scenario), resulting functional health (at each time-step for each scenario) of the system, and all possible human action classification combinations that result in human-induced component behaviors. Since the search of component behavior mode combinations is exhaustive, it can generate a large number of scenarios. The authors encourage designers to use data mining techniques to create risk metrics that are tailored to their needs. While this approach enables designers to mine important information such as the shortest event sequence to failure, the likelihood of a particular behavior mode being present during a failure, and the possibility of specific faulty human

actions being present in human-induced behaviors, such metrics do not quantify risk in terms of likelihood and severity. Without risk quantification, designers will not be able to prioritize fault scenarios to implement design solutions. This paper aims to overcome this limitation by introducing a probability and cost model for HEFFR analysis to quantify the risks of human- and component-induced failures.

2.2 Probability of Failure in Risk Assessment. Traditionally, engineers have relied on probabilistic risk assessment methods to quantify the risk of failure [7]. Probabilistic risk assessment is the quantification of the risks due to hazards in terms of severity (how bad the hazard is) and occurrence (how likely it is to occur) [24]. FTA and ETA are traditionally used to assess the risk of component failures during probabilistic risk assessment [25]. FTA [8] builds a tree of set relationships of events that must be satisfied for a hazardous top-event to occur. ETA [9], on the other hand, is used to assess all success and failure outcomes of a specific initiating failure event. Both methods rely on principles from reliability engineering to calculate the probability of failure [7]. When a constant failure rate is assumed, an exponential probability distribution can be used as in Eq. (1) to calculate the probability of failure (P_f) of a component [26] where λ is the failure rate and t is the operation time

$$P_f = 1 - e^{-\lambda t} \tag{1}$$

Human reliability assessment methods are used to quantify the human error probability in probabilistic risk assessment [7]. One common human reliability assessment method, THERP [12], uses event trees to model human errors and quantify them, giving minimal consideration for performance shaping factors. The Standard Plant Analysis Risk (SPAR-H) [27] method classifies tasks as action, diagnosis, or mixed based on them being physical, cognitive, or both, respectively. SPAR-H calculates human error probability using the task type, system operation status, task dependencies, and performance shaping factors. HEART [20] uses generic human error probabilities and performance shaping factors (called Error Producing Conditions (EPC)) to calculate human error probability. The generic human error probabilities and EPC factors in HEART have been adapted and tailored to several industries including aviation [28], nuclear power [29], railway [30], and maritime [31].

This research uses HEART and SPAR-H to calculate human error probability because these methods are easy to use, integrate well with the HEFFR framework, apply to a variety of industries, and have the most potential to predict human error probability with the minimal information available in early design. The probability of the component behavior modes is calculated using the exponential probability distribution described above, following processes previously outlined for early design reliability prediction [32].

2.3 Cost in Risk Assessment. In probabilistic risk assessment, it is necessary to assess the severity of failures so that risks can be prioritized and managed in proportion to their impact. Typically, FTA and ETA do not assess this severity of consequence(s), leaving the assessment up to the judgment of the designer. Severity is, however, assessed in detail in FMEA to prioritize faults and give details of the failure mechanisms and consequences [25]. In FMEA, each of these (as well as rate of detection) is rated on a 0–10 scale and multiplied into a risk priority number ($RPN = Severity * Occurrence * Detection$). However this approach has a number of limitations [33,34]:

(1) the ordinal scale for probabilities and severities distorts the relative impact of each since fault probabilities and costs often vary over orders of magnitude,
(2) RPNs calculated by different project groups on different systems may not correspond to the relative risks of their subsystems because each number is subjective, and
(3) there is no formal method to trade RPN for other desirable design attributes (e.g. to prescribe a risk-mitigating feature).

As a means of overcoming these limitations, expected cost has been presented as an alternative framework to design for risk [33–35]. When quantifying risk as an expected cost, the occurrence is quantified using the estimated number of times a failure scenario is to occur while the severity is quantified in terms of the cost incurred if that scenario occurs, according to:

$$C = \mathop{\mathbb{E}}_{s \in S} \{C(s)\} \approx \sum_{s \in S} n(s) * C(s) \tag{2}$$

where S is the set of fault scenarios, $n(s)$ is the lifetime number of occurrences for a scenario, and $C(s)$ is the modeled cost of a fault scenario. Expected cost can be used both for risk and resilience quantification for design optimization [36–38]. To integrate expected cost quantification with fault modeling tools, Ref. [39] considers three main costs: cost of failure, cost of repair, and cost of partial recovery [21]. Costs can also be added for risk using existing safety cost schedules (e.g., Ref. [40]), provided one is at liberty to do so. This work adapts this quantification of expected cost to the HEFFR framework to enable designers to prioritize and make sense of hazards given by a large set of fault scenarios.

3 Methodology

The objective of this research is to aid designers identify and prioritize high severity fault scenarios that result from the interactions between component failures and human errors (in addition to the scenarios that result from them acting independently) during the conceptual design stage. We use two metrics—the likelihood of failure and expected cost—to achieve this goal. This is done by processing the output of HEFFR to calculate the above metrics using cost and probability models. The following definitions will be used for the terms event and scenario for the rest of this paper:

- Event: the behavior state of components and the human action classification states in a time-step
- Scenario: a collection of events

A sample output for a HEFFR assessment of one scenario is presented in Tables 1 and 2. Table 1 shows the critical event input at each time-step and the resulting health of functions. Table 2 shows the human action classification combinations and the resulting human-induced behaviors of a component.

Table 1 HEFFR sample result: fault scenario input and resulting functional failures

	Critical event scenario (HEFFR input)			Functional failure (HEFFR output)		
t	Generic component (GC) 1	GC2	GC3	Function (F) 1	F2	F3
0	Nominal Behavior Mode (NBM) 1	NBM1	NBM1	Nominal (N)	N	N
1	Faulty Behavior Mode (FBM) 1	FBM1	NBM2	Degraded (D)	D	N
2	Human Induced Nominal Behavior (HINB) 1	FBM1	NBM2	N	D	N
3	Human Induced Faulty Behavior (HIFB) 1	FBM2	FBM2	Failed/Lost (L)	D	L

Table 2 HEFFR sample result: human action classification combinations and resulting human induced behaviors of component 1

Human actions inputs			
Action 1	A2	A3	Resulting human-induced component behavior
Nominal Action Classification (NAC) 1	NAC1	NAC1	Human Induced Nominal Behavior (HINB) 1
Faulty Action Classification (FAC) 1	NAC1	NAC1	HINB 1
FAC2	FAC1	NAC2	Human Induced Faulty Behavior (HIFB) 1
NAC2	FAC1	FAC1	HIFB1

3.1 Calculating the Cost of a Scenario and the Expected Cost of the System. The costs of a scenario come from disruptions to safety and performance and required repairs [21,39]. To quantify these costs, we use Eq. (3), where C_s is the cost of a scenario, C_f is the immediate cost (e.g., due to safety impacts), C_p is the performance cost (e.g., due to lost functionality), t_r is the time to recover, C_r is the cost of repair, NF is the functions in faulty states, and FC is the components in faulty behavior mode. For C_f and C_p, all functions that are not in a nominal state are considered. For C_r, all components that are in a non-human-induced behavior mode are considered because human-induced modes do not constitute damage, since they can be changed back to nominal by the operators. Depending on if the components are repaired in parallel or series, t_r will be equal to the recovery time of the behavior mode with the longest recovery time or the sum of the recovery times of all faulty behavior modes in the scenario.

