RELIABILITY MODELLING OF INDUSTRIAL SYSTEMS BY FAULT TREES AND STOCHASTIC PETRI NETS

Ondřej Vozár – Luboš Marek

Abstract

Knowledge of minimal cut sets and minimal path sets of a coherent system are vital for its probabilistic assessment of reliability. Fault trees and Petri Nets are two main methodologies of modeling reliability of complex systems. It is an open problem, which setting is computationally cheaper for finding minimal sets, because this problem is NP-hard both for fault trees (Rosenthal, 1975) and Petri Nets. Algorithms to find critical cut sets and minimal path sets in both settings are reviewed and its efficiency is assessed for a real-life system from electrical engineering – the “three-motor” system (Vesely et al., 1981). Different probabilistic bounds of the reliability function using minimal sets are reviewed and their performance is studied by numerical experiment for this model example. However, there is no clear decision on which setting is better to find minimal sets of a system.

Key words: reliability, fault trees, stochastic Petri Nets, time to failure, probability bounds of a reliability function

JEL Code: C10, C18, C60

Introduction

There is a growing a demand for the precise calculation of reliability of complex systems. An example of such a system is a power plant, computer network, human body. These methods are applied in many fields like energetics, computer science, medicine, transportation and engineering. The systems are classified to *Repairable* and *Non-Repairable Systems.* We treat only Non-Repairable Systems in this paper. Fault trees (see Limnios, 2007) and Petri Nets (see monograph of Bause and Kritzinger, 2002) are two main methodologies of modeling of reliability of a complex systems.

Because finding minimal sets is a NP-hard problem (Rosenthal, 1975), it is an open problem, which setting is computationally cheaper. Liu and Chiou (1997) found a one-to-one relation between a fault tree and a Petri Net of a system. Therefore, in practice we can easily switch between settings, if needed. They also developed a recursive top-down matrix algorithm to find all minimal sets of the system. They also claim without any proof this algorithm is more computationally efficient than algorithms for fault trees. To our best knowledge, no complexity analysis or computational studies have been carried out yet.

In both methodologies, a coherent system is represented as a tree in the graph theory. In both settings, it is vital to know both minimal cut sets and minimal path sets of a system. For state assessment of a system following concepts are defined (Limnios, 2007):

- *Path:* a subset of components of a system whose simultaneous good functioning assures good functioning of the system regardless of the functioning of the other components.
- *Minimal path*: a path that does not contain another path.
- *Cut set*: a subset of components of a system whose simultaneous failure leads to the system failure regardless of the failure of the other components.
- *Minimal cut set*: a cut set that does not contain another cut set.

Set of the minimal paths is denoted as $C = \{C_1, C_2, \cdots, C_c\}$ and set of minimal cuts is denoted as $K = \{K_1, K_2, \cdots, K_k\}$. The goals of the paper are twofold. In the first part, am example is worked out, which representation is more suitable to find minimal sets of a system. In the second part, we compare tightness of several probability bounds of the reliability function of a system.

1 Elements of Reliability Theory and Coherent Systems

Let X be a continuous random variable representing time to failure of the single-component system with cumulative distribution function $F(t) = P(X \leq t)$ and its density function $f(t)$. Survival function (reliability) is the complement to cumulative distribution function (Rausand and Oien, 1996)

$$R(t) = 1 - F(t) = P(X > t) = \int_t^\infty f(x)dx. \tag{1}$$

Note, that $R(0) = 1$ and $R(\infty) = 0$. *Mean time to failure (MTTF)* is defined as the expectation of the time to failure, e.g. $E(X)$. The exponential distribution is the most used for modeling time failure in reliability theory, which represents a Markovian system (without memory - a system is not aging). For fixed time $t > 0$ and parameter $\lambda > 0$ it holds

$$F(t) = 1 - e^{-\lambda t}, R(t) = e^{-\lambda t}, MTTF = E(X) = 1/\lambda.$$

Systems with memory are studied by Semi-Markov processes theory (Barbu et al., 2004).

