9

Risk and Reliability Analysis of Flexible Construction Robotized Systems

Calin Ciufudean
Stefan cel Mare University of Suceava
Romania

1. Introduction

We consider this discussion, as there is a lot of confusion about the definition of the risk and the reliability of flexible manufacturing system analysis, both being risk analysts and decision makers. Thinking of risk and reliability analysis of flexible construction robotized systems (FCRS's) from a probabilistic perspective, we come to the conclusion that probability is a measure of expressing uncertainty about the process seen through the point of view of the assessor (i.e. the controller of a process), and based on some background information and knowledge that we have at the time we quantify our uncertainty. A sharp distinction between objective, real risk, and perceived risk cannot be made, simply because complete knowledge about the world does not exist in most cases, and the analysis provides a tool for dealing with these uncertainties based on coherence by using the rules of probabilities. If sufficient data become available, consensus in probability assignments may be achieved, but not necessarily, as there are always subjective elements involved in the assessment process. Risk is primarily a judgement, not a fact. As risk expresses uncertainty about the world, i.e. about consequences and outcomes of an activity, risk perception has a role to play to guide decision makers. It is, however, not obvious how such a thinking should be implemented in practice, in a decision making context, and different frameworks can be established. This approach emphasises the so-called observable quantities and their prediction (Aven, 2004). Examples of observable quantities are the number of facilities and production volumes. The starting point is an activity or a system that we would like to analyse now, to provide decision support for investments, design, operation etc. Therefore, the interesting quantities for risk and reliability analysis of an FCRS are the performances of that system, for example measured by production, production loss, number of fatalities, and so on. Unfortunately, in most cases, we are led to predictions of these quantities that reflect our expectations. But these predictions will normally not provide sufficient information; assessment of uncertainties is required. In order to express the uncertainties, we need a measure, and we choose the probability for measuring uncertainties.

2. Basic consideration on risk and reliability analysis

Basically, uncertainty related to any value the observable quantities will take, is expressed by probabilities. This uncertainty is a result of lack of knowledge.

The purpose of risk and reliability analysis is to provide decision support. This can be done by analysing and describing risk in a decision–making context, for example for a flexible construction robotized system (FCRS) efficient job schedule, these tasks define the area of the FCRS availability. In our view the scientific basis of risk and reliability analysis (e.g. the determination of the availability of the considered manufacturing system) can be summarized by the following points (Kask & Dechter, 1999), (Aven, 2004):

1. Knowledge about the system's performance and associated observable quantities are described by models, observed data and expert opinions;
2. Coherent and certainty assessments using the rules of probability.

Models: a number of different types of models are used in risk and availability analysis. These include both quantity–oriented and event–oriented models.

The purpose of quantity–oriented models is to predict the value of an observable quantity C by expressing knowledge of C in terms of a set of quantities $X = (X_1, X_2, \ldots, X_n)$, and the functional relationship f between C and X, i.e., $C = f(X)$. The function f is typically established on the basis of a mixture of commonly accepted, constitutive models from the field of physics, mathematics, chemistry, empirical knowledge, and more intuitive assumptions regarding the analysed system.

While the quantity–oriented models describe a functional relationship between a set of factors and the numeric value of quantity, event–oriented or logical models describe the conditions under which events occur. Such models consist of conditions and logical terms, and they usually have a binary outcome space (typically 0-1, failure–not failure, etc). In risk models logical models capture one's attention by developing events from a low initial level to large scale scenarios, threatening human lives and health, environmental and economic values. Three basic examples of logical models in risk and reliability analysis are:

