PERIODICA POLYTECHNICA SER. EL. ENG. VOL. 45, NO. 2, PP. 109–118 (2001)

A DISTANCE MODEL FOR SAFETY-CRITICAL SYSTEMS

Miklós SZIJÁRTÓ, Dietmár GRŐGER and Gábor KALLÓS

Department of Computer Science
Széchenyi István University,
H–9026, Egyetem tér 1., Győr, Hungary
e-mail: szijarto@sze.hu, groger@sze.hu, kallos@sze.hu

Received: October 31, 2001; Revised: May 9, 2002

Abstract

In this paper we introduce a new, theoretical model for safety-critical systems in which the distance from the dangerous conditions can be measured. To describe these systems we use besides the graph model Petri nets, too. We illustrate the theoretical discussion with some simple examples.

Keywords: safety-critical systems, distance model, Petri nets.

1. Introduction

In real life there are a lot of systems, which are very difficult to describe. Handling them is usually very complicated, in a lot of cases we are not able to give correct answers even to easy questions. However, for most systems the questions corresponding to the safety of the systems are very important. We call a system safety-critical if its abnormal operation might endanger human lives and cause significant financial damage. For example in railway systems there are a lot of safety-critical ones. The latest and probably most important results about the investigation of safety-critical systems can be found e.g. in [2] and [5]. Of course, absolute safety is an unobtainable goal, at least for a very broad class of systems, if not for all. There are a lot of factors to consider, e.g. the complexity of the system, hidden failures, human errors, etc. A possible way of handling this situation is to 'predict' the closeness of dangerous system-states, and avoid them, if possible.

There are several references in this topic, but generally well applicable results are not known yet. In this paper we examine these systems from a rigorous mathematical point of view, by describing a mathematical model to compute the 'closeness' of critical (dangerous) conditions in safety-critical systems, using graphs. The theory of distance and probability models described below is an encouraging new result. In some simple cases we examine the possibility of practical applications, too.

The handling of these systems usually needs concurrent programming approaches. Details and some general problems can be found e.g. in [1] and [4]. To describe concurrent systems, there are some other structures besides the graphs, such as Petri nets. That is the reason why in the second part of this paper a Petri net model will be discussed, preserving the results achieved in the first part.

2. Graphs for Safety-Critical Systems

For a (real-life) system let us introduce a graph $\mathcal{G}$ in the following manner. We denote the status (or condition) of the system in a given moment with a node. The status of the system can change in the next moment, so from this node edges lead to other nodes. These edges represent the transitions between the conditions. Cycles are allowed, too.

In the following we increase the expressive power of this model by labeling the edges of the graphs in two different manners.

3. Distance Model

We initiate distances as follows (our graphs are directed):

a) edge
Let us denote the distance from status i to status j with $d_{i\to j}$. In the simplest case all distances are 1, but usually $0 < d_{i\to j} < \infty$.

b) way
Going on consecutive edges the distances are summarized, so distance is additive. Thus, for conditions i and j let $d_{i,j} = \sum_{k=1}^{n-1} d_{c_k \to c_{k+1}}$, where $c_1 = i$ and $c_n = j$.

c) between two nodes
In this case we have to consider all ways connecting these two nodes. Thus, for the resultant distance $d_{i|j}$ we have $d_{i|j} \leq \min(d_{i,j})$, according to real life. The equality can be maintained in some cases, e.g. if one of the $d_{i,j}$-s is 0, if all $d_{i,j}$-s are ∞, or if there is only one way from i to j. There are some other possibilities, too (see example below). Of course usually $d_{i|j} \neq d_{j|i}$.

d) between a node and a set (of nodes)
Similarly, as in point c).

EXAMPLE 1 Let us assume that in a distance model we can reach 2 dangerous conditions, a_1 and a_2 from condition c with distances $d_1 := d_{c,a_1}$ and $d_2 := d_{c,a_2}$, respectively.

