A Computational Framework for Prioritization of Events in Fault Tree Analysis Under Interval-Valued Probabilities

Antti Toppila and Ahti Salo

Abstract—In probabilistic safety assessment (PSA), the assessed events can be prioritized using risk importance measures, which are functions of the events’ failure probabilities. These probabilities can be uncertain, and consequently the resulting prioritization can be uncertain too. In this paper, we present a framework for computing the impacts of this uncertainty, which is modeled by interval-valued probabilities that establish lower and upper bounds, within which the probability may vary. Specifically, we make pairwise comparisons between events so that an event is said to dominate another if its risk importance measure is at least as high for all event probabilities that are within their respective intervals, and strictly higher for some probabilities. The dominance relations establish a partial order which can be visualized as a directed acyclic graph. We illustrate our method by analyzing the fault tree that represents the residual heat removal system of a nuclear reactor. The results for this fault tree with 31 events and 147 minimal cut sets was solved in seconds using a tailored algorithm. Theoretical properties of the algorithm suggest that much larger models can still be solved in reasonable time.

Index Terms—Epistemic uncertainty, fault tree analysis, interval-valued probability, prioritization, probabilistic safety assessment.

I. INTRODUCTION

In applications of Probabilistic Safety Assessment (PSA), the events that impact the safety of the system (e.g. component failures or accidents) can be prioritized using fault tree analysis. This prioritization is typically based on risk importance measures which map the events’ failure probabilities to numerical values that reflect the importance of these events. Examples of widely employed risk importance measures include the Fussell-Vesely measure, and the Birnbaum measure [1], [2].

Typically, the event probabilities are not known with certainty. Rather, they are estimated using approaches such as statistical analyses of measurements, computational simulations, or expert assessments, which all involve uncertainties [3], [4]. As a result, there is epistemic uncertainty about event probabilities [1]. It therefore follows that, when the risk importance measures are computed using these uncertain probability estimates, the numerical values of these measures are impacted by this epistemic uncertainty. Indeed, epistemic uncertainty can significantly influence the results and priorities based on risk importance measures. In this spirit, Cheok et al. [1] state that

“(Risk) Importance analyses are only as credible as the logic model upon which they are based. Furthermore, whatever approach is used, [risk] importance measures on their own cannot be used without a demonstration that the results are robust with respect to a variety of uncertainties in the model.”

Thinking about the robustness of risk importance measures with respect to uncertainties has motivated the development of many methods that help analyze and manage the impacts of these uncertainties [1], [2], [5]–[8]. These methods can be divided into probabilistic, and non-probabilistic methods. Probabilistic method rely on the distribution of the probability estimates, wherefore they can be implemented in the analysis of complex models using Monte Carlo simulation [2], [7], [9], [10]. Non-probabilistic methods such as interval-probabilities [11], fuzzy probabilities [12], coherent lower and upper probabilities [13], imprecise reliability [14], and Dempster-Shafer theory [15], [16], typically use interval arithmetic, rules, or optimization for propagating uncertainties.

In this paper, we develop a computational framework for analyzing the impact of epistemic uncertainty on the prioritization induced by risk importance measures. Our framework is based on lower, and upper bounds that define intervals within
which the probabilities vary. We do not ascribe a specific interpretation to this interval; thus, the analyst may choose to interpret the probabilities as interval-probabilities, imprecise probabilities, alpha-cuts of fuzzy probabilities, bounds for sensitivity analysis, or any other method that models uncertainty with interval-valued probabilities.

Conclusions in our method are based on the analysis of the absolute difference between the risk importance measures for pairs of events. That is, if this difference is non-negative for all probabilities within the intervals, and strictly greater for some such probabilities, then the relative priority for the two events does not depend on what value within the intervals the probabilities have. This condition is the case, for instance, if the priority of event A is at least as high as that of event B for all probability intervals that lie within their respective intervals. Moreover, if these intervals also contain some probabilities such that the priority of event A is strictly higher than that of B, we say that event A dominates event B.

If the probability intervals become narrower, for instance due to the elicitation of more precise probability estimates, more events tend to become dominated by other events, and those events that have been dominated will stay dominated. Ultimately, if all event probabilities are specified using crisp numbers, the probability intervals become singleton sets, and corresponding risk importance measures, too, become crisp numbers. In this case, the dominance relation will become a total order (with a possibility of ties) which suggests the same priorities as what would be established by sorting the events according to their risk importance measures. Thus, narrowing the intervals, which can be interpreted as the reduction of epistemic uncertainty, typically leads to more conclusive results about the prioritization of events.

Our method is developed in the context of fault tree analysis in which events can be prioritized based on risk importance measures [17]. To compute the dominance relations for interval-valued probabilities efficiently, we provide a tailored algorithm [18]. The dominance relations are presented as a directed graph in which nodes correspond to events, and in which directed arcs between nodes indicate those pairs of events for which dominance does hold. The resulting graph shows the overall impact of epistemic uncertainty on the prioritization of events, when compared to the prioritization yielded by ranking the events based on their importance measure computed with crisp probabilities.

We illustrate our method by analyzing a fault tree that represents the residual heat removal system of a nuclear power plant. This fault tree has 31 basic events, and 147 minimal cut sets. The epistemic uncertainty about each basic event is characterized by an interval with a plausible width. We employ the Fussell-Vesely risk importance measure, and compute the resulting priorities using the rare event approximation under the Fussell-Vesely risk importance measure, and compute the resulting distribution over rankings with various approaches, such as by examining the derivatives of importance measures [23], by running simulation studies [24], [25], and by uncertainty importance measures [6], [8], [26]–[28]. These methods provide insights into (i) how sensitive the risk importance measures are to changes in the numerical values of probabilities, and (ii) which uncertainties impact the uncertainty measures of system reliability most [8].

A framework for uncertainty analysis based on imprecise probability is provided by Limbourg et al. [29] who use Dempster-Shafer theory to propagate uncertainties in fault trees. They also provide an open source software package for performing the computations, which have been used by Duy et al. [30], [31] for computing bounds on traditional risk importance measures. Similar results are presented by [32], who use affine interval arithmetic to propagate the uncertainty to the importance measures.

Modarres [10] has developed a probabilistic approach for assessing the sensitivity of the prioritization that is implied by a risk importance measure. In this approach, which has been developed further by Zio [2], and by Baraldi et al. [7], the risk importance measures $I_i$ of events $i = 1, \ldots, n$ are treated as random variables so that the ranking $R_i \in \{1, \ldots, n\}$ of each component is a random variable too. These random rankings are transformed to non-random decision recommendations using a threshold rule. Specifically, if $Pr\{R_i > R_j\} > \alpha$, where $\alpha$ is a threshold level, then event $i$ should have a higher priority than event $j$. For example, with $\alpha = 0.5$, this rule states that the priority of event $i$ should be higher than that of event $j$ if it is more probable than not that the risk importance measure of $i$ is higher than that of $j$. Overall, the resulting distributions over rankings convey information about how sensitive the priorities are. For instance, if there is an event which has the highest ranking with
probability one, then it is incontestable that this event should have the highest priority. On the other hand, if the probability is evenly distributed across all rankings, then the corresponding priorities remain uncertain.