$$C_s = \sum_{i \in NF} C_{f,i} + \left(\sum_{i \in NF} C_{p,i} \right) \times t_r + \sum_{b \in FC} C_{r,b} \tag{3}$$

To adapt this cost model to the system of interest, immediate cost and the cost of lost performance must be specified for the "Lost" and "Degraded" states of each function, as well as the repair cost and recovery time for each behavior mode of each component, which may be estimates based on historic data. Any safety costs can be incorporated using cost schedules applicable to the industry (e.g., Ref. [40]). The cost of a scenario is calculated based on the functional status and the behavior modes of the components in the final time-step (i.e., $t = 3$ in Table 1) of a scenario. We use Eq. (4) to calculate the expected cost of failure of the system C_F, where T is the life-cycle time, λ_s is the failure rate of the scenario, C_s is the cost of a scenario calculated in Eq. (3), and F is a set of failures. Since HEFFR output scenarios are only those that cause the critical functions to fail, this cost calculation is only tabulated for those failures, which may be an incomplete set. Since the probability of failure is defined as in Eq. (1), the term $T\lambda_s$ in Eq. (4) is calculated using Eq. (5), where P_s is the probability of the failure scenario.

$$C_F = \sum_{S \in F} T\lambda_s C_s \tag{4}$$

$$T\lambda_s = -ln(1 - P_s) \tag{5}$$

3.2 Calculating the Likelihood of a Scenario. In this model, the behaviors of components in a time-step and the events instantiated between time-steps are considered independent. This assumption is made for simplicity and because the HEFFR simulation accounts for failures through the functional health of the system and the cascading effects of failures through the automated scenario generation. That is, when a new event is introduced to a scenario, no further events are introduced for a user-defined number of time-steps and the simulation allows the failures to propagate at the functional level. Hence, the interdependent failures will be assessed through their propagation at the functional level, so each event in a scenario can be thought of as an independent initiating event. Moreover, when an event has multiple faulty component behaviors present, each faulty behavior is considered to be independent of the others. Since the scenario generation considers all possible combinations of behaviors, cascading effects of every faulty behavior occurring alone or in tandem with others will be evaluated during the simulation. This is done mainly for simplicity; while more detailed models, such as Markov Chain Monte Carlo models or Bayesian graphs, represent events or behaviors as probabilistically dependent [41], these methods rely on transition probabilities which may be difficult to specify in the early design stages.

3.2.1 Calculating the Probability of Non-Human-Induced Behavior Modes. The probability P_f of a component operating in a faulty behavior mode is calculated using Eq. (1), assuming a constant failure rate (λ) and an exponential probability distribution. For t in Eq. (1), the expected product lifetime should be used. The probability of a component operating in a nominal behavior mode (P_n) is determined using Eq. (6). We recommend using Nonelectronic Parts Reliability Data (NPRD) and Electronic Parts Reliability Data (EPRD) to source component failure rates. These documents are created through a rigorous data collection process where historic failure events, maintenance records, and published data are used to present component failure rates [42,43]. NPRD and EPRD consider a component to be failed when a part is repaired/replaced, and the failure symptoms were no longer present [42,43], meaning that human-induced behavior modes of components are not considered during the failure rate calculations.

$$P_n = 1 - P_f \tag{6}$$

Failure Mode/Mechanism Distributions (FMD) publishes the probability of failure modes and mechanisms of components, given that there is a failure [44]. The data is sourced and scrutinized similar to NPRD and EPRD [44]. When a component is in a nominal behavior state, the probability of the current behavior of a component P_c is equal to P_n. When a component goes to a faulty behavior mode from a nominal state, data from FMD can be used to calculate the probability of a specific faulty behavior mode P_{fb} using Eq. (7), where P_{fm} is the probability of a faulty behavior mode given that a failure is present. In that case, P_c is equal to P_{fb}. When a failure mode is already present for a component, P_c is equal to P_{fm} of the current behavior mode, because a component that is in a non-human-induced behavior mode needs to be repaired to go back to a nominal state, making the probability of it returning to nominal 0. A failure mechanism is the process that caused the failure, whereas a failure mode is the effect of the failure observed [44]. In HEFFR, the behavior modes of components are similar to failure modes. Hence, only the failure mode probabilities need to be sourced from FMD. Since FMD does not distinguish between the probabilities of failure modes and mechanisms [45], failure mode probabilities need to be normalized to omit the mechanism probability distributions. For instance, if a component has two modes and a single mechanism, each mode has a distribution probability of 0.2 and 0.3, and the mechanism has a distribution probability of 0.5, the normalized probabilities of the modes will be 0.4 and 0.6, respectively.

$$P_{fb} = P_f \cdot P_{fm} \tag{7}$$

3.2.2 Calculating the Probability of Human-Induced Behavior Modes. We use a combination of SPAR-H [27] and HEART [20] methodologies to calculate the probabilities of human-induced behaviors. In HEEFR, ASGs are used to track the human actions that need to be performed to interact with a component. Since the tasks in HEART are at a higher level (e.g., reduce speed) than actions (e.g., grasp object) in ASGs, a direct comparison between the generic tasks in HEART and actions in ASGs may be confusing. Hence, we propose the partial use of SPAR-H to assign human actions to generic tasks. As in SPAR-H, we propose that designers designate each human action in an ASG as "action," "diagnosis," or "mixed" if they are physical, cognitive, or both, respectively. For instance, the action "Reach" will be designated "action" since it is physical, whereas action "Detect" will be designated "diagnosis" for being cognitive. The authors of SPAR-H have provided the HEART generic tasks that are comparable with these designations, where generic tasks D and F are comparable with designation "action" and generic tasks A-H, and M are comparable with designations "diagnosis" and "mixed." Designers can use these comparisons to assign generic tasks to human actions in the ASGs (Generic task descriptions can be found in Ref. [20]). When assigning generic tasks to human actions each action should be assigned one generic task.

The next step is to assign Error Producing Conditions (EPC) for each ASG in the system representation. In total, there are 38 EPCs that can be assigned. A list of the HEART generic tasks and the EPCs used in this research is provided in Appendix A. Note that the EPCs are evaluated for whole ASGs and not for individual actions, because the EPCs in HEART are more relevant at the task level and not at specific action levels. In practice, HEART assessment requires the assignment of generic tasks at the task level also, but doing so will not enable one to identify the actions that contribute to a task failure. Hence, we have proposed the application of generic tasks to specific actions in the ASGs to calculate the probability of individual actions failing. Some of the generic actions already incorporate EPCs. The authors of HEART recommend omitting EPCs that are already incorporated in generic tasks to avoid overestimation. The proportion of effects of an EPC must be evaluated for each action in the ASG because the effect of these factors on each action may vary depending on the action performed. In summary, the probability of an action in the ASG failing can be calculated using Eq. (8), where P_{hf} is the probability of a human action failing, P_g is the generic task probability from HEART, *EPC* is the error producing condition factor, and x (between 0 and 1) is the proportion of effect of EPC. Then, the probability of a nominal human action (P_{hn}) can be calculated using Eq. (9).

$$P_{hf} = P_g \times \prod_i ((EPC_i - 1) \times x_i + 1) \tag{8}$$

$$P_{hn} = 1 - P_{hf} \tag{9}$$

When a human does not attempt to perform an action, identifying if that action is in a nominal or faulty state depends on the context of the overall system. For instance, if operators detect some signal that requires them to reach a valve, grasp it, and turn it off, and they do not attempt to do so, these actions will be classified as faulty. However, if there was no signal and they are not expected to turn off the valve, and they make no attempt, the actions will be classified as nominal. Hence, we consider the human-induced behavior in the previous time-step and the current time-step to determine if a human action is in a nominal or faulty classification when no attempt to perform an action is made. A human action can have multiple nominal and faulty classifications. However, the calculations only identify the probability of a nominal or faulty action classification: they do not go into detail to calculate the probabilities of specific classifications, since there is no direct method to calculate such probabilities like there is for component behavior modes. Hence, to identify the influence of specific action classifications, data mining approaches (e.g., those in Ref. [18]) will need to be used.