System: $a_1 \longleftarrow c \longrightarrow a_2$

In this case obviously $d_{c,a} \leq \min(d_1, d_2)$, where a symbolizes the resultant danger condition, and $d_{c,a}$ depends on d_1 and d_2. If e.g. $d_1 = \infty$, then $d_{c,a} = d_2$. A possible solution to this problem is the use of the harmonic average, so we get

$$d_{c,a} = \frac{1}{\frac{1}{d_1} + \frac{1}{d_2}} \quad \left(= \frac{d_1 \cdot d_2}{d_1 + d_2}, \text{ if } d_1 \neq \infty \text{ and } d_2 \neq \infty \right).$$

4. Probability Model

a) edge
Let us denote the probability of the transition from condition i to condition j with $p_{i\to j}$. In the simplest case all probabilities are equal, but usually $0 < p_{i\to j} < 1$.

b) way
Going on consecutive edges the probabilities are multiplied, so the probability is multiplicative. Thus, for conditions i and j let $p_{i,j} = \prod_{k=1}^{n-1} p_{c_k\to c_{k+1}}$, where $c_1 = i$ and $c_n = j$.

c) between two nodes
In this case for the resultant probability $p_{i|j}$ we have $p_{i|j} = \sum p_{i,j}$, with $p_{i|j} \leq 1$. Of course usually $p_{i|j} \neq p_{j|i}$.

d) between a node and a set (of nodes)
Similarly, as in point c).

EXAMPLE 2 Let us consider a system in the probability model with conditions c_1, c_2 and c_3 and the transitions

trans. 1: $c_1 \longrightarrow c_2 \longrightarrow c_3$
$p_{c_1\to c_2} = 0.4, \quad p_{c_2\to c_3} = 0.2$
trans. 2: $c_1 \longrightarrow c_1 \longrightarrow c_3$
$p_{c_1\to c_1} = 0.5, \quad p_{c_1\to c_3} = 0.1$

The probability of transition 1 is

$$p^1_{c_1|c_3} = p^1_{c_1,c_3} = p_{c_1\to c_2} \cdot p_{c_2\to c_3} = 0.4 \cdot 0.2 = 0.08.$$

The probability that we arrive at c_3 from c_1 in at most two steps

$$p^2_{c_1|c_3} = p_{c_1\to c_3} + p_{c_1\to c_2} \cdot p_{c_2\to c_3} + p_{c_1\to c_1} \cdot p_{c_1\to c_3} = 0.1 + 0.08 + 0.05 = 0.23.$$

5. Connections between the Distance and Probability Models

To avoid dangerous situations in every condition we have to know how close the system will be to danger after the next step. In real life we usually only know the probability of a transition between conditions, the distance is not known. Thus, it is useful to find a connection between the two models, and for us now the transition is more important which makes distance from probability.

We are looking for a measure-function $\mu : (0, 1] \to \mathbf{R}_0^+$ which satisfies the following properties:

(i) continuous,

(ii) strictly monotonous decreasing,

$$p_1 < p_2 \Rightarrow \mu(p_1) > \mu(p_2),$$

(iii)

$$\mu(1) = 0 \text{ and } \lim_{p \to 0} \mu(p) = \infty,$$

(iv)

$$\mu(p_1 \cdot p_2) = \mu(p_1) + \mu(p_2),$$

(v) for parallel ways we have

$$\mu(p_1 + p_2) = \mu(p_1) \amalg \mu(p_2),$$

where $\amalg$ is a parallel composition operator.

Points (i)-(v) were chosen for real life considerations. E.g. point (ii) asserts that if the probability of reaching condition 1 is less than that of condition 2, then condition 2 is closer than condition 1. Point (iii) asserts that the distance of an impossible event is infinite. To point (v), operator $\amalg$ is not entirely defined yet, we can use e.g. the harmonic average.

Considering properties (i)–(iii) we have several different function candidates, e.g.

$$d_{i\to j} \sim \frac{1}{p_{i\to j}} - 1 \text{ or } \operatorname{ctg}\left(p_{i\to j} \cdot \frac{\pi}{2}\right) \text{ or } \log \frac{1}{p_{i\to j}} = -\log p_{i\to j}.$$

However, from property (iv) which can be rewritten in the form

$$d_{i,k} = d_{i,j} + d_{j,k}$$

follows that the solution can only be a kind of logarithmic function ([3]).

So for our function $d_{i\to j} \sim \log \frac{1}{p_{i\to j}} = -\log p_{i\to j}$. Knowing that $0 \leq p_{i\to j} \leq 1$, we have $\infty \geq -\log p_{i\to j} \geq 0$. Obviously [1]

$$-\log p_{i\to j} - \log p_{j\to k} = -\log(p_{i\to j} \cdot p_{j\to k}),$$

and assuming the form $c(-\log p_{i\to j}) + d$ we can choose $d = 0$. The base of the logarithm can be an arbitrary number a, with $a > 1$ from property (ii).

Thus, we have the desired connection between the two models. We can specify the distance from the danger (starting from the probability model) in the following manner:

a) Starting from a given condition we specify the probability of reaching the danger(ous conditions).

