

Modeling Event Dependencies Using Disjoint Sets in Fault Trees

David W. Twigg, Anapathur V. Ramesh, Tilak C. Sharma

Abstract

Disjoint sets are a powerful and useful tool for modeling some uncommon situations where the basic events are dependent in some manner. Such sets can be constructed from stochastically independent sets, and therefore special fault tree solvers are not needed to solve fault trees that use disjoint sets. Construction of disjoint sets is reviewed and several examples showing the usefulness of disjoint sets are provided.

Introduction:

Fault tree methodology usually assumes that the fault tree basic events are stochastically independent. Stochastically independent sets “overlap” in a predetermined way so that the probability of simultaneous occurrence of two such events equals the product of probabilities of their individual occurrences. In general for any two events, the probability of both events occurring equals the product of the probability that the first event occurs and the conditional probability that the second event occurs given the occurrence of the first event. The stochastic independence assumption is equivalent to assuming that this conditional probability equals the probability that the second event occurs. In practice, there are situations in which this conditional probability takes on an arbitrary value between zero and one. Two events might be mutually exclusive, such as a valve having failed stuck open and having failed stuck shut; in this case the conditional probability is zero. Conversely, the second event may occur whenever the first event occurs, although the reason may not be understood. To model this relationship, we want the conditional probability to equal one.

The common assumption of stochastic independence of the basic events makes these dependencies between events difficult to model in fault trees. However if mutually exclusive events are available as primitives, such modeling is considerably simplified. The pieces of the Venn diagram which maps the relationships between events can be represented as mutually exclusive events with the requisite probabilities; events are then constructed by assembling the appropriate pieces of the Venn diagram.

A systematic method for constructing mutually exclusive events is given in [1]. This method does not require specialization of fault tree solution algorithms, and thus could be easily embedded in fault tree packages. A manual procedure for constructing mutually exclusive events from ordinary, stochastically independent events is provided in the appendix. In the remainder of the paper we assume that mutually exclusive events are available as fault tree primitives or else are constructed as described in the appendix, and we focus on use of mutually exclusive events in fault tree models to model event dependencies.

Failure Coupled Events:

The assumption in fault tree solvers is that basic events are independent. For any two independent events A and B, the probability that both occur simultaneously is equal to the product of their probabilities. That is,

$$P(A \cap B) = P(A)P(B) \tag{1}$$

In practice, events may not be independent, and $P(A \cap B)$ may take on any value in the range

$$0 < P(A \cap B) \leq \min(P(A)P(B)) \tag{2}$$

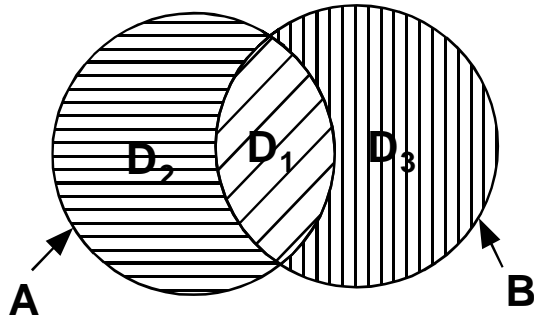


Figure 1: Disjoint sets D_1, D_2, D_3 and failure coupled events A and B

For an arbitrary number γ satisfying (2), we can construct A and B so that

$P(A \cap B) = \gamma$. We first construct disjoint events D_1, D_2, D_3 (Figure 1) with probabilities

$$\begin{aligned}
 P(D_1) &= \gamma \\
 P(D_2) &= P(A) - \gamma \\
 P(D_3) &= P(B) - \gamma
 \end{aligned}
 \tag{3}$$

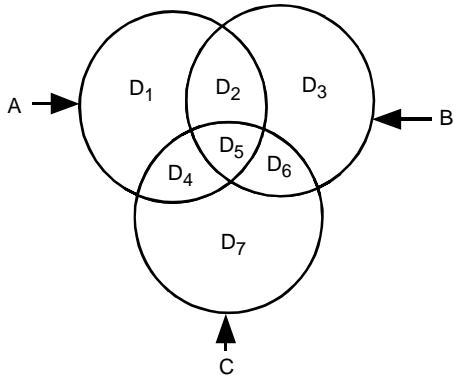
Then build sets A and B from D_1, D_2, D_3 as follows:

$$\begin{aligned}
 A &= D_1 \cup D_2 \\
 B &= D_1 \cup D_3
 \end{aligned}
 \tag{4}$$

A consequence of D_1, D_2, D_3 being disjoint is that $A \cap B = D_1$, so

$P(A \cap B) = P(D_1) = \gamma$. To summarize, given two failure coupled events A, B with probabilities $P(A)$ and $P(B)$ such that $P(A \cap B) = \gamma$ the mutually exclusive events D_1, D_2, D_3 can be constructed with probabilities as shown in (3). Then these mutually exclusive events can be represented in fault trees by use of primitives or by construction using stochastically independent basic events as shown in the Appendix or [1].