$$F = X_1 - X_2 \leq 0 \tag{1}$$

$$F_s = X_1 \cup X_2 \tag{2}$$

$$F_P = X_1 \cap X_2 \tag{3}$$

Equation (1) describes a failure event F according to a simple load capacity consideration. F occurs when a load X_2 takes a higher value than the capacity value X_1. Equation (2) shows the conditions of failure of a two components system F_s, i.e., at least one of the two components X_1 or X_2 fails. Equation (3) represents the failure of a system of two components in parallel, i.e., both components fail. As a matter of fact, natural sciences provide theories and laws describing real world phenomena. These theories and laws are models of the world or they provide a basis for establishing models of the world, i.e. simplified representations of the world. For a specific risk availability analysis, application of the models may be better or worse in describing the world and useful for its purpose. Strictly speaking, a model is always wrong; otherwise it would not be a model – a simplification of the world. The accuracy of the models as representations of the world (i.e. the analysed system) needs to be addressed to. We notice that there is always a balance to be made, i.e., we need to simplify the system (i.e. the world) to obtain a tool that can be used in practice, to see the key factors; and this would result in less accuracy. It is difficult to give a detailed specification of what a satisfactory model is. How accurate must a model be in order to be considered acceptable? Well, the ultimate requirement for an availability model is that any improvement in the model to make it more accurate should not lead to a change of the conclusions that the analyst draws.

We must notice that this requirement may be difficult to verify – the best the analyst can do in most cases is to use sensitivity analysis to see how changes in the model affect the result. A model C = f (X) is a purely deterministic representation of factors judged to be essential by the analyst. It provides a framework for mapping uncertainty about the observable quantity of interest, C, from epistemic uncertainty related to the observable quantities X, and does not introduce by itself additional uncertainty. In this approach the model is merely a tool judged to be useful for expressing the knowledge of a system. The model is a part of the background information of the probability distribution specified for C. If we change the model, we change the background information.

We must say that, when conducting a risk analysis we cannot "verify" an assigned probability, as it expresses the analyst's uncertain prior observation. What can be done is a review of the background information used as the rationale for the assignment, but in most cases it will not be possible to explicitly document all the transformation steps from this background information to the assigned probability. We do not search for the true probabilities, as such numbers do not exist, but for a consistent assessment of uncertainties steaming from the result of lack of knowledge. It seems that some probabilities are easy to assign and look sure, others are vague and it is doubtful that the single number means anything. Should the vagueness not be specified? In order to provide a basis for the reply, let us remember that probability P(A) is in fact a short version of a conditional probability of A given the background information K, i.e., P(A) = P(A/K). This means that even if we assign the same probability for two probabilities, they may be considered different, as the background information is different. For example, in some cases we may know much about the process and phenomena leading to the event A, and in other cases, very little, but still we assign a probability of 0.50 in both cases (Aven, 2004). However, by considering several similar events of the type A, i.e., we change the performance measure; the difference in the background information will often be revealed. We conclude that we always need to address the background information, as it provides a basis for the evaluation. Of course, there are a number of potential pitfalls in such judgement processes, but the risk analysts are aware of them and make use of tools in order to avoid them. Such tools include calibration procedures, the use of reference probabilities, standardisation, and more detailed modelling (Russell & Norvig, 2003). In order to exemplify the given approaches, we consider the following example, where an efficient discrete event simulation model has been proposed for reducing the risk of the availability analysis based on failure for FCRS's. The proposed model has been successfully applied and tested for the reliability value analysis of FCRS's.

3. Modelling the controllers of flexible construction robotized systems

An important characteristic of flexible construction robotized systems (FCRS's) is modularity. Since building materials transfer lines are widely used and constitute an important subclass of FCRS's, in this paper we focus on formal analysis of logic controllers for high volume transfer lines. We first propose a systematic approach to model and to verify the space size of the logic controllers using Petri nets. We consider that Petri net models of FCRS's can be decomposed in a few typical modules and the analysis of the entire system is made following a bottom-up algorithm. We have chosen to model the logic controllers with Petri nets, in order to take advantage of well developed theories for analysis and verification.

A controller is a discrete event supervisory system which controls synchronized sequences of basic operations of each data transmission cell in order to achieve the goal of the entire transmission system. Although logic controllers are very important in machining industry there is not yet a standard integrated tool, which is powerful, versatile and which can carry out formal analysis of correctness. High volume transfer lines are very usually machining systems in the FCRS's for mass building resources flow. In this paper we propose a systematic way to verify and implement the algorithms of the logic controllers for high volume transfer lines, using Petri nets. Petri nets are a well defined system modeling methodology, although the typical state-space explosion is problematic. For this reason, in this paper we describe an approach to estimate the state-space size of the Petri nets. This estimation algorithm is based on subnets and interconnections that mean a bottom-up approach. This algorithm allows typical subnets and is extendable for development of additional interconnections. We notice that the problem of state-space size estimation of PN's is being pursued in two distinct manners: top-down and bottom-up (Ferrarini, 1992), (Ferrarini, 1994). The top-down approach can analyze entire models without identifying subnets or imposing design constraints. The bottom-up approach builds the PN's model to a set of interconnected subnets. We notice that at the expense of complete generality, the bottom-up approach offers better accuracy.

