Reliability Engineering and System Safety 147 (2016) 117–122

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Importances of components and events in non-coherent systems and risk models

Jussi K. Vaurio *

Prometh Solutions, Hiihtäjänkuja 3K, 06100 Porvoo, Finland

ARTICLE INFO

Article history:
Received 20 March 2015
Received in revised form
28 August 2015
Accepted 8 November 2015
Available online 1 December 2015

Keywords:
Birnbaum
Criticality
Fault tree
Importance measures
Non-coherent
Risk analysis

ABSTRACT

Component importance measures have been defined and applied so far mostly for coherent systems. This paper develops and compares possible extensions of the traditional measures to non-coherent systems. The focus is on Birnbaum- and Criticality-type importances, both with respect to system unavailability and system failure intensity. Several versions are suggested for both measure types, each with different interpretation and potential applications. The measures are presented in terms of Boolean system logic functions so that they can be quantified with usual fault tree techniques even for large systems without manually solving and derivation of lengthy analytical functions. Examples demonstrate the method and discover some potential problems in system design if a component can initiate an accident while it is also part of a safety function to prevent an accident. Results are compared to earlier published results obtained with different algorithms.

1. Introduction

Several component and event importance measures have been introduced by many authors since the first structural measure by Birnbaum [1]. The relationships of the measures have also been presented in textbooks [2] and many journal articles. For more extensive reviews the reader is referred to the contents and references in [3,4]. Earlier work has focused mostly on coherent systems which can be modelled without NOT-gates or negations in system logic models such as fault trees. Non-coherent is a logic model that includes both failed states and success states for some or all components, or cannot be modelled without Boolean NOT-gates in a fault-tree. Importance measures are intended to be useful in ranking components or events for various applications and for optimising decision making. The roles of many measures in a variety of applications are described in Ref. [5].

This paper reviews, compares and extends importance measures that have been suggested before, and introduces several new ones for non-coherent systems and risk models. Importance measures have been traditionally defined for components with respect to system unavailability i.e. when the interest of the analyst is in system unavailability rather than system failure intensity (frequency). The basic expression for coherent system failure intensity was pointed out by Murchland [6] and is recognised as the sum of the products of component failure intensity and component Birnbaum measure, e.g. [7]. In a safety system the role of a component is to prevent an accident. In the success state the component is an accident preventer but in a failed state it can be called an accident enabler. Importance measures with respect to system failure intensity or accident frequency need to take into account that a component may appear as an initiating event having a frequency or as an enabler having unavailability, or both.

Criticality importance is defined as the relative contribution of a component to system output quantity of interest (unavailability or failure frequency). It indicates the relative reduction of the output if or when the reliability of a component is made perfect, not able to fail. This works in coherent systems and is in proportion to the product of Birnbaum measure and component unavailability (or intensity). Complications can arise if a component appears both as an initiator and an enabler. New definitions are needed especially in non-coherent systems when both failures and repairs can contribute to the system unavailability and failure intensity.

Criticality importance measures for components with respect to system failure intensity and with respect to the total system failure count were presented in [3]. These take into account the total contribution of each component i.e. (a) contribution as the last failure ("initiator") of a minimal cut set (MCS), and (b) as the unavailability contribution ("enabler") in other MCS in which the component is a factor. These are now extended to take into account also the total contributions of repairs and availabilities.

* Tel.: +358 404139949.
E-mail address: jussi.vaurio@pp1.inet.fi

http://dx.doi.org/10.1016/j.ress.2015.11.007
0951-8320/

Concerning non-coherent systems Ref. [8] compared two alternatives as potential extensions of the classical Birnbaum measure. A couple of new alternatives are suggested in the present paper.

Ref. [8] also presented the integral of system failure intensity (failure count) for non-coherent systems using partial derivatives of analytical system probability. Refs. [9] and [3] presented the failure intensity for non-coherent systems in terms of probabilities of Boolean expressions solvable by computerised fault tree methods even for very large systems. It was also pointed out that a consistent definition of Birnbaum measure for non-coherent systems is exactly like the original for coherent systems and equals the derivative of the system unavailability with respect to the component unavailability parameter.

In Ref. [3] importance measures with respect to system failure intensity were developed and it also pointed out that the Barlow–Proschan importance [12] only measures the contribution of a component as the last failure in a MCS, not the total contribution. A formula for the total contribution was presented in [13] and [3]. Ref. [11] also evaluated for a non-coherent system importance measures with respect to system failure intensity. Ref. [14] reviewed several examples of non-coherent systems analysed in the literature and also assessed methods suggested for treating other mutually exclusive events.

The rest of this article is structured as follows. In Section 2 the fundamental concepts and definitions are presented in general terms of probabilities of Boolean expressions and their relationships so that explicit analytical functions and their derivations are not needed when computerised algorithms produce the needed quantities. It turns out that several alternatives can be suggested and justified for extensions of both Birnbaum and Criticality importance measures with somewhat different definitions and interpretations, depending on the purpose or an application. Importance measures are defined and their relations are pointed out so that a minimum number of calculations from the complete system model are needed. In Section 3 comparisons to earlier approaches are made and demonstrated with numerical examples. Summary conclusions are drawn in Section 4.