[1] The $-\log p_{i\to j}$ relationship is not totally new in literature. It was presented formerly e. g. by C. E. SHANNON in his information theory ([7]).

b) Using the logarithmical proportionality we change to the distance model, getting the distance from the danger this way. Now the distance is determined independently of a constant multiplier. We can refine our model if we know the exact value of at least one of the distances (see the following example).

EXAMPLE 3 Let us assume that in a probability model we can directly go into three conditions from a given condition c_1, dangerous (a_1 and a_2). How far are we from the danger (denoted by a)? [2]

System:

$$\begin{array}{ccccc} a_2 & \longleftarrow & c_1 & \longrightarrow & a_1 \\ & & \downarrow & & \\ & & c_2 & & \end{array}$$

where $p_{c_1 \to c_2} = 0.85$, $p_{c_1 \to a_1} = 0.1$, $p_{c_1 \to a_2} = 0.05$. Then $p_{c_1,a} = 0.1 + 0.05 = 0.15$, $d_{c_1,a} = -\log 0.15$, and $-\ln 0.15 \approx 1.8971$. This distance is only determined independently of a (yet unknown) constant multiplier.

We can determine the 'expected value' of the distance from the danger with another method, using a very simple estimate. Analysing the safe transitions

$$0.85^4 \approx 0.5220 > 0.5 > 0.85^5 \approx 0.4437,$$

i.e. we expect the system to run into danger from c_1 in $4 - 5$ steps. Thus, using the function ln is suitable to apply a constant multiplier $c \approx 2.3$ to get the correct distance.

6. Petri Nets

Petri nets are special graphs. With their use we are able to examine complex concurrent systems effectively. In this section we briefly summarize the basic definitions from the Petri net theory. More detailed discussion can be found e.g. in [4] and in [6].

In a directed bipartite graph let us call the elements of the first node-set places (S elements, from the German word Stellen), and those of the second transitions (T elements). The connections between the places and the transitions are represented with arcs, this results in a relation which is called the flow relation.

DEFINITION 1 A triple $N = (S, T, F)$ is called a Petri net if

a) The sets S and T disjoint, $S \cup T$ is finite,
b) $F \subseteq (S \times T) \cup (T \times S)$ is a binary relation, the flow relation of N.

[2] Of course, this model is over-simplified because we omit the analysis of the behaviour of the system after conditions a_1, a_2 and c_1.

Graphically, the S elements are represented with circles, while the T elements with boxes. We represent the flow relation with arcs between the circles and boxes.

The theory of Petri nets was developed by C. A. PETRI in 1962. He used these nets to describe connections between events and conditions. To the occurrence of an event the realization of some conditions is needed, and after it the realization of some other new conditions starts. Events and conditions are symbolized with circles and boxes, respectively. The realization of a condition is marked graphically by a token (dot symbol) in the circle. In one circle there can only be one token, since the condition is either satisfied or not. According to the above description, we use a marking function $M_1 : S \to \{0, 1\}$. Thus, $M(S) = 1$ and $M(S) = 0$ is denoted in the net by $\odot$ and $\bigcirc$, respectively.

The concept of Petri net was generalized by A. W. HOLT in 1968. He allowed more than one token in one place. Thus, we initiate a weight function, $M_2 : S \to \mathbf{N}$.

DEFINITION 2

1 A transition is *firing* if the weights of its input places are non-zero (in a given moment).
2 The *action* of the transitions changes the weights, decreasing the weight of all input places and increasing the weight of all output places (with one unit) – during this tokens can disappear or arise.

7. Application of Petri Nets in Safety-Critical Systems

We can characterize a system-state $\mathcal{A}_i$ with a list, which contains the places with token(s). If there are $n > 1$ tokens in a given place, then this place can be found in the list n-times. Concurrency is realized with the use of parallel ways. Then from transition T_i we can reach more than one places. In this case during the action of the given transition at least one token arises. In '*or*' construct we can reach more than one transitions from place s_i. In this case the number of tokens does not change, the system-flow can proceed only in one direction.