A multi-component system defined as a binary system with n components: $C = \{1,2,\dots,n\}$. For each component i it is defined a binary variable x_i (0: the component works, 1: the component is down). Let $\boldsymbol{x} = (x_1, x_2, \dots, x_n) \in \{0,1\}^n$ be the vector jointly describing the states of the components. A binary *structural function* $\boldsymbol{\varphi}(\boldsymbol{x})$ is defined as $\boldsymbol{\varphi}(\boldsymbol{x}) = 1$, if the system works,$\boldsymbol{\varphi}(\boldsymbol{x}) = 0$, if the system fails.

Good functioning of a *series system* depends on the simultaneous functioning of all its components. If at least one component fails, then the system also fails. In fault tree setting it is modeled by gate OR. Good functioning of a *parallel system* depends on good functioning is assured by functioning of least one of its components. Only if all components fail, then the whole system also fails. In fault tree setting is modeled by gate AND.

Both in theory and application of the reliability theory, research is limited mostly to *coherent systems.* A coherent system has these properties (Limnios, 2007):

- It consists only of parallel and series systems (e.g. gates AND and OR).
- It has no redundant components (whose states do not affect the state of the system).
- It does not contain a component and its negation simultaneously.
- It contains neither loops nor circuits in its graph representation.

Using minimal path sets or minimal cut sets its structural function can be simplified as

$$\boldsymbol{\varphi}(\boldsymbol{x}) = 1 - \prod_{j=1}^{c}\left(1 - \prod_{i \in C_j} x_i\right), \boldsymbol{\varphi}(\boldsymbol{x}) = \prod_{j=1}^{k}\left(1 - \prod_{i \in K_j}(1 - x_i)\right). \tag{2}$$

Let be $S = (C, \boldsymbol{\varphi})$ a coherent system of order (number of its components) $n \geq 1$ and X_i be an alternative random variable (with values $x_i \in \{0,1\}$) with parameter p_i describing the state of the i^{th} component $(i = 1,2,\dots,n)$. *Reliability of the system* $R(\mathbf{p})$, where $\mathbf{p} = (p_1, p_2, \dots, p_n)$ is defined as the probability, that the system is works well. Using minimal cut sets or minimal path sets, it holds

$$R(\mathbf{p}) = P(C_1 \cup C_2 \cup \cdots C_k) = 1 - P(K_1 \cup K_2 \cup \cdots K_k). \tag{3}$$

Different bounds for reliability function were established (see Limnios (2007)) using minimal sets. *Minimal sets bounds* are established as follows. A lower bound is derived using minimal cut sets and an upper bound is using minimal paths sets

$$\prod_{j=1}^{k}\left[1 - \prod_{i \in K_j}(1 - p_i)\right] \leq R(\mathbf{p}) \leq 1 - \prod_{j=1}^{c}\left(1 - \prod_{i \in C_j} p_i\right). \tag{4}$$

For 2-by-2 disjoint cut minimal sets ($K_i \cap K_j = \{\emptyset\}$, if $i \neq j$) the upper bound equals to the reliability function . The same rule applies to minimal paths and the lower bound. *“Min-max” bounds* are

$$\max_{1\le j\le c}\left(\prod_{i\in C_j} p_i\right) \le R(\boldsymbol{p}) \le \min_{1\le j\le k}\left(1-\prod_{i\in K_j}(1-p_i)\right). \tag{5}$$

Trivial bounds are since the reliability of a coherent system lies between the reliabilities of the series and parallel system

$$\prod_{i=1}^{n} p_i \le R(\boldsymbol{p}) \le 1-\prod_{i=1}^{n}(1-p_i). \tag{6}$$

Note that, these bounds work poor.

1 Fault Trees and Petri Nets

We present both representations of a system in a form enabling only static analysis. This setting can be further extended by adding a time variable, but this extension is not a goal of the paper. Events of fault trees are represented by these graphic symbols (Limnios (2007), Vesely et al. (1981)):

- *Rectangle* – top or intermediate event (the system is down).
- *Circle* – basic event.
- *Triangle* – transfer (the fault tree is further developed).
  Petri Nets (Petri, 1962) was designed to study information systems in computer science.