Once the probabilities of each action in the ASG is assigned, the probability of the resulting human-induced behavior can be calculated using Eq. (10). Multiple action classification combinations can result in the same human-induced behaviors. Hence, a union of all these action classification combination probabilities is taken to calculate the actual probability of a human-induced behavior P_h. For instance, if a human-induced behavior has two action classification combinations and their probabilities calculated using Eq. (10) is equal to $P_{h'_1}$ and $P_{h'_2}$, the actual probability of the human-induced behavior is calculated using Eq. (11). Since the human-induced faults are not considered in the failure rate calculations, the probability of nominal component behavior (P_n) incorporates the human-induced behaviors. Hence, When a human-induced behavior is present in a component, the probability of the current behavior P_c is calculated using Eq. (12).

$$P_{h'} = \prod_i P_{hf,i} \cdot \prod_j P_{hn,j} \tag{10}$$

$$P_h = P_{h'_1} + P_{h'_2} - P_{h'_1} \cdot P_{h'_2} \tag{11}$$

$$P_c = P_h \cdot P_n \tag{12}$$

3.2.3 Calculating the Probability of an Event and a Scenario. The next step is to calculate the probability of an event P_e using Eq. (13), where i is all components. Then, for every time-step j, where the event is not equal to the event in the previous time-step, the probability of a scenario is calculated using Eq. (14). When an event is allowed to propagate, no new events are introduced in the following time-step. Hence, such time-steps are omitted in the probability of scenario calculation. Note that since the simulation is time-based, each time-step represents a discrete change in system state, and the simulation runs until a critical function has failed or a maximum number of time-steps are reached, the total number of time-steps need to be chosen to minimize event repetition. More details on how to choose the total number of time-steps can be found in Ref. [18]. If not the simulation may become computationally expensive. In summary, the simulation takes inputs for costs, failure rates, system life cycle time, human generic tasks, EPCs, and EPC proportion effect factors in addition to the HEFFR automated scenario generation inputs. After the simulation, the cost of a scenario, expected cost of failure of the system, probability of a scenario occurring, and probabilities of action classification combinations are recorded along with the outputs from the HEFFR automated scenario generation simulation.

$$P_e = \prod_i P_{c,i} \tag{13}$$

$$P_s = \prod_j P_{e,j} \tag{14}$$

3.3 Understanding the Results. The execution of the simulation yields a list of fault scenarios that result in the critical function failing and their probabilities, costs, and expected costs. We have not added any data synthesis as part of this work. Instead, we provide as much data as possible, so designers can extract information tailored to the requirements and challenges of the system they are designing. The goal of this approach is to not give exact probabilities for action/task or component failures, but to provide estimates that are reliable enough to study the relative impact of faults during conceptualization. Providing detailed probabilistic models for failures requires very specific information relating to the system. To comprehensively quantify human error probabilities, details on actual tasks, the environment where the task is performed, and the operator need to be considered. Since this information is not readily available early in design, estimating the corresponding probabilities in early design stages is difficult and subject to uncertainty.

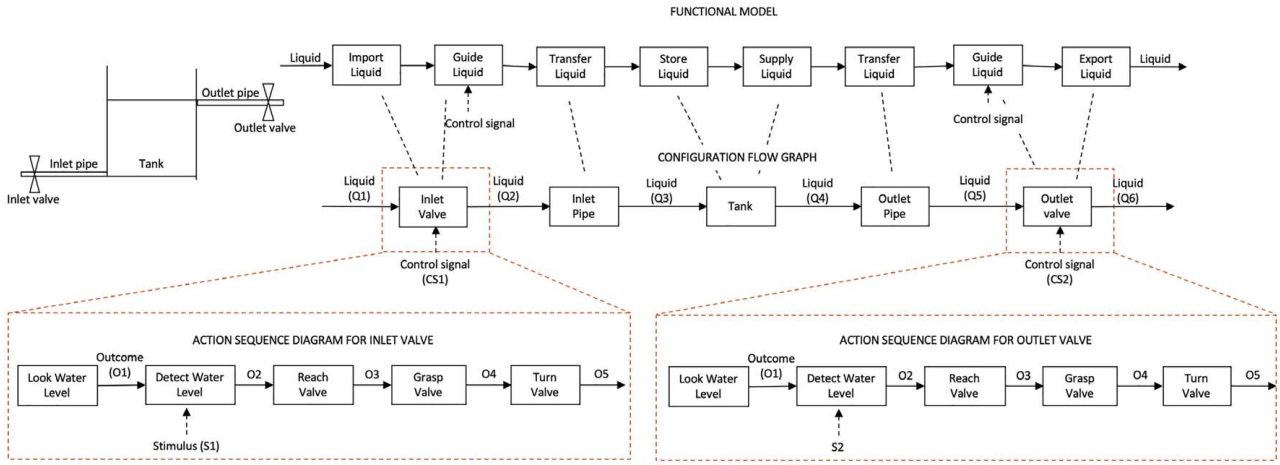

Fig. 2 The system representation of the hold up tank [16]

Thus, we focus on providing designers with an appropriate level of model fidelity to identify and prioritize risks early, without making the analysis too detailed.

4 Case Study

We have chosen a liquid tank design problem to demonstrate the capabilities of the proposed work. Various forms of this problem have appeared in previous studies [16,18,22,46,47]. The problem is to design a liquid cooling tank that can maintain its coolant level between a minimum and maximum threshold. The cooling tank is expected to maintain the temperature of a certain industrial machine that can explode if overheated (i.e., if the coolant level becomes too low). If the coolant level is above a certain level, the machine will cool down too much, resulting in severe damage. The coolant is a hazardous chemical which can cause health issues to human if exposed in large quantities. A human operator is expected to monitor the liquid level of the tank and shut off the incoming liquid if the water level is too high, and shut off the outgoing liquid if the water level is too low. This set-up is a simplified archetype of nuclear reactors and industrial plant operation, where maintaining optimal temperature is critical for both performance and safety. Aircraft pilots and submarine operators also face similar situations where they monitor displays and act based on the given information [48,49].

The system representation of this problem, including the functional model, configuration flow graph, and ASGs, is provided in Fig. 2. The system has eight functions and five components, two of which interact with the human. The operator will interact with the valves to shut off the flow of liquid. The functions, corresponding components, and their behavior modes are shown in Table 3. The human-induced behaviors are shown in bold in Table 3, and Table 4 shows the human actions and their classifications. We use the function "Store Liquid" as the critical function because of its importance in maintaining the temperature of the equipment and its failure can impact safety. The number of time-steps a failure is allowed to propagate was set to two because the simulation is set up, so any failure event takes no more than two time-steps to cause the critical function to fail given no more events are introduced. The maximum number of time-steps was set to four to avoid scenario repetition.