One important observation, and also a source of concern, is that, for probabilities which are close to the threshold $\alpha$, the ordering given by this metric can be cyclic. In other words, it is possible that $\Pr\{R_i > R_j\} > \alpha$, $\Pr\{R_j > R_k\} > \alpha$, and $\Pr\{R_k > R_i\} > \alpha$, suggesting that $i$ is more important than $j$, which is more important than $k$, which in turn is more important than $i$.

III. METHODOLOGICAL DEVELOPMENT

Consider a system whose success or failure depends on $n$ statistically independent events $e_1, \ldots, e_n$. Let $Z = \{Z_1, \ldots, Z_n\}$ be the state vector of events such that $Z_i = 1$ if event $e_i$ has occurred, and $Z_i = 0$ if its complement event $e_i^c$ has occurred. Then the state of the system $\phi$ is a binary function of $Z$, that is $\phi = \phi(Z)$, where the values $\phi = 1$ and $\phi = 0$ indicate success, and failure of the system, respectively. The system is characterized by its prime implicants for success-failure, which are the minimal joint events that guarantee the success-failure of the system, and consist of events $e_i$ and their complements. For a coherent system, the prime implicants for failure correspond to the minimal cut sets of the system. Prime implicants for success correspond to the minimal paths of the system.

The reliability, and unreliability of the system are given by $h = \Pr\{\phi = 1\}$, and $Q = \Pr\{\phi = 0\}$, respectively; where $\Pr\{\cdot\}$ is the probability of an event. Let $p = (p_1, \ldots, p_n)$, where $p_i = \Pr\{e_i\}$, $i = 1, \ldots, n$. Then, as shown by Borgonovo [23], both $h$ and $Q$ are multilinear functions of the vector $p$.

Definition 1: A function $g : \mathbb{R}^n \rightarrow \mathbb{R}$ is multilinear if it is of the form

$$g(x) = g(x_1, \ldots, x_n) = \sum_{J \subseteq \{1, \ldots, n\}} \alpha_J \prod_{i \in J} x_i,$$

where $\alpha_J \in \mathbb{R}$ are the multilinear coefficients of the function.

Remark 1: We define $\prod_{i \in \emptyset} x_i = 1$ so that $\alpha_{\emptyset}$ is the coefficient associated with the constant term.

In fault tree analysis, the events $e_i$ are commonly prioritized by using risk importance measures such as Fussell-Vesely (FV), Birnbaum (B), or risk reduction worth [17], [33]. Many of these measures can be expressed using scaled differences of conditional (un)reliabilities. For instance, the FV measure for a failure event $e_i$ in a coherent system can be defined as

$$\text{FV}(e_i) = \text{FV}(p, e_i) = \frac{Q(p) - Q(p e_i^c)}{Q(p)}, \quad Q(p) \neq 0.$$

Here, the numerator is the difference of the unconditional and conditional unreliabilities, which difference is then scaled by the unconditional unreliability. Because conditional unreliabilities, too, are multilinear functions of the components of the vector $p$, these unscaled differences in the numerator are multilinear in $p$. Consequently, to determine whether or not the risk importance of event $e_i$ is higher than that of event $e_j$, it is sufficient to check the sign of the multilinear function, which is the difference of the two numerators. For instance, to check if the FV measure of $e_i$ is higher than the FV measure of $e_j$, one needs to check whether or not the multilinear function

$$g_{e_i \Rightarrow e_j}(x) = Q(x) - Q(x e_j^c) - (Q(x) - Q(x e_i^c))$$

is positive at $x = p$. Thus, it follows that sensitivity analyses for the prioritizations implied by widely used risk importance measures can be carried out by analyzing multilinear functions.

A. Interval-Valued Probabilities

We model uncertainties about event probabilities using feasible sets of probabilities. Formally, the probabilities $\{p_1, \ldots, p_n\}$ are assumed to belong to the set $\mathcal{P}_F \subseteq \mathbb{R}^n$, where

$$\mathcal{P}_F^0 = \{ (p_1, \ldots, p_n) \in \mathbb{R}^n : 0 \leq p_i \leq 1 \, \forall i \in \{1, \ldots, n\} \}.$$ 

This approach is a generalization of standard probability theory, in which $\mathcal{P}_F$ is a point in $\mathcal{P}_F^0$.

The size of the set $\mathcal{P}_F$ reflects knowledge about the probabilities; that is, the smaller the feasible set $\mathcal{P}_F$, the more precisely the probabilities are characterized. In what follows, we consider feasible sets $\mathcal{P}_F$ that are formed by constraints of the form $p_i \leq p_i \leq \bar{p}_i$, where $p_i$ and $\bar{p}_i$ are the lower, and upper bounds of the probability of $\Pr\{e_i\}$. These bounds can be established by employing methods in imprecise probability elicitation [34], [35]. These intervals can also be formed by employing the confidence intervals for the estimators of the probabilities $p_i$ which can be regarded as sensitivity bounds for the probabilities that are used in sensitivity analysis [24].

B. Dominance

We now formally define dominance as follows.

Definition 2: Event $e_i$ dominates event $e_j$ based on the risk importance measure $I$, denoted as $e_i \succ_I e_j$, iff

(i) $I(p, e_i) \geq I(p, e_j)$ for all $p \in \mathcal{P}_F$, and
(ii) $I(p, e_i) > I(p, e_j)$ for some $p \in \mathcal{P}_F$, where $I(p, e_i)$ is the risk importance measure of event $e_i$ evaluated with probabilities $p$. To simplify notation, we omit the subscript, and simply denote dominance as $e_i \succ e_j$, when the risk importance measure is clear from the context, or when discussing any risk importance measure.

We next consider risk importance measures $I$ such that the difference between the risk importance measures that are associated with events $e_i$ and $e_j$ can be characterized by a multilinear function $g_{e_i \Rightarrow e_j}(p)$. As discussed above, such multilinear functions exist for all of the most widely used risk importance measures [17]. In these cases, $e_i \succ_I e_j$, iff

(i) $g_{e_i \Rightarrow e_j}(p) \geq 0$ for all $p \in \mathcal{P}_F$, and
(ii) $g_{e_i \Rightarrow e_j}(p) > 0$ for some $p \in \mathcal{P}_F$.

Dominance is a conservative approach for comparing the risk importance of events. If an ordinary fault tree analysis were to be conducted by using event probabilities that belong to the intervals, a dominated event would not have a higher risk importance than an event that dominates it, and for some probabilities within the intervals it would have a strictly lower risk importance.