They have been generalized and applied in many other fields (for applications in reliability modelling see monograph of Bause and Kritzinger (2002) among others). The graphic symbols of Petri Nets are summarized below (Bause and Kritzinger, 2002)

- *Circle (place)* – object, component of a system.
- *Dot (token)* – specific value or state of the object, component.
- *Rectangle (transition)* – activities changing state or value of the object, component.
- *Arrow (arc)* – connection of places and transitions.

Places can represent hardware and software components or modules of a software system. Transitions represent relations of components of a system (i.e. transactions between hardware components or modules of software).

Place-Transition Petri Nets enable only static analysis of the coherent system. To add time domain of a system Place-Transition Petri Nets were generalized to Stochastic Petri Nets (Natkin, 1980 or Molloy, 1981). Coherent system can be easily analyzed in both settings simultaneously because Liu and Chiou (1997) established the one-to-one relationship between its Place-Transition Petri Net and corresponding fault tree. Top, intermediate, and basic events are represented as places in Petri Nets. Note that, the events in the fault tree setting resemble hardware/software components of a system.

1.1 Algorithms to find minimal cut sets and minimal path sets

Algorithms for both settings are presented. Liu and Chiou (1997) proposed a recursive top-down matrix algorithm to find both minimal cut sets and minimal path sets simultaneously. It proceeds as follows:

- Write down the numbers of places horizontally if the output place is connected by multi-arcs to transitions.
- Write down the numbers of places vertically if the output place is connected by an arc to a common transition.
- As soon as all places are replaced by places representing basic events, a matrix is created. If there is a common entry located between rows or columns, it is also the entry present in each row or column. The column vectors of the matrix contain cut sets, the row vectors then paths sets.
- Finally, select the minimal cut sets and minimal path sets.

Liu and Chiou (1997) claim without any proof this algorithm is more efficient than the ones for fault trees. By our best knowledge, no computational study of algorithms was done yet.

There is many algorithms for fault tree setting (see Limnios (2007) for an extensive review). The most used algorithm is *MOCUS* (Fussel and Vesely, 1972), which has many modifications. It is also a top-down recursive algorithm as one of Liu and Chiou (1997). This algorithm proceeds as follows (Limnios, 2007):

1. Initialize the first element of a matrix with the top event operator.
2. The operator $G_i(A_1, \cdots, A_s)$ occupying the place (i, j) of the matrix B_k is to be resolved at the stage k.
3. If it is an AND operator, replace it with its inputs in the row. The first input takes the place of the operator, and the subsequent inputs the places $(i, j+1), (i, j+2), \cdots, (i, j+s-1)$.
4. If it is an OR operator, replace it with its inputs in the column. The first input takes the place of the operator, and the subsequent inputs the places $(i+1, j), (i+2, j), \cdots, (i+s, j)$. Also, each element $b_{i,m}, m = 1,2, \cdots, s$; $m \neq i$, is repeated. The block matrices B_1, B_2 remain unaltered.
5. If there is another operator in B, then continue as in 2.