The human actions were designated as "Action," "Diagnosis," or "Mixed." Then, the generic tasks were chosen based on nature of the actions and their ability to match with generic task descriptions. For example, the action "Grasp" was assigned generic task D because it is a simple task requiring minimal attention. Six EPCs were identified for each ASG based on the system model and the expected human-system interactions. The EPCs related to the operator (e.g., operator experience) were not considered since no such information is available in the design problem. We assigned the proportion of effects of each EPC for each action based on the action performed, the component the action will be performed on, how the action will be performed, and the conditions surrounding performing the action. For instance, for the EPC "No clear direct and time confirmation of an intended action from the portion of the system over which control is to be exerted," the action "Detect" was assigned a proportion of effect 0.1 for both inlet and outlet valves because the system model did not include any means of confirmation for the detection of signal. However, if the operator fails to detect the signal, the effects on the system will only be seen if they acted upon it (through action "Turn," a different action), making the proportion of effect of the EPC for the action "Detect" low.

We selected the failure modes of components from NPRD-95 [50], assuming the Ground Fixed operating environment when rates were available. If they were not, failure rates from other ground environments were chosen depending on their applicability for this case study. The total life cycle time was chosen as two years, given that the system will be in constant operation. The failure

Table 3 Functions, corresponding generic components, and their behavior modes [18]

Functions	Generic components	Behavior modes
Import Liquid Guide Liquid Export Liquid	Valve	**Nominal On**, **Nominal Off**, **Failed Open**, **Failed Close, Stuck Open, Stuck Close**
Transfer Liquid	Pipe	Leak, Ruptured, Nominal
Store Liquid Supply Liquid	Tank	Nominal, Leak

Note: The human-induced behaviors are shown in bold.

Table 4 Action classifications of actions in action sequence graph [18]

Actions	Classifications			
Look	Visible	Not Visible		
Detect	Detected – Nominal	Not Detected – Nominal	Detected – Failed	Not Detected – Failed
Reach	Reached – Nominal	Reached – Failed	Cannot Reach	No Action
Grasp	Grasped	Cannot Grasp	No Action	
Turn	Turn to Close	Turn to Open	Cannot Turn	No Action

mode distributions of the components were selected from FMD-97 [51]. The repair costs of the components were estimated based on the cost of part replacement and diagnosis. The recovery times included the time to repair components and time to clean up any resulting spills. The performance costs of each function considered the impact of the function being degraded or lost on overall system performance. The immediate costs of each function were estimated considering the chemical exposure, safety, and necessary cleanup if there was a coolant spill. Assigned values relating to human actions, components, and costs are available in Appendix B.

In this case study, we demonstrate the use of expected cost modeling to quantify risk in an HEFFR simulation. We then explore the results to see if the proposed method is capable of giving insight to designers about potential worst-case fault scenarios that cause the critical function to fail by answering the following questions. Can we prioritize fault scenarios in terms of severity and likelihood? Are there any fault scenarios that can be discarded? What are the worst-case component behavior modes? What is the contribution of specific human actions to failures? In summary, we try to understand if the proposed risk metrics calculations can help designers quantify the risk of component failures and human errors acting in combination and identify and prioritize worst-case fault scenarios to inform risk mitigation. Note that we do not go into detail on how to perform a HEFFR analysis or automatically generate fault scenarios in this paper because they have been documented in previous work [16–18]. Instead, we have focused on the new elements introduced in this paper: calculation of the likelihood of occurrence of a scenario and the expected cost of failures.

5 Results

In this section, we discuss the results of the HEFFR simulation for the coolant tank case study in detail. The simulation begins by taking the critical function ("Store Liquid" failing), initial component behavior modes (nominal for all components), initial liquid flowrate (nominal), initial tank coolant level (nominal), the maximum number of time-steps (4), and the number of time-steps a failure event is allowed to propagate (2) as inputs. Next, the inputs for likelihood of occurrence and expected cost calculations are read (the input values are listed in Appendix B). In total, around one million scenarios that could cause critical function failure were generated. The total expected cost of the system was found to be around one million dollars. The highest failure cost was around 52 million dollars, and the maximum likelihood of occurrence was around 3.5×10^{-3}. The lowest-likelihood scenario had a probability of around 2.8×10^{-24}, and the minimum scenario cost was around 13 million dollars. A majority of the scenarios modeled had low probabilities and thus low expected costs. One reason for the low probabilities is the independence assumption used in the probability model, where the probability of every independent behavior or event is multiplied with the others. Another reason for this is because adverse events are rare by definition. As a result, it may be expedient to put the scenarios in groups so that the high-cost scenarios are given priority.

Figure 3 shows a set of priority groups for the scenarios by setting a cut-off for the expected cost of scenarios. As shown, the *cumulative* expected cost of the scenarios in the green is below 1000 dollars. As a result, the designer may choose to ignore them. The cumulative expected cost of all scenarios in yellow is less than 10,000 dollars and thus *may be* worth considering as a group. The high-impact scenarios are labeled in orange and red, with the highest impact scenarios in red. Based on these cut-offs, these scenarios should be given individual attention to mitigate hazards effectively. For instance, one of these worst-case scenarios caused the critical function to fail in three time-steps. In the first time-step, the tank is in a faulty behavior mode ("Leak"). In the next time-step, no further failures are present (failure from the last time-step is allowed to propagate). Finally, the outlet valve goes into a human-induced faulty behavior ("Failed Open") while the tank is still leaking. The benefit of this cost model is it identifies high-cost, high-probability scenarios like this and gives them priority over less likely, less costly scenarios.

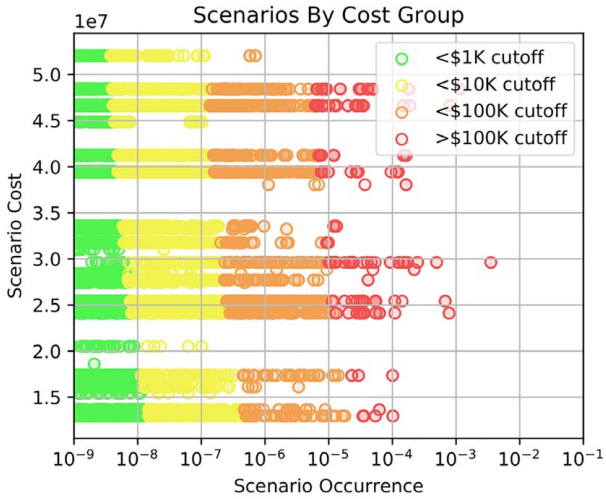

Fig. 3 Cost groups of fault scenarios

The impacts of each fault mode can be assessed by calculating the respective cumulative expected cost of scenarios for each (Fig. 4). The behavior modes "Leak" for the tank and "Ruptured" for the inlet pipe have the highest expected cost among the non-human-induced faulty behaviors. Designers may mitigate these risks by selecting components with lower failure rates, adding redundancies, including advanced failure detection mechanisms, performing tests to understand the failure mechanisms, and minimizing the chemical exposure when a failure occurs. As shown, the human-induced faulty behaviors for inlet and outlet valves ("Failed Open" and "Failed Close") have a high expected cost. Hence, further assessment is needed to understand the specific human action combinations that contribute to the faulty human-induced behaviors. Figure 5 shows the maximum reduction of probability by eliminating action classification combinations. For example, for the inlet valve, the probability for faulty behaviors can be reduced by 80%, if the top 45 of the total 112 action classification combinations are eliminated. While one cannot *eliminate* action classification combinations, this plot shows that the human failure probability can be reduced significantly by focusing on a small subset of combinations. The human action failure probabilities of