Definition 2 implies that the dominance relation is irreflexive, asymmetric, and transitive. Irreflexiveness implies that $e_i \not\succ e_i$.
\( e_i \forall i, \) so that no event dominates itself. Asymmetry gives \( e_i > e_j \Rightarrow e_j \not> e_i, \forall i \neq j. \) Thus, if dominance is established, then the reverse dominance relation cannot hold. Transitivity implies that, if \( e_i > e_j, \) and \( e_j > e_k, \) then also \( e_i > e_k \forall i, j, k. \)

These three properties of the dominance relation can offer significant computational advantages because it may be possible to infer many dominance relations without determining the corresponding multilinear function \( g. \) In the worst case, however, all pairs of distinct events may have to be checked. For instance, if no event dominates any other, then asymmetry and transitivity relations do not reduce the number of required checks.

### C. Solving Dominance Through Multilinear Optimization

Because the function \( g_{e_i \geq e_j} \) is multilinear, the determination of dominance in Definition 2 can be done by checking the sign of a multilinear function over a hyperrectangle. This problem is known to be NP-hard [36], [37]. Even if this worst case computation time can cause computational challenges, algorithms to solve realistic problem instances have been developed [38]–[41].

Our algorithm makes use of a well-known result from multilinear programming.

**Lemma 1:** The extreme values of a multilinear function \( f : R \rightarrow R, \) where \( R \) is a hyperrectangle in \( \mathbb{R}^n, \) are attained at the vertices of \( R. \)

**Proof:** A proof can be found in [42], Corollary 2.3. Here we give only an outline of the proof. Multilinear functions do not have local optima unless all of their multilinear coefficients are zero (with exception of the term \( a_0 \) that is related to the constant part of the function). The proof of this property is technical, and can be found in [42] Theorem 2.2. The property implies that the extreme values must be on the boundaries of the feasible set \( \mathcal{P}_F \) (this result is similar to [43], errata [44] Proposition 2.1). On the boundary of a hyperrectangle, at least one variable is at its lower or upper bound. Let this variable be \( x_1, \) and consider the multilinear function that is obtained by substituting this optimal bound to \( f(x), \) that is \( g(x_2, \ldots, x_n) = f(x^*, x_2, \ldots, x_n), \) where \( x^* \) is either the lower or upper bound of \( x_1 \) in the hyperrectangle \( R. \) Function \( g \) is multilinear, so we may continue recursively to set another variable at its lower or upper bound, because we can again use the property that the extreme values are attained on the boundary. After \( n \) iterations, we have evaluated \( f(x) \) at a point which is optimal, and where every variable is either at its lower or upper bound. Thus the extreme values of \( f(x) \) are attained at the vertices of \( R. \)

By Lemma 1, the dominance condition for interval-valued probabilities, defined by lower and upper bounds, holds iff the multilinear function \( f : H \rightarrow R \) is (i) non-negative at all the vertices of the bounded hyperrectangle \( H \subset \mathbb{R}^n, \) and (ii) strictly positive at some vertex. The vertices can be evaluated by a branch and bound algorithm in which branches are created sequentially by setting components of the probability vector at their lower or upper bounds. Specifically, a branch for variable \( p_i \) is created by considering the sets \( H^- = \{ p_1, \ldots, p_i - 1, p_i + 1, \ldots, p_n \} \subseteq H \}, \) and \( H^+ = \{ p_1, \ldots, p_i - 1, p_i + 1, \ldots, p_n \} \subseteq H \}. \)

Then the multilinear functions \( g^- : (p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n) \mapsto f(p_1, \ldots, p_{i-1}, p_i + 1, \ldots, p_n), \) and \( g^+ : (p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n) \mapsto f(p_1, \ldots, p_{i-1}, p_i - 1, \ldots, p_n) \) coincide with \( f(p) \) on the sets \( H^-, \) and \( H^+, \) respectively. Because there is a finite number of elements in the probability vector, this algorithm terminates after a finite number of branches has been evaluated.

To avoid the need to create all branches explicitly, we note that \( f(p) \) can be expressed as a sum of products in the form \( f(p) = \sum_{J \subseteq \{1, \ldots, n\}} \alpha_J \prod_{j \in J} p_j \) where \( \alpha_J \) are constants. Arranging the terms leads to \( f(p) = a_0 + f^+(p) + f^-(p), \) where \( f^+(p) \) and \( f^-(p) \) denote the sums of product terms of \( f(p) \) with positive, and negative coefficients \( \alpha_J, \) respectively. Then, a lower bound for the value of \( f(p) \) is given by \( a_0 + f^+(p) + f^-(p), \) where \( p = (p_1, \ldots, p_n), \) and \( \bar{p} = (p_1, \ldots, p_n). \) If this bound is non-negative, then \( f(p) \) is non-negative and no more branching is needed. Similarly, an upper bound for \( f(p) \) is given by \( a_0 + f^+(p) + f^-(p). \) If this bound is negative, then \( f(p) \) cannot be non-negative, and no more branching is needed.

Branches can also be bounded by factoring \( f(p) \) in the form \( f(p) = g_f^+(p^-)p_i + g_f^-(p^-) \), where \( p^- = (p_1, \ldots, p_i - 1, p_{i+1}, \ldots, p_n), \) \( g_f^+(p^-) \) contains all product terms of \( f(p) \) that include \( p_i \) (where \( p_i \) has been factored out), and \( g_f^-(p^-) \) contains the remaining terms. This definition implies that \( g_f^+(p^-) \) is a multilinear expression which has at least one variable less than \( f(p). \) If it is non-negative, \( p_i \) should be at its lower bound to minimize \( f(p); \) and if it is negative, \( p_i \) should be at its upper bound. Establishing the non-negativity of \( g_f^+(p^-) \) is therefore a problem of the same type as the original one, except that there is at least one variable less to be considered, which permits a recursive solution scheme.

The branching and bounding rules discussed above are exploited by our algorithm in Table I, which resolves the sign of a multilinear function in a hyperrectangle. This algorithm is guaranteed to terminate after a finite number of steps, and returns the value TRUE if the value of the multilinear function is non-negative in the hyperrectangle, and FALSE otherwise.