2 Application to „Three-Motor" System

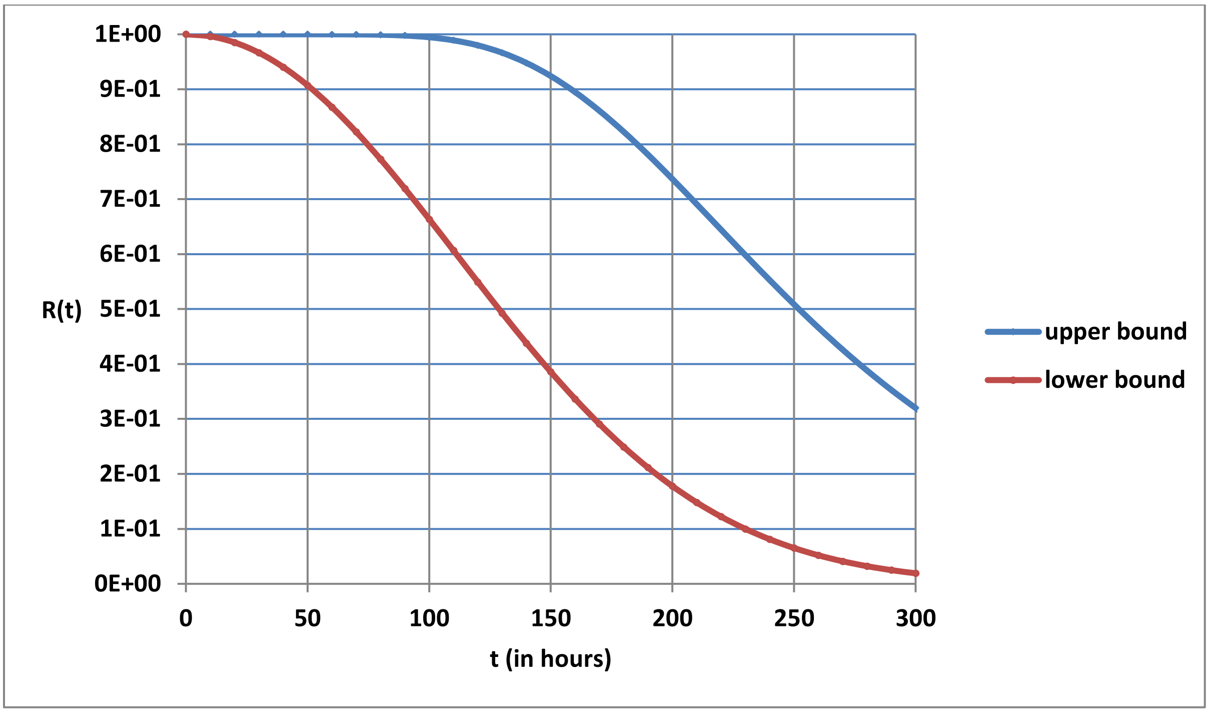
The three-motor system (Vesely et al., 1981) is a benchmark for the assessment of reliability methods. It is a real-life control system of the identical three motors in series wiring. A 60-second signal test is impressed to shut down the motors. The system is in failure if the electromagnetic force (EMF) is applied to any of the three motors for more than 60 seconds after the start of signal test. We refer to Vesely et al. (1981), p. 116 for more technical details of the system components. Fault tree and Petri Net of the system and finding all minimal sets by algorithm of Liu and Chiou (1997) was carried out for example in Vozár (2020).

Any motor has 12 minimal cuts and 4 minimal paths. The minimal cut sets of the system are a union of the minimal cut sets of the three motors, because the system consists of the series system of three identical motors. For the same reason, the minimal path sets of the system are the Cartesian product of the minimal path sets of the three motors. The "three-motor" system has 3x12=36 minimal cuts and 4^3=64 minimal paths. For such complex system reliability function cannot be calculated analytically or guessed.

Algorithms to find minimal cut sets and minimal path sets from Section 1.1 were applied to the "three-motor" system. The part of the algorithms to find matrix containing minimal sets requires the same number of operations in both cases. For the MOCUS algorithm, this part must be applied twice because it gives minimal cut sets/minimal paths in one run. In this part algorithm of Liu and Chiou algorithm is superior. The result by Liu and Chiou algorithm contains all path sets and cut sets. To find the minimal path sets is computationally demanding. The MOCUS algorithm provides a matrix containing in its rows minimal cut sets/minimal path sets. Redundant rows must be eliminated. There is no clear result which representation is better to find minimal sets. Performance of the bounds by (4), (5) and (6) is illustrated by example on the "three-motor" system on interval $0 \leq \mathrm{t} \leq 300$ hours. We assume the system with independent, identically exponentially distributed times to failure (MTTF=500 hours, $\lambda = 1/500$).