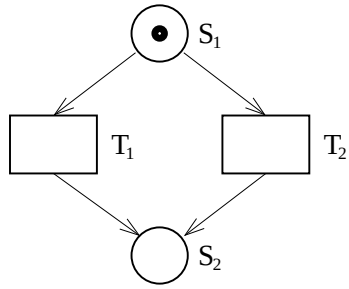

Fig. 1. 'Or' construct

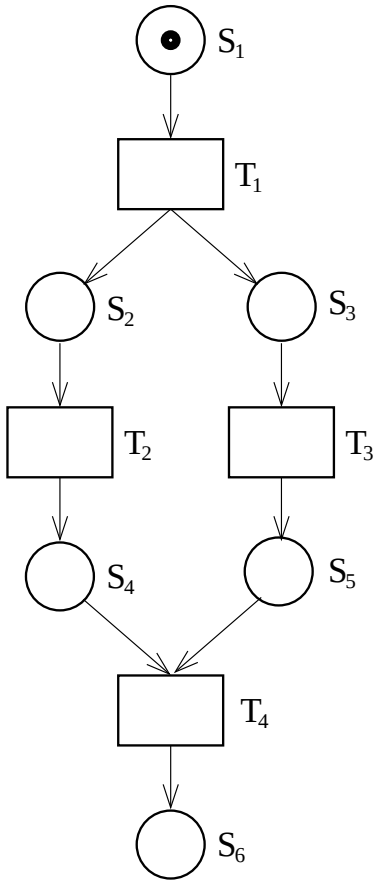

Fig. 2. Concurrency

The possible system-states in *Fig. 1* are $\mathcal{A}_1 = (s_1)$ and $\mathcal{A}_2 = (s_2)$.

The possible system-states in *Fig. 2* are $\mathcal{A}_1 = (s_1)$, $\mathcal{A}_2 = (s_2, s_3)$, $\mathcal{A}_3 = (s_2, s_5)$, $\mathcal{A}_4 = (s_3, s_4)$, $\mathcal{A}_5 = (s_4, s_5)$, $\mathcal{A}_6 = (s_6)$.

According to our former results we have to 'develop' the distance and probability models for Petri nets. First, let us give distances $d(T_i)$ and probabilities $p(T_i)$ to the transitions. As in real life we stipulate $d(T_i) \geq 0$. Probabilities clearly satisfy $0 \leq p(T_i) \leq 1$. Furthermore, for transitions which can be reached from a given place $\sum p(T_i) \leq 1$ holds, i.e. the token remains unchanged with probability $1 - \sum p(T_i)$ (which is allowed in assyncron Petri nets). This essentially means that the system can have a transition $c \to c$ with a probability greater than 0.

8. Distance Model

We initiate distances for lists containing places (i.e. for system-states):

Let us assume that state $\mathcal{A}_j$ follows state $\mathcal{A}_i$. Then $d(\mathcal{A}_i, \mathcal{A}_j)$ is computed taken the rules for normal graphs – concerning the possible 'or' construct and concurrency (see the following example). If $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ is a sequence of consecutive system-states (without concurrency and 'or' construct), then

$$d(\mathcal{A}_1, \mathcal{A}_n) = \sum_{i=1}^{n-1} d(\mathcal{A}_i, \mathcal{A}_{i+1}),$$

where $d(\mathcal{A}_i, \mathcal{A}_{i+1}) = d(T_i)$ (which is only true in this simple case).

EXAMPLE 4 In the previous net with 'or' construct

$$d(\mathcal{A}_1, \mathcal{A}_2) = \frac{d(T_1)d(T_2)}{d(T_1) + d(T_2)} \quad \text{or } \min(d(T_1), d(T_2)).$$

In the previous net with parallel ways

$$\begin{aligned} d(\mathcal{A}_1, \mathcal{A}_2) &= d(T_1), \\ d(\mathcal{A}_2, \mathcal{A}_4) &= d(T_2), \\ d(\mathcal{A}_2, \mathcal{A}_5) &= \max(d(T_2), d(T_3)), \\ d(\mathcal{A}_1, \mathcal{A}_6) &= d(T_1) + \max(d(T_2), d(T_3)) + d(T_4). \end{aligned}$$

We use the max() function 'intuitively', following real-life considerations.

9. Probability Model

Let us assume that state $\mathcal{A}_j$ follows state $\mathcal{A}_i$.

Without 'or' construct and parallel ways, $p(\mathcal{A}_i, \mathcal{A}_j)$ is the probability $p(T_i)$, according to the transition. If there is an 'or' construct, then the probabilities are summarized, in the case of parallel ways they are multiplied. If $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ is a sequence of consecutive system-states without 'or' construct, then

$$p(\mathcal{A}_1, \mathcal{A}_n) = \prod_{i=1}^{n-1} p(\mathcal{A}_i, \mathcal{A}_{i+1}).$$

Thus, we have the interesting situation that in the probability model concurrency and consecutivity are computed with the same formula in spite of the different background (see the following example).