This method generalizes to more than two failure coupled events. The idea is to build disjoint sets



to

Figure 2: Three events A,B,C represented by union of disjoint sets

represent each piece of the Venn diagram and then assemble the disjoint sets to form the coupled events with the desired properties. The disjoint sets are constructed to have the required probabilities. Figure 2 shows the three-event case. Seven disjoint sets D_1, \dots, D_7 are needed to represent the seven independent pieces in the

Venn diagram. Probabilities are assigned to each D_k according to its observed event frequency.

For example, $P(D_5) = P(A \cap B \cap C)$.

Events A, B and C are built up from the D_k in the obvious way:

$$\begin{aligned}
 A &= D_1 \cup D_2 \cup D_4 \cup D_5 \\
 B &= D_2 \cup D_3 \cup D_5 \cup D_6 \\
 C &= D_4 \cup D_5 \cup D_6 \cup D_7
 \end{aligned}
 \tag{5}$$

Cascading Failure Events:

Nested sets ($A_1 \subset A_2 \subset \dots \subset A_n$) represent cascaded failure coupling in which failure of any member of the chain of events implies failure of all following members (whenever A_k fails, A_{k+1}, \dots, A_n also fail). To model cascading failures of this type, construct n disjoint sets with probabilities:

$$\begin{aligned}
 P(D_1) &= P(A_1) \\
 P(D_2) &= P(A_2) - P(A_1) \\
 \dots
 \end{aligned}
 \tag{6}$$

$$P(D_n) = P(A_n) - P(A_{n-1})$$

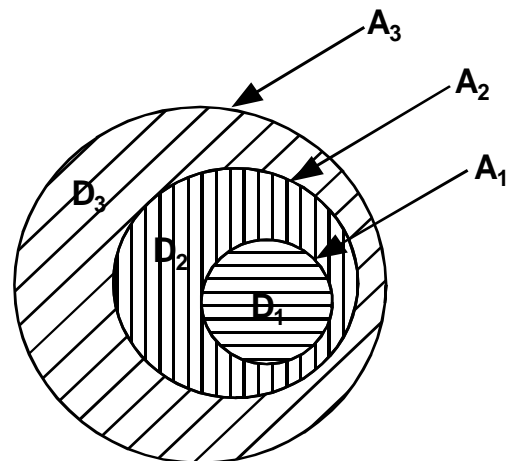
and set

$$\begin{aligned}
 A_1 &= D_1 \\
 A_2 &= A_1 \cup D_2 \\
 \dots
 \end{aligned}
 \tag{7}$$

$$A_n = A_{n-1} \cup D_n$$

Note that the disjoint events are interpreted as:

$$D_k = A_k \cap \overline{A_{k-1}}; k = 2, \dots, n.$$

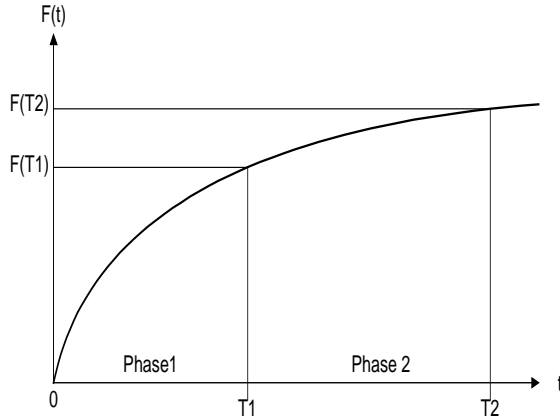


shows three cascading failure events.

Disjoint Sets in Phased Mission Systems:

A phased mission comprises distinct phases, and failure in any phase equates to failure of the entire mission. Failure conditions for each phase

may differ, failure rates of the components for each phase can differ and failed components are



not repaired during the mission.

Since there is no repair of component during a phase or between any two phases its failure time

Figure 4: Phased mission system component CDF

component in the system. Consider the cumulative distribution function $F(t)$ of a component in a 2-phase mission system as shown in Figure 4. In Figure 4, $T1$ and $T2$ represent the end of the first phase and second phase. If we define the events:

$E1$ = Component fails in first phase, i.e., in time interval $(0, T1)$

$E2$ = Component fails in second phase, i.e., in time interval $(T1, T2)$

E = Component fails in first or second phase, i.e., in time interval $(0, T2)$

Then from the definition of CDF, we have

$$P(E1) = F(T1) - F(0)$$

$$P(E2) = F(T2) - F(T1)$$

$$P(E) = F(T2) - F(0) = P(E1) + P(E2) \quad (8)$$

Noting that logically $E = E1 \cup E2$ it follows

from (8) that $P(E1 \cap E2) = 0$ and therefore

$E1$ and $E2$ are disjoint. Therefore the failure of a single independent component in the phases can be represented by disjoint sets whose probabilities are known from the CDF of the component and the phase times. In general if there are m mission phases and we have m disjoint events $E1, \dots, Em$ that represent the failure of the independent component in the respective phases. The failure of the component in any of the first p phases is:

$$E_{1,p} = E1 \cup E2 \cup \dots \cup Ep$$

To model the system failure across the entire mission we follow the methodology first proposed by Esary and Ziehms [1]. Esary and Ziehms focused on a reliability block diagram formulation, but also mentioned a fault tree method. A fault tree is written for the system failure for each phase, using $E_{1,p}$ to represent the component being failed at the end of phase p . The mission fault tree for the system is the logical OR of the phase fault trees. This formulation and the Esary and Ziehms variant have the advantage that conventional fault tree solution methods apply. As mentioned in the previous sections we can use disjoint set primitives if available or construct the disjoint events from stochastically independent events as shown in [1] and the Appendix.