Trivial bounds fail for such a system with $n = 30$ components. Lower bound is close to zero; the upper bound is one. Min-max bounds (see (5)) also fail, its lower bound is close to zero. The minimal sets bounds (see (4)) are the best for this example; but they cannot be further improved by a combination of the other bounds. The bounds do not provide exact reliability function, because the minimal sets are not 2-by-2 disjoint. The minimal bounds are quite broad, especially due to its lower bound.

Fig. 1: Minimal sets bounds for the reliability of the "three-motor"



Source: authors

Conclusion

The aim of the paper was to determine which setting of a system is more efficient to find its minimal sets reliability. The recursive top-down algorithm to find minimal sets for Petri Nets and the MOCUS algorithm for fault trees were analyzed by the example of the "three-motor" system (Vesely et al., 1981). This study showed no approach is better if both minimal path sets and minimal cut sets are required simultaneously. Furthermore, the numerical study of minimal sets bounds, "min-max" and trivial bounds showed, that minimal sets bounds are superior. They cannot be further improved by combining with other bounds. In future work, we focus on the assessment of more algorithms to find minimal sets. The three bounds will be analyzed by numerical studies in more detail. The tightness of minimal sets bounds will be compared with Bonferroni-type bounds using only minimal cut sets (Limnios 2007).

Acknowledgment

The first author was supported by the grant F4/20/2020 (Metody pro výpočet rizika, spolehlivosti a pohotovosti složitých systémů) by IGS of the University of Economics in Prague.

References

Barbu, V., Boussemart, M., Limnios, N. (2004). Discrete-time semi-Markov model for reliability and survival analysis. *Communications in Statistics – Theory and Methods*. 33(11-12). 2833-2868.

Bause, F., Kritzinger, P. S. (2002). Stochastic Petri Nets. An Introduction to Theory. Braunschweig/Wiesbaden: Friedr. Wieweg & Sohn Verlagsgesellschaft GmBh, 2002. ISBN 3-525-15535-3.

Fussell, J. B., Vesely, W. E. (1972). A new methodology for obtaining cut sets. *Amer. Nucl. Soc. Trans.*, 15(1), 262–263.

Limnios, N. (2007). Fault trees. Newport Beach, CA: ISTE Ltd., 2007. ISBN 978-1-905209-30-9.

Liu, T. S., Chiou, S. B. (1997). The application of Petri Nets to failure analysis. *Reliability Engineering and System Safety*. 57(2), 129-142.

Moloy, M. K. (1981). *On the Integration of Delay and Throughput Measures in Distributed Processing Models.* Ph.D. thesis. The University of California.

Natkin, S. (1980) *Les Reseaux de Petri Stochastiques et leur Application a l'Evaluation des Systemes Informatiques.* Paris. PhD thesis. CNAM.

Petri, C. A. (1962). *Kommunikation mit Automaten. Bonn.* PhD thesis. Universitaet Bonn.

Rausand, M., Oien, K. (1996). The basic concepts of failure analysis. Reliability Engineering and System Safety. 53(1), 73-83.

Rosenthal, A. A. (1975). Computer scientist looks at reliability computations. In*: Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 133–152.

Vesely, W. E., et al. (1981). *Fault tree handbook*. Washington, D.C.: U.S. Nuclear Regulatory Commission. NUREG-0492.

Vozár, Ondřej. (2020) Equivalence of Fault Trees and Stochastic Petri Nets in Reliability Modelling. Statistika: *Statistics and Economy Journal*. 100(3), 282-295.

Contacts

Ing. Ondřej Vozár
University of Economics, Prague
Dept. of Statistics and Probability
W. Churchill Sq. 4
130 67 Prague
vozo01@vse.cz

doc. RNDr. Luboš Marek, CSc.
University of Economics, Prague
Dept. of Statistics and Probability
W. Churchill Sq. 4
130 67 Prague
marek@vse.cz