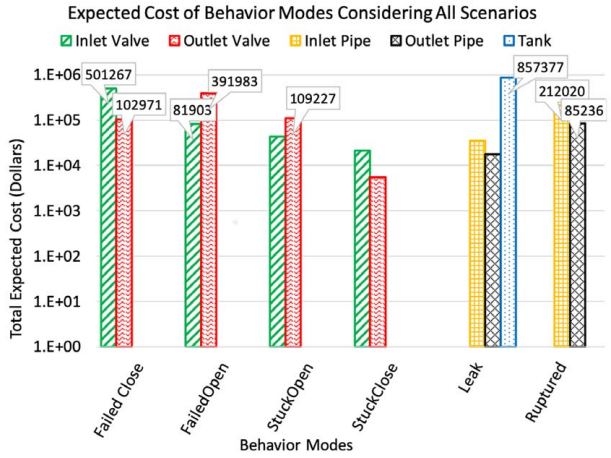

Fig. 4 Expected cost of behavior modes

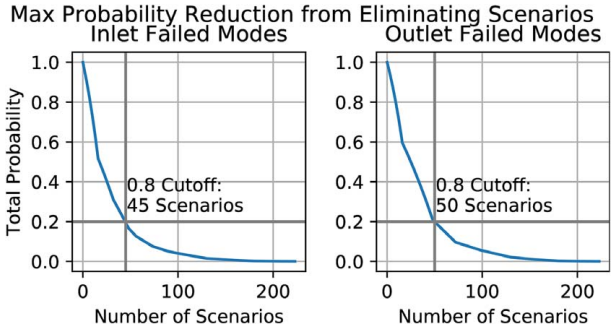

Fig. 5 Maximum probability reduction from human action combination elimination

these combinations can be reduced by changing the system design and operational setting.

Figure 6 shows the number of times faulty action classifications are present among the scenarios that can reduce the likelihood of behavior modes "Failed Open" and "Failed Close" of both valves by 80% each. As shown, faulty action classifications were only present for actions "Detect," "Reach," and "Turn." Also, not all faulty action classifications of these actions were present (e.g., Cannot Reach for action "Reach"). Cognitive errors (detection related and when actions are not attempted) were more prevalent when compared with non-cognitive errors (Cannot Turn). One way to reduce the likelihood of the faulty action classifications occurring is to reduce the effect of EPCs through the design of the system. For instance, designers may include action feedback mechanisms to eliminate EPC-14. For cognitive errors, the designers may suggest training or operating procedures to improve operator situation awareness as a means of mitigating them. They may also follow Human Factors Engineering guidelines to improve the design to support error mitigation. For the non-cognitive human error, they may use Digital Human Modeling to visualize the interaction and perform further ergonomic assessments.

One of the major limitations of using an expected cost model to prioritize fault scenarios is that the input information (rates and costs) may be low-fidelity. In this situation, it is important to understand how changes in the model inputs variables affect the expected cost of scenarios and thus the results of the analysis. To consider this uncertainty, we performed a Sobol [52] sensitivity analysis with 10,000 samples (using Saltelli [53] sampling 560,000 model inputs in total) for the hold-up tank study. Performance cost, repair cost, repair time, immediate cost, the proportion of effects for error producing conditions, and failure rates related variables (54 in total) were considered to have uncertainty. When assigning uncertainty ranges, ±20% of the original values were used to

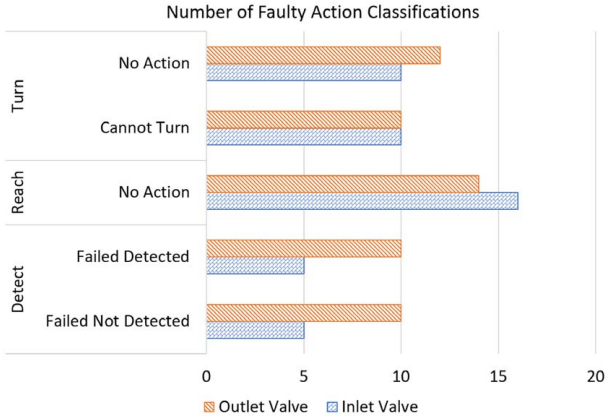

Fig. 6 The number of faulty action states

assign minimums and maximums for all variables except for the proportion of effects for error producing conditions related variables. For the proportion of effects for error producing conditions related variables ±0.2 of the original values were used to represent the uncertainty better. Since variables considered in the expected cost calculation vary scenario-to-scenario, we randomly chose 100 scenarios to perform the sensitivity assessments. The average first-order and total sensitivity indexes were calculated to understand the sensitivity of the model for each of the input variables with uncertainty. The first-order sensitivity index indicates the effect of individual input variables, whereas the total sensitivity index indicates the effect of individual variables and the effect of all interactions.

The first-order and total sensitivity indexes for failure rates and the proportion of effects of EPC factors were the highest (first order: 54.9% and 40.8%; total: 50.8% and 38.5%), followed by repair time-related variables (first order: 3.7%, total: 4.2%). The first order and total sensitivity indexes for the other variable groups were negligible. Among the failure rates, the failure rate of the pipe had the highest first order and total sensitivity indexes (66% and 61%). Among the proportion of effects of EPC factor variables, variables relating to the action "Turn" for inlet and outlet valves had the highest first-order and total sensitivity indexes. Because of the high uncertainty in these variables, designers may focus on designing the system to both improve the EPC factors and lower the sensitivity in the cost model (thus making the cost assessment more accurate and reducing project risk). As shown, sensitivity analysis helps pinpoint variables that require attention when considering uncertainties. When used in design, the HEFFR analysis and corresponding sensitivity analysis can be repeated iteratively as the design changes to ensure risk-related design goals are fulfilled.

6 Discussion

The example presented above shows how using a probability and cost model in the HEFFR framework can extend its capabilities to quantify the severity of component failures and human errors acting alone and in combination, compare fault scenarios, and identify the worst-case scenarios in terms of overall impact. The results show that the generated data can be assessed further to examine the impact of faulty behavior modes, identify action combinations with the greatest potential for improvement, and pinpoint human actions that need further refinement. In the case of the coolant tank design problem, we were able to identify the high-cost high probability failures requiring individual attention, low-cost high probability failures, and scenarios too rare to require further assessment. The faulty behavior modes relating to the inlet pipe and tank had a higher expected cost among non-human-induced faulty behaviors. The expected costs of human-induced faulty behaviors were also

high. We also found that the likelihood of human-induced faulty behavior modes can be reduced significantly by only assessing a fraction of the action classification combinations. Among the action classification combinations with the highest potential for faulty behavior likelihood reduction, cognitive errors relating to actions "Detect," "Reach," and "Turn" were prevalent, though a few combinations also included non-cognitive errors relating to the action "Turn."

The approach presented in this paper is limited by the uncertainties present in the expected cost and likelihood calculations, including those in parameter estimates and modeled behaviors [54,55]. This is an important limitation, because while some decisions may not need completely accurate inputs [56], design failures are theorized to result from designer biases [57]. A sensitivity analysis allows designers to account for some of these uncertainties (specially, uncertainty relating to parameter input variables) by pin-pointing variables that can have the highest effect on the system when uncertainties are present. This enables designers to account for these uncertainties and make better-informed decisions. The sensitivity analysis performed here showed that variables that are directly influenced by design decisions (failure rates of components and EPC-related variables) had a high impact on the expected cost when compared to cost-related variables, showing the importance of the designers' role when it comes to risk mitigation. The fact that both human error- and component failure-related variables having high total sensitivity indexes (or the effect of individual variables and the effect of all interactions) shows the importance of assessing both human errors and component failure in combination rather than in isolation. The results also show that performing a sensitivity analysis will allow designers to pinpoint specific variables or areas of design that need to be focused on to improve overall risk effectively.