In coherent systems, the unreliability is an increasing function in the failure probability. This property can be used in the initialization phase of our algorithm for eliminating one branching phase (a similar approach has been used in [12], pp. 23–26). Take, for instance, the Fussell-Vesely dominance, which can be characterized by \( g_{e_i \leq e_j} \) (\( p \)) \( = Q(p|e_i^c) - Q(p|e_j^c) \). Because the multilinear function \( Q(p|e_i^c) \) does not depend on \( p_i \), and \( Q(p|e_j^c) \) does not depend on \( p_i \), it is possible to set \( p_i \) at its lower bound, and \( p_j \) at its upper bound, when seeking the minimum value of \( g_{e_i \leq e_j} \) (\( p \)). This same principle can be extended to any risk importance measure that uses conditioning on one event (or its complement), and is monotone with respect to the event probabilities. For instance, consider the Birnbaum (B) risk importance measure, which is defined as

\[
B(p, e_i) = Q(p|e_i) - Q(p|e_i^c) - Q\{p|e_j^c\}.
\]

In coherent systems, \( B(p, e_i) \) is non-decreasing with respect to \( p. \) Because the unreliability terms are conditioned on event \( i \) or its complement, \( B(p, e_i) \) does not depend on \( p_i. \) Thus, the multilinear function \( Q(p|e_i) - Q(p|e_i^c) - Q\{p|e_j^c\} \) that characterizes Birnbaum dominance between events \( e_i \) and \( e_j \) can be expressed recursively to set another variable at its lower or upper bound.
TABLE I

ALGORITHM: NON-NEGATIVITY OF MULTILINEAR FUNCTION

Input Lower, and upper bounds \(0 < p \leq \bar{p}\); and multilinear function \(f(p)\).
Output Boolean \(\text{TRUE}\) if \(f(p)\) is non-negative when \(p < p \leq \bar{p}\), and \(\text{FALSE}\) otherwise.

1: Arrange terms of \(f(p)\) into \(a_k, f^+(p), f^-(p)\), and \(f(p)\).
2: if \(a_k + f^+(p) - f^-(\bar{p}) \geq 0\) then
3: return \(\text{TRUE}\).

4: else if \(a_k + f^+(\bar{p}) - f^-(p) < 0\) then
5: return \(\text{FALSE}\).
6: Select any variable \(p_i\) for branching.
7: Define \(\bar{P}^{-1} = (p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n)\) and \(\bar{P}^{-1} = (\bar{p}_1, \ldots, \bar{p}_{i-1}, \bar{p}_{i+1}, \ldots, \bar{p}_n)\).
8: Define \(g^{-1} = f(p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n)\) and \(g^{-1} = f(\bar{p}_1, \ldots, \bar{p}_{i-1}, \bar{p}_{i+1}, \ldots, \bar{p}_n)\).
9: Factor \(f(p)\) with regard to \(p_i\) to get \(g^{-1} = f(p)\) or \(g^{-1} = f(p)\).
10: if Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\) then
11: return Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\).
12: else if Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\) then
13: return Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\).
14: else
15: return Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\) ∧ Algorithm\((\bar{P}^{-1}, \bar{P}^{-1}, g^{-1}(p))\).

\(e_j\) is such that \(p_j\) can be set at its lower bound, and \(p_i\) at its upper bound. However, this method may not apply to all widely used risk importance measures. For instance, the Critical Importance risk importance measure, which is defined as

\[
CI(p, e_i) = \frac{B(e_i)}{Q(p)}
\]

depends on \(p_i\). Thus the multilinear function that characterizes Critical Importance dominance is \((Q(p)e_i) - Q(p|e_i)^2)e_j\). However, it is possible for the multilinear function \(Q(p, e_i) - Q(p\mid e_i)\) to have both positive and negative values, wherefore it is not possible to set \(p_i\) at either bound to check dominance. Thus, in the case of Critical Importance, also the variable \(p_i\) must be branched.

If our algorithm returns \(\text{TRUE}\), then to prove dominance, the condition \(g(p) > 0\) for some \(p \in \mathcal{P}_F\) must also be checked. This can be done using the following proposition.

**Proposition 1:** Let \(g(p): \mathbb{R}^n \to \mathbb{R}\) be a multilinear function and \(\mathcal{P}_F\) a hyperrectangle in \(\mathbb{R}^n\) defined by lower and upper bounds \(p_u\) and \(p_l\), \(p_l \leq \bar{p} < \bar{p} = 1, \ldots, n\), such that \(g(p) \geq 0\) for all \(p \in \mathcal{P}_F\). If the multilinear coefficients of \(g\) are non-zero, then \(g(p) > 0\) for some \(p \in \mathcal{P}_F\).

**Proof:** Assume contrary to the claim that \(g(p) = 0\) for all \(p \in \mathcal{P}_F\). Multilinear functions do not have local optima unless all of their multilinear coefficients are zero (with exception of the term \(a_k\) that is related to the constant part of the function) ([42] Theorem 2.2). If \(a_k > 0\), and the other multilinear coefficients are zero, then the results follows. Otherwise, the value of \(g\) cannot remain constant in the hyperrectangle \(\mathcal{P}_F\), and hence \(g\), which is non-negative, is bound to be positive for some \(p \in \mathcal{P}_F\).

By Proposition 1, dominance can be shown to hold by verifying only the condition \(g(p) \geq 0\) if none of the intervals are singletons. Otherwise, the second condition for dominance, that is \(g(p) > 0\) for some \(p \in \mathcal{P}_F\), may not hold. However, the variables that are constrained to be in singleton sets have unique values, which can be substituted into the function \(g\). This substitution results in a new multilinear function \(g'\), which depends only on variables that are constrained in non-singleton sets, and Proposition 1 applies to \(g'\), which is equivalent to \(g\). Thus by considering \(g'\), the condition \(g(p) > 0\) for some \(p \in \mathcal{P}_F\) can be checked.

With crisp probabilities, the risk importance measures have crisp values, and the events can be sorted in an increasing order with respect to their importance. Then, if the value of the risk importance of event \(e_i\) is strictly greater than the risk importance of event \(e_j\), then \(e_i \not< e_j\). Because in typical applications the crisp values of risk importance measures are different, many cases of dominance can be ruled out based on this information. For instance, if the events \(e_1, e_2, \ldots, e_n\) are ordered for some \(p \in \mathcal{P}_F\) such that \(g(e_i, e_j) > 0\), then \(e_i \not< e_j\) for some \(p \in \mathcal{P}_F\), then \(e_i \not< e_j\) for some \(p \in \mathcal{P}_F\). This condition, together with irreflexiveness, reduces the number of required checks from \(n^2\) to \(\sum_{i=1}^{n-1} i = (n^2 - n)/2\).

D. Visualization of Dominance Structures

We define a dominance matrix \(D\) such that \(D_{ij} = 1\) if \(e_i \not< e_j\), and \(D_{ij} = 0\) if \(e_i \not< e_j\). This matrix can be interpreted as a node-arc incidence graph in which each event \(e_i\) is a node, and in which there is a directed arc \((i, j)\) from \(e_i\) to \(e_j\) if \(D_{ij} = 1\). The number of arcs in the graph can be reduced using transitivity. Specifically, the arc \((i, k)\) is implied by other arcs if there exists a path from \(i\) to \(k\), that is, a sequence of \(n\) arcs \((i, j_1), (j_1, j_2), \ldots, (j_{n-1}, j_n), (j_n, k)\). Because the graph represents a partial order, this reduction of arcs leads to a unique acyclic graph \(G\).

