A Qualitative Model for Conditions in Safety-Critical Systems *

Miklós Szijártó (szijarto@rs1.szif.hu)
Dietmár Grőger (groger@rs1.szif.hu)
Gábor Kallós (kallos@rs1.szif.hu)
Department of Computer Science,
Széchenyi István College, H-9026,
Hédervári út 3., Győr, Hungary.

HU ISSN 1418-7108: HEJ Manuscript no.: ANM-991102-A

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. The connection between this distance model and real-life probability model will be discussed, too. We illustrate the theoretical discussion with some simple examples.

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, questions concerning the safety of the systems are very important. These problems are examined by the theory of safety-critical systems. The newest and probably most important results about this theory can be found e.g. in [2] and [5].

In spite of the many references, there are no universal results, which examine these systems from rigorous mathematical point of view. In this paper we describe a mathematical model to compute the "closeness" of critical (dangerous) conditions in safety-critical systems, using graphs. The theory of the distance and probability model described below is a hopeful new result. In some simple cases we examine the possibility of practical applications, too.

Handling these systems usually needs concurrent programming approach, details and some general problems can be found e.g. in [1] and [4]. To describe concurrent systems, besides the graphs there are some other structures. A possible improvement can be, if we discuss the validity of our results in some special graph models. We will revert to this question in a subsequent paper.

*The topic of this paper was partially presented by the authors in conferences [6] and [7].

2 Possible models

We can specify the conditions of a system in two different ways. If the system is very complicated, then usually one system-condition can be described only with a lot of surrounding elements.

a) Considering the system as a whole, one condition represents all of the information about the surrounding elements. During the examination we can not see these elements.

b) In the other case we describe the conditions as vectors. The components of these condition-vectors are the conditions of the surrounding elements. From vector a we can reach vector b, if from the conditions in vector a with the change of surrounding elements in one or more steps we get the conditions in vector b.

In both of the cases it is possible, that several surrounding elements change in one step. Of course, the second model fits real life better, although the management of it is more complicated.

The chance of reaching dangerous conditions can be specified in two models.

2.1 Distance model

We initiate distances in the following manner (our graphs are directed):

a) edge

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

b) way

Going on subsequent edges the distances are summarized, so the distance is additive.

c) between two nodes

In this case we have to consider all of the ways connecting these two nodes. Thus, according to real life for the resultant distance $d_{i,j}$ we have $d_{i,j} \leq \min(d_{i\to j})$. The equality can holds only in degenerated cases, if one of the $d_{i\to j}$-s is 0 or if all of the $d_{i\to j}$-s are ∞. 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

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

System: $\mathrm{a}_1 \longleftarrow \mathrm{c} \longrightarrow \mathrm{a}_2$

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 for this problem is the use of the harmonic average, so we get

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

2.2 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 of the probabilities are equal, but usually $0 < p_{i\to j} < 1$.

b) way

Going on subsequent edges the probabilities are multiplied, so the probability is multiplicative.

c) between two nodes

In this case for the resultant probability $p_{i,j}$ we have $p_{i,j} = \sum p_{i\to j}$, 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

Let us consider a system in the whole-type 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: $c_1 \longrightarrow c_1 \longrightarrow c_3$

$p_{11\to 11} = 0.5 \quad p_{11\to 13} = 0.1$

The probability of transition 1 is

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

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

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

2.3 Connections between the distance- and probability models

To avoid the dangerous situations we have to know in every condition, how close the system will be to the danger after the next step. In real life usually we know only the probability of a transition between conditions, the distance is unknown. Thus, it is useful to find a connection between the two models, and for us now it is more important the transition, which makes distance from probability.

So we are looking for a function $\mu : (0, 1] \to \mathbf{R}_0^+$, which has the following properties:

(i) continuous,

(ii) strictly monotonously 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 paralell ways we have

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

where $\amalg$ is a paralell composition operator.

Considering properties (i)–(iii) we have more 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

$$d_{ik} = d_{ij} + d_{jk}$$

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

EXAMPLE

Let us investigate the problem with the candidate $d_{i \to j} \sim \frac{1}{p_{i \to j}} - 1$. In this case we search the solution in the form $d_{i \to j} = c \cdot \left(\frac{1}{p_{i \to j}} - 1\right) + d$. From property (iv) the following equality holds:

$$c \cdot \left(\frac{1}{p_{i \to j}} - 1\right) + d + c \cdot \left(\frac{1}{p_{j \to k}} - 1\right) + d = c \cdot \left(\frac{1}{p_{i \to j} \cdot p_{j \to k}} - 1\right) + d,$$

from which with simple transformations

$$\frac{c}{p_{i \to j}} + \frac{c}{p_{j \to k}} - 2c + 2d = \frac{c}{p_{i \to j} \cdot p_{j \to k}} - c + d,$$

$$\frac{cp_{i \to j} + cp_{j \to k}}{p_{i \to j} \cdot p_{j \to k}} - c + d = \frac{c}{p_{i \to j} \cdot p_{j \to k}}.$$

Thus, we are not able to choose c and d independently from $p_{i \to j}$ and $p_{j \to k}$, so this function is not appropriate.