2. System models with negations

The formalism and definitions of importance measures for non-coherent systems are presented here following mostly notations in [9,3]. Capital letters indicate Boolean variables. Logic unions and intersections are indicated with regular plus sign and multiplication. Consider a TOP-event Y of a fault tree of a system or a risk model, a Boolean expression of the failed state of a system or function in terms of the basic event failed states Z_k and possibly also success states $Z_{k'}$, $k=1, \ldots, K$. The complements $Z_{k'}$ are for the time being considered individual events with probabilities $z_{k'}=P(Z_{k'})=1-z_k$. The probability $y=P(Y)=y(\mathbf{z},\mathbf{z}')$ is multi-linear in terms of all K basic event probabilities $z_k=P(Z_k)$ and possibly K or less complements $z_{k'}$. This is understandable based on quantification of Eq. (1) below with the inclusion–exclusion principle, and also proved in [19]. Each event $Z_{k'}$ is assumed s-independent of the other events like Z_k but these two are mutually exclusive and $P(Z_k Z_k')=0$.

The order of computation of importance measures is presented largely so that a minimum number of model runs are needed. All variables can be time-dependent but the time argument t is not always marked. It is generally possible to write Y in terms of the minimal cut sets (MCS) or prime implicants of any Z_k as

$$Y=Z_kG_k+Z_k'D_k+H_k, \tag{1}$$

where the unions of terms containing Z_k or $Z_{k'}$ are separated from each other and from other terms H_k. The Boolean functions G_k, D_k and H_k are independent of both Z_k and $Z_{k'}$. Z_kG_k is the union of all MCS containing Z_k, and $Z_k'D_k$ consists of all terms containing Z_k'. H_k contains neither Z_k nor Z_k'. Besides, G_k and D_k contain no common terms because any such would be part of H_k. In coherent systems $D_k=\phi$ (empty). The probability $P(Y)$ can be quantified with normal inclusion–exclusion (Sylvester–Poincaré) principle with the exception that all terms and products of terms that contain both Z_k and Z_k' must be deleted due to the logic product $Z_k\cdot Z_k'=\phi$ ("FALSE").

Taking into account that $z_k'=P(Z_k')=1-z_k$ with $z_k=P(Z_k)$, the probability $P(Y)$ can be written as

$$\begin{aligned} y=P(Y)&=z_k[P(G_k)-P(G_kH_k)]+z_k'[P(D_k)-P(D_kH_k)]+P(H_k)\\ &=y_k^-+z_k(y_k^+-y_k^-)=y_k^++z_k'(y_k^--y_k^+), \end{aligned} \tag{2}$$

where $y_k^+=P(G_k+H_k)$ and $y_k^-=P(D_k+H_k)$ are conditional probabilities of Y under conditions

Z_k=TRUE and Z_k=FALSE, respectively.

These y_k^+ and y_k^- can be solved by fault trees setting Z_k TRUE and FALSE in (1), respectively. Or, having solved y by any means, one can obtain $y_k^+(\mathbf{z})=y(\mathbf{z}|z_k=1,z_{k'}=0)$, $y_k^-(\mathbf{z})=y(\mathbf{z}|z_k=0,z_{k'}=1)$, and $h_k=P(H_k)=y(\mathbf{z}|z_k=z_k'=0)$. However, all these need not be quantified from the complete model because of the relationship $z_ky_k^++z_k'y_k^-=y$. Having solved y and y_k^- one can get y_k^+ as

$$y_k^+=(y-z_k'y_k^-)/z_k. \tag{3}$$

It is possible that y_k^- is larger or smaller than y_k^+. Thus, the optimal value for z_k is $z_k=0$ if $y_k^+>y_k^-$ and $z_k=1$ if $y_k^+<y_k^-$. In the latter case it is natural to ask: why not set component k to a failed state $z_k=1$? That would be the optimal state for this component. However, if the same component participates in a production function there may be economical reasons to keep it operating as reliably as possible. This contradictory situation calls for a compromise between economy and safety and it could not be solved only with importance measures.

The ratio y_k^+/y corresponds to the traditional risk achievement worth RAW(Z_k) or risk increase factor RIF(Z_k) for coherent systems and has been applied widely for determining acceptable allowed repair or outage times, AOT. In noncoherent systems there are two such measures that may be called "risk gains" (RG) because either one can be larger or smaller than one

$$RG_k^+=y_k^+/y, \quad RG_k^-=y_k^-/y \tag{4}$$

Decision making has to use one or both of these depending on the situation.

2.1. NOT-gates in a fault-tree

Non-coherence is not always presented only by negated events in a system model. There can be logic NOT-gates higher up in a fault-tree. In that case the model can be modified so that it contains negations of basic events but no NOT-gates. This is accomplished as follows:

- NOT-gates are pushed down toward basic events by de Morgan's Laws,
- new variable names (basic events) are introduced to represent negated basic events,
- minimal cut sets (MCS) of the rewritten formula are determined,
- those terms that contain both an event and its encoded complement are deleted,
- the probability of the remaining union of MCSs is quantified. When a higher-order inclusion–exclusion development is used, also higher-order terms (products of MCSs) containing both an event and the complement are deleted.