One intuitive way to visualize the graph \(G\) is to start with no-dominated events which have no arcs at all, or which have outgoing arcs only. Following this intuition, it would be instructive to draw several layers of nodes such that each layer would be dominated by the nodes on the layer just above it. However, this drawing is not possible. For instance, if there are two events which are dominated by the same event, and if there exists some other event which dominates only one of these two events, then it is not possible to place the nodes in layers. In general, with partial orders, it is not always possible to assign unique importance classes to each node. Further discussion on how to place nodes in layers can be found in textbooks on graph visualization. We have used the LayeredGraphPlot function in Wolfram Mathematica\(^1\) to produce our visualizations. Even other software tools can be applied, such as the open source software Graphviz.\(^2\)

E. Approximative Formulas for Dominance

Fault trees are often coherent so that their structure can be described using minimal cut sets. Then using these minimal cut sets, the reliability function \(Q(p)\) can be derived using standard techniques (e.g. [45]). However, evaluation of the reliability


TABLE II
MINIMAL CUT SETS GROUPED FOR RESOLVING THE DOMINANCE $e_1 \succ_F V e_2$

<table>
<thead>
<tr>
<th>Both</th>
<th>Neither</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3 &amp; 4/5 &amp; 6</td>
<td>2/3 &amp; 4/7</td>
</tr>
<tr>
<td>1/4 &amp; 3/5 &amp; 6</td>
<td>2/4 &amp; 4/7</td>
</tr>
<tr>
<td>1, not 5</td>
<td>3, not 1</td>
</tr>
<tr>
<td>1/3 &amp; 4/5 &amp; 6</td>
<td>2/3 &amp; 5/6</td>
</tr>
<tr>
<td>1/4 &amp; 3/5 &amp; 6</td>
<td>2/4 &amp; 5/6</td>
</tr>
</tbody>
</table>

function of fault trees with many events and a complex structure can be computationally expensive. Because our method relies on evaluating the multilinear function several times, we provide an approximative method for computing the dominances.

In fault tree analysis, two simplifications are common. The events are assumed infrequent, wherefore the rare event approximation is appropriate, and they are also assumed statistically independent. Then the unreliability of a system can be approximated with $Q(p|e_k) \approx \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j$, where $C_j$ is the $j$th minimal cut set of the system, and $N_{cut}$ is the total number of these minimal cut sets. The conditional unreliability given event $e_k$ is therefore $Q(p|e_k) \approx \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j$, while the conditional unreliability given the complement event $e_k^c$ is given by $Q(p|e_k^c) \approx \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j$. Then, if $Q(p|e_k) > 0$ for all $p \in \mathcal{P}_F$, the possibility of the FV dominance relation $e_1 \succ_F V e_2$ can be checked from

$$\frac{Q(p) - Q(p|e_1)}{Q(p)} \geq \frac{Q(p) - Q(p|e_2)}{Q(p)} \iff Q(p|e_2) \geq Q(p|e_1)^c$$

$$\sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j - \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j \geq 0 \forall p \in \mathcal{P}_F,$$

where the inequality is strict for some $p \in \mathcal{P}_F$. Because the minimal cut sets in both sums are the same, there are many terms that cancel out. This result leads to the following condition for FV dominance.

$$\sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j - \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j \geq 0 \forall p \in \mathcal{P}_F,$$  \hspace{1cm} (1)

where the inequality is strict for some $p \in \mathcal{P}_F$. The Birnbaum (B) risk importance measure, defined as

$$B(e_i) = Q(p|e_i) - Q(p|e_i^c),$$

can also be used to derive dominance relations. That is, the Birnbaum dominance relation $e_1 \succ_B e_2$ is equivalent to

$$Q(p|e_1) - Q(p|e_2) \geq Q(p|e_1^c) - Q(p|e_2^c) \iff$$

$$\sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j - \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j \geq 0 \forall p \in \mathcal{P}_F,$$

with a strict inequality for some $p \in \mathcal{P}_F$. After canceling out terms, the Birnbaum dominance relation holds iff

$$\sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j - \sum_{i=1}^{N_{cut}} \prod_{j \in C_i} p_j \geq 0 \forall p \in \mathcal{P}_F,$$  \hspace{1cm} (2)

with a strict inequality for some $p \in \mathcal{P}_F$.

The left hand sides of (1) and (2) are multilinear functions, defined on the hyperrectangle that is specified by the lower, and upper bounds of the probabilities. Thus, these functions fall within the scope of Lemma 1, and our algorithm can be applied.

F. Example

Consider the coherent system which consists of seven statistically independent components $1, \ldots, 7$ as shown in Fig. 1. Let the failure probabilities be $p_i = p_{F1} \{e_i\}$, where $e_i$ is the event that component $i$ fails, and denote the unreliability of the system by $Q = Q(p)$. Because the system is coherent, its behavior is described by the minimal cut sets in Table II. Using these sets, standard techniques (e.g. [45], p. 27) can be applied to conclude that the unreliability of the system is given by the multilinear function $Q(p) = p_1p_2p_5p_6 + p_1p_5p_6p_9 - p_1p_2p_3p_5p_6 + p_1p_4p_5p_6 + p_2p_3p_5p_6 - p_1p_2p_5p_6 - p_2p_5p_6p_9 + p_2p_2p_4p_5p_6 + p_1p_4p_5p_6 + p_1p_5p_6 + p_2p_3p_7 - p_1p_2p_3p_7 + p_1p_4p_7 + p_2p_4p_7 - p_1p_2p_4p_7 - p_1p_2p_3p_7 + p_2p_2p_4p_7 + p_2p_4p_7p_9 - p_1p_2p_3p_7p_9 - p_1p_2p_4p_7p_9 + p_2p_2p_4p_7p_9p_9 - p_1p_2p_3p_7p_9p_9 - p_1p_2p_4p_7p_9p_9.

We analyze the system by using the FV measure. First, we consider the conventional prioritization, resulting from the use of crisp probabilities such that each component fails with probability 0.02. For these probabilities, the FV measures are, in decreasing order, such that $FV_7 \approx 0.98$ is the highest, followed by $FV_1 = FV_2 = FV_3 = FV_4 \approx 0.49$, and finally $FV_5 = FV_6 \approx 0.02$ (here, $FV_i$ is a shorthand notation for $FV(e_i)$). This ranking reflects the fact that, if component 7 is guaranteed not to fail, then the system will fail only if components 5 and 6 fail. But because these components are in parallel,
the unreliability of the system is low if component 7 does not fail, and consequently it has a high risk importance.

Now, assume that the probability estimates \( p_i \) are uncertain. We model these uncertainties by using interval-valued probabilities such that each probability is within the interval \([0.01, 0.03]\). These intervals contain the crisp estimates 0.02.