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

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

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).

b) Using the logarithmics proportionality we change to the distance model, getting so the distance from the danger (finally, we apply a constant multiplier if needed).

EXAMPLE

Let us assume, that in a whole-type probability model from a given condition c_1 we can go directly into three conditions, from which two are dangerous (a_1 and a_2). How far are we from the danger?

System:

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

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 $p_{a_1 \to v} = 0.1 + 0.05 = 0.15$, $d_{a_1 v} = -\log 0.15$. Applying a probability estimate

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

i.e. the system runs into danger in $4 - 5$ steps, prospectively. Since $-\ln 0.15 \approx 1.8971$, using the function ln it is suitable to apply a constant multiplier $c = 2$ to get the correct distance.

Let us denote the inverse of function μ with $\pi : \mathbf{R}_0^+ \to [0, 1]$. Then π assures way through from distance model to probability model. Its required properties can be written similarly, as those of function μ:

(i) continuous,

(ii) strictly monotonously decreasing,

$$d_1 < d_2 \Rightarrow \pi(d_1) > \pi(d_2),$$

(iii)

$$\pi(0) = 1 \text{ and } \lim_{d \to \infty} \pi(d) = 0,$$

(iv)

$$\pi(d_1 + d_2) = \pi(d_1) \cdot \pi(d_2),$$

(v) for paralell ways we have

$$\pi(d_1 \amalg d_2) = \pi(d_1) + \pi(d_2).$$

Similarly as above it can be proved, that π is some kind of exponential function. Usually it can be written in the form a^{-d}, where $a > 1$ from property (ii).

3 Problems with operator II

From property (iv) of functions μ and π we have to specify operator II so, that it has to satisfy the following two equalities:

$$p_1 + p_2 = \pi(\mu(p_1) \amalg \mu(p_2)) \text{ and}$$

$$d_1 \amalg d_2 = \mu(\pi(d_1) + \pi(d_2)).$$

Above we have applied the harmonic average to "produce" operator II, but – as it will be presented below – we are not able to fit it exactly to these requirements. From the definitions of functions μ and π follows

$$d_1 \amalg d_2 = -\log_a(a^{-d_1} + a^{-d_2}),$$

so we would need

$$\frac{d_1 \cdot d_2}{d_1 + d_2} = -\log_a(a^{-d_1} + a^{-d_2}).$$

Choosing $d_1 = d_2 \neq 0$ we get

$$\frac{d_1}{2} = -\log_a(2a^{-d_1}),$$

$$a^{-\frac{d_1}{2}} = 2a^{-d_1},$$

$$2 = a^{\frac{d_1}{2}}$$

with the obligation, that this must be held for all d_1. This is clearly not possible.

Thus, we have "two different" operators II. Using the harmonic average we get only an approach. The result is exact if one of the distances d_1 and d_2 is ∞, in other cases there is an error-term. However, this approach is well useable, because of its simplicity. But, by an exact transition from probability model to distance model, we have to use the logarithmic formula for operator II.

References

[1] Alan Burns, Geoff Davies, *Concurrent Programming*, Addison-Wesley Publ., 1993.

[2] Dai Davis et al., Safety-Critical Systems, Special Feature, *Computing & Control Enginering Journal*, Volume 5, 1994.

[3] J. Dieudonné, *Foundations of Modern Analysis*, Academic Press, New York and London, 1968.

[4] Ryszard Janicki, Peter E. Lauer, *Specification and Analysis of Concurrent Systems*, Springer-Verlag, Berlin, 1992.

[5] Felix Redmill, Tom Anderson, *Safety-critical Systems*, Chapman & Hall, 1993.

[6] Miklós Szijártó, Dietmár Grőger, Gábor Kallós, Biztonságkritikus rendszerek állapotainak kvalitatív modellje, *Jubileumi Tudományos Konferencia*, SZIF, Győr, 1998.

[7] Miklós Szijártó, Dietmár Grőger, Gábor Kallós, Biztonságkritikus rendszerek távolság modellje, *Akadémiai Napok*, SZIF, Győr, 1999.