The above results show how the introduction of the likelihood of scenarios and expected cost to the HEFFR framework can aid designers to evaluate fault scenarios and take risk mitigation action. Without these metrics, there is no way to distinguish between fault scenarios in the output of the HEFFR framework, which creates the necessity to consider all scenarios equally. Since these simulations produce millions of potential fault scenarios that cause critical function failure, considering all fault scenarios to be equal is not feasible. Using these metrics in the HEFFR framework, fault scenarios can be prioritized based on their severity, enabling designers to prioritize the most important scenarios when designing mitigating features. In summary, this approach helps designers understand the impacts of component failure and human errors acting alone or in tandem in the early design phase to make risk-informed decisions. This is important because in traditional risk assessment methods, such vulnerabilities come to light later–when design changes are costly and time-consuming–forcing designers to find workarounds and retrofit changes (to meet deadlines and cost targets) rather than proactively guarding against such vulnerabilities by design. The early design application of the proposed approach reduces the chances of making such costly and time-consuming design changes.

When failure occurs, often, the impact on the operators and the surroundings is much higher compared to the impact of lost performance. Hence, it is important to understand how failures affect the environment and the human to be able to minimize risk appropriately. The proposed approach includes the immediate costs in the cost calculation model, enabling the quantification of the detrimental effects of failures on the environment and the safety of the human. With the proposed approach, we try to generate as much data as possible. With the advances in the field of data science, we believe that designers should be able to leverage as much data as possible to extract the information they need to solve a design problem. For example, the case study presented in this research tries to identify worst-case fault scenarios and impacts of faulty behavior modes and human actions. The data analysis presented in the results section was tailored to address these questions. Others may want to use this framework to compare design alternatives; for this, the expected cost of each can be used to trade design risk with other performance attributes (e.g., efficiency). For example, if one wishes to consider automating a process, system designs with and without human-component interactions can be assessed on the basis of expected cost. Similarly, if concept refinement and component selection are desired, the component behavior mode costs and probability can be assessed to identify points of potential improvement.

On the human front, designers might want to identify safe operating procedures, training requirements, or safety protocols, which all can be identified by analyzing the human actions and human-induced behaviors of components. Given the amount of data present, the potential ways to analyze the data are not limited to what is listed here—the data can be synthesized to address design problems as designers see fit. All the benefits listed above, especially the data assessment requirements, encourage designers to think more deeply about the system under development early in the design process, which can result in well-thought-out designs. As a result, the potential for identifying vulnerabilities relating to human interactions and components later in the design stages or even after the system is in use is minimized.

One limitation of the model used in this work is that it assumes independence in the probability calculations, which may be an underestimate. The fact that a majority of scenarios as shown in Fig. 3 were given very low probabilities was a result of the underlying probability model form, which is subject to mathematical model uncertainty [58]. Thus, while using expected cost is shown here to help identify the highest-priority scenarios, valuing the set of scenarios remains a challenge because of the effect of epistemic model and parameter uncertainties [54]. However, in the early design stages, establishing dependencies to any reasonable accuracy is difficult, especially for human interactions. Hence, we recommend the use of the proposed metrics only to compare between scenarios and alternative designs rather than using them to quantify exact likelihood and cost. It should be noted that many of the later design stage probabilistic risk and safety assessment methods such as ETA, FTA, THERP, and SPAR-H incorporate dependencies in the probability calculations. Hence, the application of these methods later on in the design will allow engineers to understand the likelihood and cost of failure more accurately. Nevertheless, identifying the ideal underlying cost function and probability model to use in early design remains a challenge, and the use of different probability model assumptions should be explored in future work to determine the sensitivity of the value of these scenarios to model assumptions and identify the most appropriate model forms.

Also, the user-defined proportion of effects of EPCs can be subjective. Previous work has attempted to remove the subjectivity surrounding this variable by replacing it with fuzzy linguistic expressions [59]. A similar approach can be taken if no subjectivity is desired. In summary, with the introduction of the risk metrics, designers can use the HEFFR framework to identify worst-case fault scenarios, perform trade-off studies, establish operating procedures and training, identify points of potential human product interaction, and many more early in design. However, the probabilities calculated may be subjective or be an underestimate due to assumptions made. As a result, we advise using this framework to complement, not replace, traditional probabilistic risk assessment methods.

7 Conclusions and Future Work

This paper integrates probability and cost modeling with the HEFFR framework to quantify the risks of human and component failures. With these metrics, designers can use the HEFFR framework to identify worst-case fault scenarios, prioritize fault scenarios, quantify the impact of human errors and component failure, and pinpoint areas (both component and human interaction related) where improvements can yield the greatest risk mitigation. Additionally, the framework can be used for risk-based trade-off

studies, to establish operating procedures and training, and to come up with safety protocols.

One limitation in the presented approach is that it does not consider the uncertainties when calculating expected cost and likelihood. While performing a sensitivity analysis (as presented here) can help designers to account for some of the uncertainties, it does not give designers a full picture of the effects of the uncertainties present within the model. Future work should study how to understand the effect of uncertainties on the model to enable designers to best account for it in hazard modeling and risk-based decision-making. Additionally, there is no confirmation that the modeled scenarios identified in this study match the modeled scenarios for a real system. We intend to address these issues by validating the results against traditional risk assessment methods. Furthermore, this study mainly focused on demonstrating the proposed model. The performance of the proposed calculation models surrounding its various applications (trade studies, component exploration, etc.) is yet to be demonstrated. Future work will focus on incorporating uncertainty in the risk models, validating the methodology, and exploring its applications.

Acknowledgment

This research is supported by The National Aeronautics and Space Administration (NASA) award number 80NSSC18K0940. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

Conflict of Interest

There are no conflicts of interest.

Data Availability Statement

The datasets generated and supporting the findings of this article are obtainable from the corresponding author upon reasonable request.

Appendix A: Descriptions of HEART Generic Tasks and Error Producing Conditions Used in This Research

Table 5 Description of heart generic task types used in this research [20]

Generic task type	Description	Proposed nominal human unreliability
(D)	Fairly simple task performed rapidly or given scant attention	0.09
(E)	Routine, highly practised, rapid task involving relatively low level of skill	0.02
(F)	Restore or shift a system to original or new state following procedures, with some checking	0.003
(M)	Miscellaneous task for which no description can be found	0.03

Table 6 Descriptions and maximum effect factors for heart error producing conditions used in this research [20]

EPC #	Error producing conditions	Maximum effect factor
2	A shortage of time available for error detection and corrections	11
10	The need to transfer specific knowledge from task to task without loss	5.5
13	Poor, ambiguous or ill-matched system feedback	4
14	No clear direct and timely confirmation of an intended action from the portion of the system over which control is to be exerted	4
17	Little or no independent checking or testing of output	3
34	Prolonged inactivity or highly repetitious cycling of low mental workload tasks	1.1 (for 1st half-hour)/1.0 (for each hour thereafter)

Appendix B: Simulation Inputs

Table 7 Component failure rates, distributions, repair cost, and recovery times

Component	Failure modes	Failure rate (NPRD-95) [50] per million hours	Distributions (FMD-97) [51]	Notes	Repair cost ($)	Repair time (h)
Tank	Leak	1.616	100%	Summary data from storage tank was used due to its similarities with the coolant tank case study	20,000	24
Valve	StuckOpen StuckClose	3.0764	47.44% 52.56%	A hydraulic valve was chosen. The failure mode leak was omitted because it is modeled in the pipe and modeling it here will be redundant	10,000 10,000	6 6
Pipe	Leak Ruptured	0.4734	7.42% 92.58%	Summary data of the component Piping was chosen for the pipe failure rate. The Failure Mode Broken is Considered as ruptured	10,000 15,000	6 12