As shown earlier, Fussell-Vesely dominance \( e_i \succ \text{FV} \ e_j \) is equivalent to \( Q(p|e_i p) - Q(p|e_j p) \geq 0 \forall p \), where the inequality is strict for some \( p \). The conditional unreliability, conditioned on the event \( e_i \), is equivalent to substituting \( p_i = 0 \) in \( Q \). For instance, the relation \( e_1 \succ \text{FV} \ e_5 \) is equivalent to \(-p_2 p_3 p_5 p_6 - p_2 p_4 p_5 p_6 + p_2 p_3 p_4 p_5 p_6 + p_1 p_3 p_7 - p_1 p_2 p_5 p_7 + p_1 p_4 p_7 - p_1 p_3 p_4 p_7 - p_1 p_3 p_5 p_7 + p_1 p_5 p_7 - p_2 p_3 p_4 p_5 p_7 - p_2 p_3 p_4 p_5 p_7 \geq 0 \forall p \). Our algorithm gives the value \( \text{TRUE} \) for this function and probability set, which indicates that the difference between the FV measures of events \( e_1 \) and \( e_5 \) cannot be negative. Also, because \( e_1 \) and \( e_5 \) have different FV values for the crisp probability \( p_i = 0.02 \), we conclude that \( e_1 \succ \text{FV} \ e_5 \) holds.

Next we apply the approximative formula derived in (1) to determine whether \( e_1 \) dominates \( e_5 \). This calculation yields the inequality \( p_1 p_4 p_7 + p_1 p_4 p_7 - p_2 p_3 p_4 p_5 p_6 - p_2 p_3 p_5 p_6 \geq 0 \forall p \). Comparing to the exact formulation, all terms of high order are missing as a result of the rare event approximation. The reduction on the number of terms is quite substantial, but this does not affect the results. Using our algorithm on this function yields the same result as above. Again, either the case \( p_i = 0.02 \) or Proposition 1 can be used to conclude that \( e_1 \succ \text{FV} \ e_5 \) when using the approximate dominance formula as well.

Solving all the dominance relations with Algorithm 1 gives the dominance graph in Fig. 2. In this graph, \( e_7 \) dominates all other events, whereas events \( e_5 \) and \( e_6 \) are dominated by all other events. This result is in line with the prioritization suggested by crisp probabilities in which event \( e_7 \) was identified as the most important one, and \( e_5 \) and \( e_6 \) as least important.

To demonstrate the impact of uncertainty, we next compute the dominance graph with wider intervals which reflect greater uncertainty about the probability estimates. When the failure probabilities are such that \( \mathcal{P}_F = \{p \in \mathbb{R}^7 | 0.01 \leq p_i \leq 0.05 \} \), the dominances change so that only event 7 dominates events 5 and 6. No definitive priority is given among the remaining events because we can find feasible probabilities for which one event has higher risk importance than the other, and vice versa. For instance, for the feasible probabilities \( p_1 = 0.05, p_2 = 0.01, p_3 = 0.03, p_4 = 0.03, p_5 = 0.05, p_6 = 0.05, p_7 = 0.01 \), we have that \( FV(e_1) \approx 0.83 \), whereas \( FV(e_7) \approx 0.80 \), which shows that event 1, that was dominated by event 7 with the previous set of feasible probabilities, is no longer dominated by event 7.

IV. APPLICATION TO THE RESIDUAL HEAT REMOVAL SYSTEM OF A NUCLEAR REACTOR

We apply our method to analyze the fault tree that represents a residual heat removal system (RHR) of a nuclear reactor. The structure and failure probabilities of this fault tree are representative of existing reactors. The RHR fault tree has 31 events, and 147 minimal cut sets. Table III contains the crisp probabilities of the events, the numerical values of the Fussell-Vesely risk importance measures computed with crisp probabilities, and the lower and upper bound of the 90% confidence intervals. The events are sorted by the Fussell-Vesely measure column of this table. They are also labeled based on their ranking with regard to this measure.
The events’ crisp probabilities are in the range from 5.8 \times 10^{-2} to 1 \times 10^{-7}. These probabilities were estimated with standard PSA methods from the Risk Spectrum software (mean unavailability or failure probability per demand, depending on the event). Each failure probability is estimated with a standard reliability model such that the expected value of the estimated distribution is used as the numerical value for failure probability. The reliability models also give standard 90% confidence intervals for the probability estimates, which are employed as the lower and upper bounds on the probabilities.

Table IV contains the minimal cut sets of the system, as well as their crisp probabilities (for reference). The cut sets consist of one to three components, and each component typically belongs to 1–13 cut sets. The top event in the fault tree is the failure of the RHRS, which occurs with a crisp probability of 5.83 \times 10^{-3}.

The Fussell-Vesely and Birnbaum dominance matrices were determined by checking the sign of (1), (2). Using our algorithm, checking the non-negativity of the resulting functions, and checking that Proposition 1 is valid, lasted about 15 seconds with our Mathematica implementation of this algorithm on a regular laptop PC (Intel(R) Core(TM)2 Duo CPU T5870 @ 2.00GHz processor, and 4 GB RAM).

In the Fussell-Vesely dominance graph in Fig. 3, the first five events are non-dominated, and thus they should receive the highest priority. That events 1 and 5 should both be prioritized the highest may be considered counterintuitive, because $F_{V_1} = 0.57$, and $F_{V_2} = 0.06$, whereas their risk importance measures have almost a tenfold difference. However, because neither dominates the other, there exist probabilities within the intervals in Table III for which $F_{V_2} > F_{V_1}$. Thus, the uncertainties about the probabilities are large enough to reject a definitive priority between events 1 and 5.

Even if the layout of the graph would suggest that there are three classes of events that do not dominate each other, this is not the case. For instance, the non-dominated events 1–5 do not dominate all the other events. Event 1 dominates events 6–31; event 2 dominates events 10, 13, 14, 15, 19–31; event 3 dominates 12, 14, 15, 19–31; event 4 dominates 20, 22, 23–31; and event 5 dominates 20, 23–25, 27–31. The same argument applies to event 31, which is at the bottom of the graph. Even if it does not dominate any other event, it is still not dominated by all events (that is events 16, 17, 25–30). In fact, all events dominate, or are themselves dominated by, different sets of events.

An upper bound for the highest ranking \{1 = highest priority, 31 = lowest priority\} that an event may have is given by the number of events that dominate the event plus one. This result is true because, if an event is dominated by \(n\) other events, then these \(n\) events must be assigned a higher rank. Similarly, a lower bound is given by 31 minus the number of events that the event dominates. These bounds may or may not be the tightest possible (that is, these bounds are based on the dominance graph alone). Let us compute the highest, and lowest priorities for the non-dominated events. The ranking of event 1 is in the set \{1, \ldots, 5\}; event 2 in \{1, \ldots, 15\}; event 3 in \{1, \ldots, 16\}; event 4 in \{1, \ldots, 21\}; and event 5 in \{1, \ldots, 24\}. Thus, based on this result, the non-dominated events should not automatically be considered as the highest priorities, because there may be significant uncertainty about their ranking. However, because these ranking intervals may not be tight, this analysis may overemphasize the impact of uncertainty.

### A. Insight From the Results

The Fussell-Vesely is a measure of risk significance [1] in that it describes how significant the realization of a single event is for the risk of the system. Using this risk importance measure, we consider the insights that can be gained by the dominance graph.