An alternative representation of the component failure in the different phases can be as described by Esary and Ziehms [2]. They define the random variables C_1, \dots, C_m to represent the behavior of component C in the m mission phases. C_p represents the conditional event that component C fails in phase p given that it is operational at the beginning of the phase. Then the event

$$A_p = C_1 \cup \dots \cup C_p \quad (8)$$

represents the failure of the component C in any of the first p phases. The fault tree formulation, has been explored by several authors, most recently Somani and Trivedi [3] and Trivedi [4]. Both [3] and [4] use A_p as basic events in the fault tree formulation. These events are not stochastically independent and conventional solution methods cannot solve the resulting fault trees, so [3] and [4] devote a significant part of their effort to discussing modification of standard fault tree solution methods to accommodate this representation of the events. We believe that the representation $E1, \dots, Em$ as described earlier is conceptually simple. Also in some instances it matters in which phase the failure occurred. For example component failure one phase might be accommodated by switching to a spare, whereas there might not be time to switch during the next phase. In such situations it is convenient to have phase failures such as $E1, \dots, Em$ directly available in the model.

References:

- [1] Twigg D.W., Ramesh, A. V., Sandadi, U.R., Sharma, T.C., " ", RAMS 2000, Los Angeles, CA. USA.

- [2] Esary J.D., Ziehms H, "Reliability Analysis of phased missions" In Barlow R.E., Fussel, J.V., Singpurwalla N.D. editors. Reliability and Fault Tree Analysis: Theoretical and Applied Aspects of System Reliability and Safety Assessment, Philadelphia: SIAM, 1975, pp. 213-236.
- [3] A. K. Somani, K.S. Trivedi, "Phased-Mission Analysis Using Boolean Algebraic Methods", SIGMETRICS 94 - 5/94, Santa Clara, CA., USA, pp 98 -107
- [4] Ma, Y., Trivedi, K.S., "An algorithm for reliability analysis of phased-mission systems", Reliability Engineering and System Safety, Vol 66, 1999, pp. 157 - 170.

Appendix: Construction of Disjoint events

The following procedure produces n mutually disjoint sets $\{S_1, \dots, S_n\}$, where $S_j \cap S_k = 0$ for any pair of the sets. n stochastically independent sets (A, E_1, \dots, E_{n-1}) are used in the construction. Probabilities of the stochastically independent sets are chosen to force the probabilities of the disjoint sets to have specified values $\{\pi_1, \dots, \pi_n\}$; that is, $P(S_k) = \pi_k$. This procedure is described in [1].

It can be verified that sets $\{S_1, \dots, S_n\}$ defined below are mutually disjoint. In a fault tree each S_i would be treated as a developed event, and would be expanded as a combination of a single AND gate and several NOT gates.

$$S_1 = A \cap E_1 \tag{1A}$$

$$S_2 = A \cap \bar{E}_1 \cap E_2$$

...

$$S_{n-1} = A \cap \bar{E}_1 \cap \dots \cap \bar{E}_{n-2} \cap E_{n-1}$$

$$S_n = A \cap \bar{E}_1 \cap \dots \cap \bar{E}_{n-1}.$$

If the probabilities of the independent events are set as shown below, the S_i will have the desired probabilities:

$$P(A) = \sum_{k=1}^n \pi_k = \alpha \tag{2A}$$

$$P(E_1) = \frac{\pi_1}{\alpha}$$

$$P(E_2) = \frac{\pi_2}{\alpha - \pi_1}$$

...

$$P(E_{n-1}) = \frac{\pi_k}{\alpha - \sum_{j=1}^{k-1} \pi_j}$$

For example, to construct mutually exclusive sets S_1, S_2 and S_3 , where

$$P(S_1) = 0.1$$

$$P(S_2) = 0.2$$

$$P(S_{31}) = 0.3$$

(3A)

Use stochastically independent sets A, E_1 and E_2 :

$$S_1 = A \cap E_1$$

(4A)

$$S_2 = A \cap \bar{E}_1 \cap E_2$$

$$S_3 = A \cap \bar{E}_1 \cap \bar{E}_2.$$

Calculate probabilities

$$P(A) = .1 + .2 + .3 = .6$$

$$P(E_1) = \frac{.1}{.6} = .167$$

$$P(E_2) = \frac{.2}{.6 - .1} = .4$$

(5A)

David Twigg -- david.w.twigg@boeing.com
425-266-7919