Table 8 Human actions, designations, and related generic tasks

Actions	Designation	Generic task
Look	Both	E – 0.02
Detect	Diagnosis	M – 0.03
Reach	Action	D – 0.09
Grasp	Action	D – 0.09
Turn	Action	F – 0.003

Table 9 Costs of function failures

	Performance cost		Immediate cost
Function	Degraded	Lost	Lost
Import liquid	35,000	175,000	0
Guide liquid	60,000	300,000	0
Transfer liquid	80,000	400,000	200,0000
Store liquid	100,000	500,000	500,0000
Supply liquid	40,000	200,000	0
Transfer liquid	25,000	125,000	3,000,000
Guide liquid	75,000	375,000	0
Export liquid	30,000	150,000	0

Table 10 Human error producing conditions and their proportion of effects for each action

Error producing conditions (EPC)		EPC proportion of effects									
		Look		Detect		Reach		Grasp		Turn	
Inlet valve	Outlet valve	Inlet	Outlet	Inlet	Outlet	Inlet	Outlet	Inlet	Outlet	Inlet	Outlet
EPC2-11	EPC2-11	0	0	0.1	0.2	0.1	0.1	0	0	0.4	0.6
EPC10-5.5	EPC10-5.5	0	0	0.2	0.2	0	0	0	0	0.2	0.2
EPC13-4	EPC13-4	0.1	0.2	0	0	0.1	0.1	0	0	0	0
EPC14-4	EPC14-4	0.6	0.3	0.1	0.1	0	0	0	0	0	0
EPC17-3	EPC17-3	0	0	0	0	0	0	0	0	0.6	0.4
EPC34-1.1	EPC34-1.1	0.9	0.9	0.6	0.6	0	0	0	0	0	0

References

[1] Shappell, S. A., and Wiegmann, D. A., 1996, "U.S. Naval Aviation Mishaps, 1977-92: Differences Between Single- and Dual-Piloted Aircraft," Aviat. Space Environ. Med., **67**(1), pp. 65–69.

[2] Högberg, L., 2013, "Root Causes and Impacts of Severe Accidents At Large Nuclear Power Plants," Ambio, **42**(3), pp. 267–284.

[3] Sneddon, A., Mearns, K., and Flin, R., 2006, "Situation Awareness and Safety in Offshore Drill Crews," Cognit. Technol. Work, **8**(4), pp. 255–267.

[4] Wiegmann, D. A., and Shappell, S. A., 2001, "Human Error Analysis of Commercial Aviation Accidents: Application of the Human Factors Analysis and Classification System (HFACS)," Aviat. Space Environ. Med., **72**(11), pp. 1006–1016.

[5] Demirel, H. O., 2015, "Modular Human-in-the-Loop Design Framework Based on Human Factors," Ph.D. thesis, Purdue University, West Lafayette, IN.

[6] Ullman, D. G., 1992, *The Mechanical Design Process*, Vol. 2, McGraw-Hill, New York.

[7] Stamatelatos, M., Dezfuli, H., Apostolakis, G., Everline, C., Guarro, S., Mathias, D., Mosleh, A., Paulos, T., Riha, D., Smith, C., Vesely, W., and Youngblood, R., 2011, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," NASA, Report No: NASA/SP-2011-3421, Washington, DC, https://ntrs.nasa.gov/citations/20120001369.

[8] Vesely, W. E., Goldberg, F. F., Roberts, N. H., and Haasl, D. F., 1981, "Fault Tree Handbook," Technical Report, Nuclear Regulatory Commission Washington DC.

[9] Ericson, C. A., 2015, "Event Tree Analysis," *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Hoboken, NJ, pp. 223–234.

[10] US Department of Defense, 1980, Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Military Standard MIL-STD-1629A, US Department of Defense, Washington DC.

[11] Embrey, D., 1986, "Sherpa: A Systematic Human Error Reduction and Prediction Approach," Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems, Knoxville, TN, Apr. 21–24, pp. 184–193.

[12] Swain, A., 1964, "Therp Technique for Human Error Rate Prediction," Proceedings of the Symposium on Quantification of Human Performance, Albuquerque, NM, Aug. 17–19.

[13] Short, A. R., 2016, "Design of Autonomous Systems for Survivability Through Conceptual Object-Based Risk Analysis," Ph.D. thesis, Colorado School of Mines, Arthur Lakes Library, Golden, CO.

[14] Lough, K. G., Stone, R., and Tumer, I. Y., 2009, "The Risk in Early Design Method," J. Eng. Des., **20**(2), pp. 155–173.

[15] Huang, Z., and Jin, Y., 2008, "Conceptual Stress and Conceptual Strength for Functional Design-for-Reliability," ASME 2008 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Brooklyn, NY, Aug. 3–6, American Society of Mechanical Engineers, pp. 437–447.

[16] Irshad, L., Ahmed, S., Demirel, H. O., and Tumer, I., 2019, "Computational Functional Failure Analysis to Identify Human Errors During Early Design Stages," ASME J. Comput. Inf. Sci. Eng., **19**(3), p. 031005.

[17] Irshad, L., Demirel, H. O., Tumer, I. Y., and Brat, G., 2020, "Using Rio-Paris Flight 447 Crash to Assess Human Error and Failure Propagation Analysis Early in Design," ASCE-ASME J. Risk Uncertainty Eng. Syst. Part B: Mech. Eng., **6**(1), p. 011008.

[18] Irshad, L., Demirel, H. O., and Tumer, I. Y., 2020, "Automated Generation of Fault Scenarios to Assess Potential Human Errors and Functional Failures in Early Design Stages," ASME J. Comput. Inf. Sci. Eng., **20**(5), p. 051009.

[19] Irshad, L., Hulse, D., Demirel, H. O., Tumer, I. Y., and Jensen, D. C., 2020, "Introducing Likelihood of Occurrence and Expected Cost to Human Error and Functional Failure Reasoning Framework," ASME 2020 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, ASME Paper No. IDETC2020-22406.

[20] Williams, J., 1988, "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance," Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA, June 5–9, IEEE, pp. 436–450.

[21] Hulse, D., Hoyle, C., Goebel, K., and Tumer, I. Y., 2019, "Quantifying the Resilience-Informed Scenario Cost Sum: A Value-Driven Design Approach for Functional Hazard Assessment," ASME J. Mech. Des., **141**(2), p. 021403.

[22] Kurtoglu, T., and Tumer, I. Y., 2008, "A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems," ASME J. Mech. Des., **130**(5), p. 051401.