In traditional prioritization based on the crisp risk importance measures, one could think that a large relative difference in the values of the importance measures would be guarantee that the priority is not sensitive to small deviations in the probabilities. However, as in this case, even a high crisp value of the Fussell-Vesely measure (event 1) cannot guarantee that the event would be the most important one for all probabilities that are allowed within the bounds. Still, event 1 was clearly the most important with respect to the Fussell-Vesely measure, because it dominated most of the events, and none of the events dominated it. Thus, this conclusion about the priority of event 1 is not much affected by epistemic uncertainty.

Events 2 through 5 are non-dominated, but do not dominate as many events as event 1. This means that even though there may be events that have higher risk importance when computing the measures with different probabilities within the bounds, there is no other events that systematically would have higher risk importance than these events. Thus, this analysis of epistemic uncertainty suggests that these events should be considered as potential candidates of having high priority even when more information (that would correspond to narrower intervals) about the probabilities is acquired.

Events 6 through 30 are dominated, and most of them dominate some other event as well. However, the overall pattern seems to be that there is not much dominance structure between these events. This suggests that the priority of these events is highly impacted by the epistemic uncertainty.

Event 31 is dominated by most other events, and it is the only event that does not dominate any other event. Therefore, this event is among the lowest prioritized events, even if some of the epistemic uncertainty was to be reduced by narrowing the intervals. Similarly as was concluded above for the non-dominated events, this event should be considered as a candidate for having the lowest priority. Thus, if some of the events where to be selected for further analysis for finding the most important component, this event could be excluded because it is dominated by so many events.

### V. Discussion

The method we have developed helps analyze the impact of epistemic uncertainty on the priorities that are implied by commonly used risk importance measures. In practice, this method can be implemented as an add-on which uses information that can be obtained from standard probabilistic safety assessment software, such as Risk Spectrum. For example, in the application to the residual heat removal system in Section IV, the dominance relations were computed using the 90% confidence interval for probability estimates. The results in this application...
suggest that plausible numerical variations that reflect uncertainties in the elicited probabilities can cause significant changes in the prioritization based on risk importance measures.

In this paper, we have employed primarily confidence intervals as a means of inferring bounds for the interval-valued probabilities, and we have also argued that more information often corresponds to narrower intervals. Yet, this argument should not be confused with Bayesian updating of confidence intervals, because in some cases the arrival of new evidence can result in wider confidence intervals. However, when more information is obtained about probabilities that have well behaved distributions (for example, by testing a larger number of components), the arrival of new evidence tends to result in narrower confidence intervals. It is from this perspective that narrower intervals are likely to be applicable in situations where there is more information, while broad intervals can be applied if less is known about the probabilities.

Global sensitivity analysis (e.g. [24]) has been used to analyze how sensitive risk importance measures are with respect to uncertainties about event probabilities. When applying this method in risk importance analysis, such analyses establish distributions on the risk importance measures of the events. However, when deciding on actions for improving system reliability, most attention is given to events that have the highest risk importance. If the distributions do not overlap (at least significantly), then the prioritization given by the risk importance measures is not sensitive. If the distributions overlap, then further analysis is needed. Note that this is complicated by the fact that the distributions of the risk importance measures are not statistically independent, as discussed in Section II. Thus, this analysis could be supplemented by our method in that the impact on priorities can be visualized with a graph. This analysis can also be considered as pre-screening that allows us to focus uncertainty analysis on the events which impact prioritization.

Modarres [10], Zio [2], and Baraldi et al. [7] examine the behavior of risk importance measures by using Monte Carlo simulation to derive distributions on prioritizations of the events. Their method can be seen as the dual to ours in that they use the distributions of the probabilities to derive a distribution for the priorities, and then use a confidence level to distinguish between which events have a higher priority than the other (as described in Section II). Our method on the other hand first bounds the probabilities within confidence intervals, and then derives partial priorities without considering the distribution of the priorities. Thus both methods arrive at partial priorities on the events using a similar simplification.

A difference between the methods is that our method cannot result in cyclic priorities, which is possible when using the simulation based approach. However, establishing dominance using the say 90% confidence intervals on the probabilities does not imply a 90% confidence that the dominating event does have a higher value of the risk importance measure. This disconnect is because the probability of all probability estimates being simultaneously within their confidence intervals is strictly less than 90% if the estimates can vary statistically independently. Therefore, the results produced by our method are not directly comparable with the simulation based prioritization methods. In this regard, non-probabilistic methods for deriving the intervals for the probabilities have a more natural interpretation, because they derive bounds for the probability without specifying a confidence level on the interval. Nevertheless, using confidence intervals for the parameters can be regarded as plausible deviations in parameter values in the sense of [4] that can be used as a basis for sensitivity analysis. Therefore, these methods can be seen to complement each other in that they have different strengths, even if they analyze essentially the same types of uncertainties.

In our framework, it is possible that the priority among events is inconclusive. For instance, in the case study in Section IV, events 1–5 where non-dominated, yet our method did not recommend a definite priority among these events. However, if one would like to derive a complete priority among the events, there are several ways to proceed. An interactive approach would be to elicit more information about the probabilities, which in turn would make the intervals narrower. The elicitation can be stopped when the dominance relations form a complete prioritization among the events (with the possibility of events being equal).

The interactive approach may require significant effort and resources, and furthermore is not even guaranteed to always yield a complete prioritization. Then one way to generate a complete prioritization is to select unique probability estimates for each event, that is reduce the interval-valued probabilities to singleton sets. This selection could be made with decision rules [46], [47], which in the context of this framework could be stated as follows.

1) Maximax-Select as most important the event whose largest risk importance measure over the feasible probabilities is the highest.

2) Maximin-Select as most important the event whose least risk importance measure over the feasible probabilities is the largest.

3) Minimax regret-Select as most important the event which has the smallest maximum regret, where maximum regret is the largest difference between an event’s risk importance measure and the risk importance measures of the other events over the feasible probabilities (for recent application if this decision rule in reliability engineering, see [48]). These decision rules can be computed if the importance measures can be expressed as a difference of two multilinear functions, whereas our branch and bound algorithm can be modified to find the bounds of the risk importance measures.

A. Computational Aspects

In our framework, it is necessary to optimize a multilinear function formed from the minimal cut sets of the system. This optimum can be determined with the branch and bound algorithm (see Table I), which however can take an exponential computation time. This result would suggest that the computational effort would be a greater issue for our framework than it is for methods that use Monte Carlo simulation for obtaining the distribution of the rankings of the events (e.g. [2], [7], [9], [10]). However, the algorithm is exponential only with respect to the number of probabilities \( p_i \) in the multilinear function that is derived from the risk importance measure under consideration. Therefore, the required computational effort does not grow.
significantly when the number of minimal cut sets increase, and consequently systems with a complicated structure function can be analyzed. However, our framework is not as straightforward to be used for analyzing uncertainty on the parameters of reliability models [27], because the relationship between parameters and probabilities cannot be expressed with multilinear functions with typical reliability models.