EXAMPLE 5 In the previous net with 'or' construct

$$p(\mathcal{A}_1, \mathcal{A}_2) = p(T_1) + p(T_2).$$

In the previous net with parallel ways

$$p(\mathcal{A}_1, \mathcal{A}_6) = p(T_1) \cdot p(T_2) \cdot p(T_3) \cdot p(T_4),$$

since the token(s) has/have to overcome transitions T_2 and T_3 to reach system-state $\mathcal{A}_6 = (s_6)$.

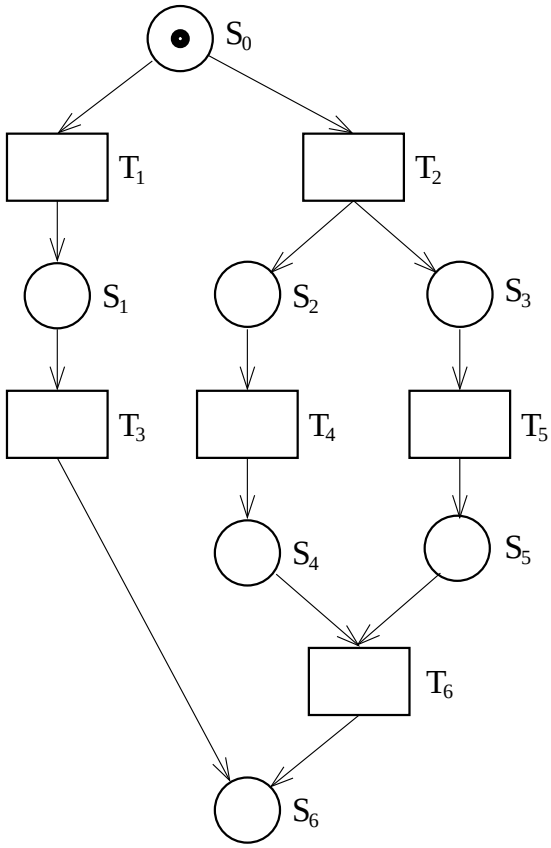

Fig. 3. Example-net

EXAMPLE 6 The possible system-states in *Fig. 3* are

$\mathcal{A}_0 = (s_0)$, $\mathcal{A}_1 = (s_1)$, $\mathcal{A}_2 = (s_6)$, $\mathcal{A}_3 = (s_2, s_3)$, $\mathcal{A}_4 = (s_2, s_5)$, $\mathcal{A}_5 = (s_3, s_4)$, $\mathcal{A}_6 = (s_4, s_5)$,

$d(\mathcal{A}_0, \mathcal{A}_2) =$ (two possibilities)

$$1^\circ = \min(\underbrace{d(T_1) + d(T_3)}_{d_1}, \underbrace{(T_2) + \max(d(T_4), d(T_5)) + d(T_6)}_{d_2}),$$

$$2^\circ = \frac{d_1 \cdot d_2}{d_1 + d_2},$$

$$p(\mathcal{A}_0, \mathcal{A}_2) = p(T_1) \cdot p(T_3) + p(T_2) \cdot p(T_4) \cdot p(T_5) \cdot p(T_6).$$

10. An Algorithm

Finally, we present an algorithm for systems which can be described by graphs (Petri nets) without circles.

1. Let us order the nodes in the following way: if $i < j$, then it is only allowed to go from i to j.
2. Let us determine the length of the ways in the graph, using the edges.
3. Using the ways and the operators above, the distances can now be introduced.

This method is applicable to wide classes of safety-critical systems.

References

[1] BURNS, A. – DAVIES, G., *Concurrent Programming*, Addison-Wesley Publ., 1993.
[2] DAVIS, D. et al., Safety-Critical Systems, Special Feature, *Computing & Control Enginering Journal*, **5** (1994).
[3] DIEUDONNÉ, J., *Foundations of Modern Analysis*, Academic Press, New York and London, 1968.
[4] JANICKI, R. – LAUER, P. E., *Specification and Analysis of Concurrent Systems*, Springer-Verlag, Berlin, 1992.
[5] REDMILL, F. – ANDERSON, T., *Safety-critical Systems*, Chapman & Hall, 1993.
[6] REISIG, W., *Petri Nets – an Introduction*, Springer-Verlag, Berlin, 1985.
[7] SHANNON, C. E., A Mathematical Theory of Communication, *The Bell System Technical Journal*, **XXVII** (1948).