[23] Hirtz, J., Stone, R. B., McAdams, D. A., Szykman, S., and Wood, K. L., 2002, "A Functional Basis for Engineering Design: Reconciling and Evolving Previous Efforts," Res. Eng. Des., **13**(2), pp. 65–82.
[24] Aven, T., 2016, "Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation," Eur. J. Oper. Res., **253**(1), pp. 1–13.
[25] Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J., and Railsback, J., 2002, "Fault Tree Handbook With Aerospace Applications," Technical Report, NASA.
[26] Kapur, K. C., and Pecht, M., 2014, *Reliability Engineering*, Wiley, Hoboken, New Jersey.
[27] Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., and O'Reilly, P., 2005, *The Spar-h Human Reliability Analysis Method*, US Nuclear Regulatory Commission, Washington, DC, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/index.html#pub-info
[28] Kirwan, B., and Gibson, H., 2007, "CARA: A Human Reliability Assessment Tool for Air Traffic Safety Management – Technical Basis and Preliminary Architecture," *The Safety of Systems*, F. Redmill and T. Anderson, eds., Springer, London, pp. 197–214.
[29] Kirwan, B., Gibson, H., Kennedy, R., Edmunds, J., Cooksley, G., and Umbers, I., 2004, "Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool," *Probabilistic Safety Assessment and Management*, C. Spitzer, U. Schmocker, and V. N. Dang, eds., Springer, London, pp. 1206–1211.
[30] Gibson, W., Mills, A., Smith, S., and Kirwan, B., 2013, "Railway Action Reliability Assessment, a Railway-Specific Approach to Human Error Quantification," Proceedings of the Australian System Safety Conference, Adelaide, SA, Australia, May 22–24, Vol. 145, pp. 3–8.
[31] Akyuz, E., Celik, M., and Cebi, S., 2016, "A Phase of Comprehensive Research to Determine Marine-specific EPC Values in Human Error Assessment and Reduction Technique," Saf. Sci., **87**, pp. 63–75.
[32] O'Halloran, B. M., Hoyle, C., Tumer, I. Y., and Stone, R. B., 2019, "The Early Design Reliability Prediction Method," Res. Eng. Des., **30**(4), pp. 489–508.
[33] Rhee, S. J., and Ishii, K., 2003, "Using Cost Based FMEA to Enhance Reliability and Serviceability," Adv. Eng. Inf., **17**(3–4), pp. 179–188.
[34] Kmenta, S., and Ishii, K., 2004, "Scenario-Based Failure Modes and Effects Analysis Using Expected Cost," ASME J. Mech. Des., **126**(6), pp. 1027–1035.
[35] von Ahsen, A., 2008, "Cost-Oriented Failure Mode and Effects Analysis," Int. J. Qual. Reliab. Manage., **25**(5), pp. 466–476.
[36] Yodo, N., and Wang, P., 2016, "Engineering Resilience Quantification and System Design Implications: A Literature Survey," ASME J. Mech. Des., **138**(11), p. 111408.
[37] Miller-Hooks, E., Zhang, X., and Faturechi, R., 2012, "Measuring and Maximizing Resilience of Freight Transportation Networks," Comput. Oper. Res., **39**(7), pp. 1633–1643.
[38] MacKenzie, C. A., and Hu, C., 2019, "Decision Making Under Uncertainty for Design of Resilient Engineered Systems," Reliab. Eng. Syst. Saf., **192**, p. 106171.
[39] Hulse, D., Hoyle, C., Goebel, K., and Tumer, I. Y., 2018, "Optimizing Function-Based Fault Propagation Model Resilience Using Expected Cost Scoring," ASME 2018 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Quebec City, Quebec, Canada, Aug. 26–29, American Society of Mechanical Engineers, p. V02AT03A052.
[40] U.S. Department of Transportation, 2013, "Revised Departmental Guidance 2013: Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses," Washington, DC.
[41] Giudici, P., Givens, G. H., and Mallick, B. K., 2013, *Wiley Series in Computational Statistics*, Wiley Online Library, Hoboken, NJ.
[42] Quanterion Solutions Incorporated, 2016, *Nonelectronic Parts Reliability Data 2016*, Reliability Analysis Center, Rome, NY.
[43] Quanterion Solutions Incorporated, 2014, *Electronic Parts Reliability Data 2014*, Reliability Analysis Center, Rome, NY.
[44] Quanterion Solutions Incorporated, 2016, *Failure Mode/Mechanism Distributions*, Reliability Analysis Center, Rome, NY.
[45] O'Halloran, B. M., Stone, R. B., and Tumer, I. Y., 2012, "A Failure Modes and Mechanisms Naming Taxonomy," 2012 Proceedings Annual Reliability and Maintainability Symposium, Reno, NV, Jan. 23–26, IEEE, pp. 1–6.
[46] Hofer, E., Kloos, M., Krzykacz-Hausmann, B., Peschke, J., and Woltereck, M., 2002, "An Approximate Epistemic Uncertainty Analysis Approach in the Presence of Epistemic and Aleatory Uncertainties," Reliab. Eng. Syst. Saf., **77**(3), pp. 229–238.
[47] Cojazzi, G., 1996, "The Dylam Approach for the Dynamic Reliability Analysis of Systems," Reliab. Eng. Syst. Saf., **52**(3), pp. 279–296.
[48] Harris, D., Stanton, N. A., Marshall, A., Young, M. S., Demagalski, J., and Salmon, P., 2005, "Using Sherpa to Predict Design-Induced Error on the Flight Deck," Aerosp. Sci. Technol., **9**(6), pp. 525–532.
[49] Stanton, N. A., 2014, "Representing Distributed Cognition in Complex Systems: How a Submarine Returns to Periscope Depth," Ergonomics, **57**(3), pp. 403–418.
[50] Denson, W., Chandler, G., Crowell, W., Clark, A., and Jaworski, P., 1994, "Nonelectronic Parts Reliability Data – 1995," Technical Report NPRD-95, Reliability Analysis Center, Rome, NY.
[51] Crowell, W., Denson, W., Jaworski, P., and Mahar, D., 1997, "Failure Mode/Mechanism Distributions 1997," Technical Report FMD-97, Reliability Analysis Center, Rome, NY.
[52] Sobol, I. M., 2001, "Global Sensitivity Indices for Nonlinear Mathematical Models and Their Monte Carlo Estimates," Math. Comput. Simul., **55**(1–3), pp. 271–280.
[53] Saltelli, A., 2002, "Making Best Use of Model Evaluations to Compute Sensitivity Indices," Comput. Phys. Commun., **145**(2), pp. 280–297.
[54] Aven, T., and Flage, R., 2009, "Use of Decision Criteria Based on Expected Values to Support Decision-Making in a Production Assurance and Safety Setting," Reliab. Eng. Syst. Saf., **94**(9), pp. 1491–1498.
[55] Wright, M. K., Stokes, L., and Dyer, J. S., 1994, "Reliability and Coherence of Causal, Diagnostic, and Joint Subjective Probabilities," Dec. Sci., **25**(5–6), pp. 691–709.
[56] Hulse, D., Hoyle, C., Tumer, I. Y., and Goebel, K., 2019, "Decomposing Incentives for Early Resilient Design: Method and Validation," ASME 2019 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Anaheim, CA, Aug. 18–21, American Society of Mechanical Engineers, p. V02BT03A015.
[57] Kattakuri, V., and Panchal, J. H., 2019, "Spacecraft Failure Analysis From the Perspective of Design Decision-Making," ASME 2019 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Anaheim, CA, Aug. 18–21, American Society of Mechanical Engineers, p. V001T02A068.
[58] Kreye, M. E., Goh, Y. M., and Newnes, L. B., 2011, "Manifestation of Uncertainty-A Classification," DS 68-6: Proceedings of the 18th International Conference on Engineering Design (ICED 11), Impacting Society through Engineering Design, Vol. 6: Design Information and Knowledge, Lyngby/Copenhagen, Denmark, Aug. 15–19, 2011.
[59] Castiglia, F., Giardina, M., and Tomarchio, E., 2010, "Risk Analysis Using Fuzzy Set Theory of the Accidental Exposure of Medical Staff During Brachytherapy Procedures," J. Radiol. Prot., **30**(1), p. 49.