In the development of our method, no assumptions have been made about how the probabilities can vary within their intervals. This choice is a conservative approach in that the probabilities can take on all the values within their respective intervals, regardless of what the other probabilities are. Often, however, parameters are estimated with the help of models that contain shared parameters. For instance, [24] analyzed a large loss of coolant accident (LLOCA) in which the system included three identical pumps. The reliabilities of these pumps were elicited with a model with shared parameters. When analyzed in our framework, the failure probabilities of the three pumps would then be identical and vary within their respective intervals.

To show how such interdependencies can be modeled, we revisit the example in Section III-F, where the results were computed using the feasible set \( \{ p \in H^+ | 0.01 \leq p_i \leq 0.03 \ \forall i \} \) in which different \( p_i, i = 1, \ldots, 7 \) were allowed to vary within their intervals freely of each other. Thus, even if the intervals were identical, this feasible set contained vectors such as

![Fig. 3. Fussell-Vesely importance dominance graph for the RHRS case.](image-url)
\[ p = \{0.01, 0.03, 0.02, 0.025, 0.015, 0.015, 0.03\}, \]

where the event probabilities are not equal. Now, a model in which the probabilities are equal can be built by forming the feasible set \( \{ p \in \mathbb{R}^7 | p_i = \pi, 0.01 \leq \pi \leq 0.03 \} \). The algorithm that we developed was defined for feasible probabilities that form a hyperrectangle, whereas it cannot solve the problem in this form. However, because this hyperrectangle is a superset of the feasible set with constraints for interdependencies, the algorithm can still be used to analyze possible dominance relations. That is, the constraint \( p_i = \pi \) can be relaxed by disregarding it and adding the constraints \( 0.01 \leq p_i \leq 0.03 \) \( \forall i \), and the dominance relation can then be checked with Algorithm 1 over the resulting hyperrectangle. When this relaxation is made, the dominance results are conservative in that all dominance relations which hold over the relaxed set will hold over the smaller set with constraints for interdependencies, but some dominance relations may be missed.

**B. Future Research**

In Section IV, we have computed bounds for the highest and lowest possible rankings for events by considering dominance relations between events. However, it may be that the highest, and lowest rankings do not occur when the probabilities are at their upper, and lower bound respectively. This relationship is because the ranking depends on the values of the other events’ importance measures as well. Thus, converting a dominance graph into ranking intervals has the potential of losing information, and hence providing intervals that are not the tightest possible. In other words, the bounds obtained on rankings in this way are not necessarily tight, and may consequently exaggerate the impact of epistemic uncertainty.

Here, one possible extension is to establish tight bounds for rankings, analogously to the approach of Salo and Punkka [49] who develop a method for determining the highest and lowest efficiency rankings of a decision making unit in ratio-based efficiency analysis. Yet in the context of fault tree analysis, the computation of these tight bounds can lead to relatively complex multilinear programming problems. Such problems could be solved, for instance, by using the algorithm of Sherali and Tunçbilek [50], [51] which uses the Reformulation-Linearization technique to find a global optimum. Other applicable approaches are covered by the review of Desai [52].

The method can also be extended by permitting other kinds of statements in the elicitation of probabilities. For instance, ordinal information about probabilities could be incorporated through statements such as “the probability of event 1 is larger than the probability of event 2” (see [53] for a treatment of comparable statements in the elicitation of weight estimates in decision analysis). This ordinal statement would correspond to the constraint \( p_1 > p_2 \) on the feasible probability set. Thus, statistical interdependence between the probabilities can be modeled through constraints on the feasible probabilities. Here, one concern is that the solution effort for the solution of resulting multilinear programs may grow exponentially with problem size, which is likely to limit the size of the problems that can be solved in practice. It appears that existing general purpose algorithms can be modified along the lines suggested by [52] to speed up the optimization. Computational challenges notwithstanding, enriching the ways in which feasible probabilities are characterized makes it possible to accommodate many types of information that cannot be captured through interval-valued probabilities only. Consequently, this research direction appears promising.

In this paper, we have considered the prioritization of single events that are associated with individual components. However, PSA models are often used for informing decisions about how resources should be allocated to maintenance activities. Such decisions can be supported by framing them as maximization problems where the objective is to achieve the highest risk reduction subject to the requirement that the maintenance activities do not use more resources than what is available. This problem is essentially a portfolio selection problem that entails epistemic uncertainties about both the failure probabilities and the resources that are required by the maintenance activities. Ideas for development in this direction can be found in the literature on portfolio decision analysis (for a review, see [54]).

**VI. CONCLUSIONS**

We have developed a computational framework for analyzing the impact of epistemic uncertainty about event probabilities in fault tree analysis. This uncertainty is captured through interval-valued probabilities, and its implications for the relative priorities of events are explored by considering commonly used risk importance measures, and by establishing dominance relations for the events based on these measures. The dominance relations can be displayed with the help of directed graphs, which gives an easy-to-understand way of illustrating the results. These graphs show which events deserve the highest priority, in view of the epistemic uncertainties that are accommodated by the probability intervals.

We have applied our method to examine the fault tree of a complex system that represents the residual heat removal system of a nuclear power plant. Specifically, this application in Section IV showed that the relative priorities of events can change significantly when the probabilities are allowed to vary within their respective probability intervals. From this perspective, our method can also be seen as a means of conducting global sensitivity analyses ex post. Technically, it is possible to introduce also other kinds of constraints on the probabilities, even if a greater computational effort may be needed to derive dominance results.

**ACKNOWLEDGMENT**

The authors would like thank J.-E. Holmberg for his comments.

**REFERENCES**


Antti Toppila is a doctoral student in the Aalto University School of Science. His research interests are in risk analysis, portfolio decision analysis, and decision-making and optimization under uncertainty. He was a board member of the Finnish Operational Research Society (FORS) from 2006 to 2011.

Ahti Salo has worked extensively on the development of decision analytic methods, and their uses in resource allocation, innovation management, risk management, technology foresight, and efficiency analysis. He has published widely in leading international journals (including Management Science and Operations Research), and received awards for his research from the Decision Analysis Society of the Institute for Operations Research and Management Sciences (INFORMS). He is the Editor-in-Chief of the EURO Journal on Decision Processes, and on the Editorial Boards of Decision Analysis and five other refereed journals. Professor Salo has directed a broad range of basic and applied research projects funded by leading industrial firms, industrial federations, and funding agencies. He has been a visiting professor at the London Business School, University Paris-Dauphine, and the University of Vienna. In 2010–11, he was the President of the Finnish Operations Research Society (FORS), and served as the European and Middle East representative of the International Activities Committee of INFORMS. He is a jury member of the EDDA 2012 Doctoral Dissertation Award of the Association of European Operational Research Societies (EURO). He has been on the Board of the Association of Parliament Members and Researchers (Tutkas) since 1999.