4. Petri nets models for FCRS's controllers

We will assume that the reader is familiar with Petri nets theory and their application to discrete event systems (such as those involved in data transmission) or we refer the reader to (Murata 1989), (Zhon & DiCesare, 1992). In an ordinary Petri net PN = (P, T, F, M_0), where P and T are two disjointed sets of nodes named, respectively, places and transitions. $F \subseteq$ (PXT) U (TXP) is a set of directed arcs. M_0: $P \rightarrow N$ is the initial marking.
Two transitions t_i and t_j are said to be in conflict if they have at least one common input place. A transition t is said to be conflict free if it is not in conflict with any other transition. A transition may fire if it is enabled. A transition $t \in T$ is said to be enabled at marking M if for all $p \in {}^*t$, $M(p) \geq 1$. The SPN's considered here are ordinary Petri nets with timed transitions. Timed transitions can be in conflict therefore we say that a marking is stable if no conflict transitions are enabled. In the following lines we assume that the initial marking is a stable marking. We note by (M,T) a stable marking reachable from M by firing t. The new stable marking M* is obtained from M according to some routing probability. The basic idea is that in order to guarantee that a stable marking can be reached we must ensure that the respective circuit contains at least one timed transition. A SPN can be defined by the following elements (Park, 1999), (Tilburg & Khargonekar, 1999): T_t - Set of timed transitions; $M_s(M,t)$ - Set of stable markings reachable from M by firing transition t; p(M*,M,t) - Probability of reaching a stable marking M* from M when t fires (obviously, we have: $p(M^*,M,t) = 0$ if $M^* \notin Ms(M,t)$); $F_t(.)$ - Distribution functions of the firing time of t.
The GSMP representation of the SPN can be characterized by the following parameters:
X(t,k) - Independent random variables, where $t \in T_t$, and $k \in N$(each X(t,k) has distribution F_t and corresponds to the time of the k^{th} firing of transition t); U(t,k) - Random variables on [0,1]. Each U(t,k) corresponds to the routing indicator at the k^{th} completion of t. $r_n(t)$ - Remaining firing time of transition t at S_n; S(t,k) - Independent uniform random variables on [0,1], where $t \in T_t$, $k \in N$ (each U(t,k) corresponds to the routing indicator at the k^{th}

completion of t); t_n - n^{th} completed timed transition; M_n - Stable marking reached at the firing of t_n; S_n - Completion time of t_n; τ_n - Holding time of marking M_{n-1}; V(t,n) - Number of instances of t among t_1 , …, t_n.
The dynamic behaviour of an SPN can be explained in the following way: at the initial marking M_0, set $r_n(t) = X(t,1)$, $\forall\ t \in T_t(M_0)$ and set $V(t,0) = 0$, $\forall\ t \in T_t$. All other parameters t_{n+1}, τ_{n+1}, s_{n+1}, $V(t,n+1)$, M_{n+1}, r_{n+1} can be determined recursively as usually done in discrete event simulation. Recursive equations are given in (Zhou & Twiss 1998). The following routing mechanism is used in GSMP:

$$M_{n+1} = \varnothing(M_n, t_{n+1}, U(t_{n+1},V(t_{n+1},n+1))) \tag{4}$$

Where $\varnothing$ is a mapping so that $P(\varnothing(M,t,U) = M^*) = P(M^*,M,t)$.
Following the approach given in (Hopkins, 2002), we suppose that the distributions of firing times depend on a parameter Θ. In perturbation analysis the following results hold (Watson & Desrochers 1994), where the performance measures under consideration are of the form $g(M_1, t_1, \tau_1, \ldots, M_n, t_n, \tau_n)$ and a shorthand notation g(Θ) is used:
a) For each Θ, g(Θ) is a.s. continuously differentiable at Θ and the infinitesimal perturbation indicator is:

$$\frac{dg(\theta)}{d\theta} = \sum_{i=1}^{n} \frac{\partial g}{\partial \tau_i} \cdot \frac{d\tau_i}{d\theta} \tag{5}$$

b) If $d \in [g(\Theta)]/d\Theta$ exists, the following perturbation estimator is unbiased:

$$\sum_{i=1}^{n} \frac{\partial g}{\partial \tau_i} \cdot \frac{d\tau_i}{d\theta} + \sum_{k=1}^{n} f_k(h_k) \cdot G_k \tag{6}$$

$$f_k = \frac{f_{tk+1}(L_k(t_{k+1}))}{F_{tk+1}(L_k(t_{k+1}) + y_k - F_{tk+1}(L_k(t_{k+1})))} \tag{7}$$

$$y_k = \min\{r_k(t) : \forall t \in T(M_k) - \{t_{k+1}\}\} \tag{8}$$

$$\tau_k = \frac{dL_k(t_{k+1})}{d\theta} - \frac{dX(t_{k+1})}{d\theta} \tag{9}$$

$L_k(t)$ is the age of time transition t at S_k; $G_k = g_{pp,k} - g_{DNP,k}$. The sample path $(M_1(\Theta), t_1(\Theta), \tau_1(\Theta), \ldots, M_n(\Theta), t_n(\Theta), \tau_n(\Theta))$ is the nominal path denoted by NP.
The $g_{DNP,k}$ is the performance measure of the k^{th} degenerated nominal path, denoted by DNP_k. It is identical to NP except for the sojourn time of the $(k+1)^{th}$ stable marking in DNP_k. $g_{pp,k}$ is the performance measure of a so-called k^{th} perturbed path, denoted by PP_k. It is identical to DNP_k up to time s_k. At this instant the order of transition t_k and t_{k+1} is reversed, i.e., the firing of t_{k+1} completes just before that of t_k in PP_k. We notice that by definition, DNP_k and PP_k are identical up to s_k. At s_k, the events t_k and t_{k+1} occur almost simultaneously, but t_k occurs first in DNP and t_{k+1} occurs first in PP_k.
The commuting condition given in (Hopkins, 2002) guarantees that the two sample paths became identical after the firing of both t_k and t_{k+1}. Our goal is to introduce a correction

mechanism in the structure of the SPN so that the transition t_k and t_{k+1} fire in the desired order, and the routing mechanism given in relation (4) is re-established. We will exemplify this approach, and we will correlate the theoretical assumption with some practical mechanisms in order to verify the approach. In a high volume transfer line (i.e., in a FCRS's, as shown above) the logic controller modules are related by synchronizations. Using these synchronizations, the Petri nets models for modules can be integrated in one Petri net for the entire logic controller (Zaitoon, 1996), (Murata, 1989). Some advantages of this module synthesis are that the structure of the entire net model is a marked graph and the synchronized transitions in the model have physical meaning.

The functional properties of the synthesized model can be analyzed using well-developed theories of marked graphs. The Petri net model of the entire system is defined as a modular logic controller.

The modules in a modular logic controller are simplified by the modified reduction rule to overcome the complexity in the Petri net model. For example, any transition which is not a synchronized transition can be rejected. Therefore, only synchronized transitions appear in the modular logic controller. Modules are connected by transitions. Each transition in a module is a synchronized transition, and appears in at least one other module. For example, in the figure 1 we have a modular logic controller which consists of three modules and three synchronized transitions. The initial place of each module has one token. The Petri net model for a logic controller is a reduced size model, which represents the specifications of the controller hierarchically. Therefore, the structure and initial marking of a modular logic controller should be live, safe, and reversible (Murata, 1989).

We notice that the logical behavior of the controller can be ensured from the functional correctness of its Petri net model. A common and convenient representation of a marked Petri net is by its state equation.

The main terms involved in the state equation of a Petri net are the incidence matrix, C and the initial marking M_0, which can be represented for the modular logic controllers, as the above given matrix, see relation (10).

Following the definition of an incidence matrix, for a Petri net with k modules and n_i number of places in the i^{th} module, the incidence matrix of each module, C_i, where i = 1, …, k, can be represented as a (n_i x m) matrix, where m is the number of transitions in the system. This matrix is constructed with the places of each module and the transitions of the system: $C_i(t)$.

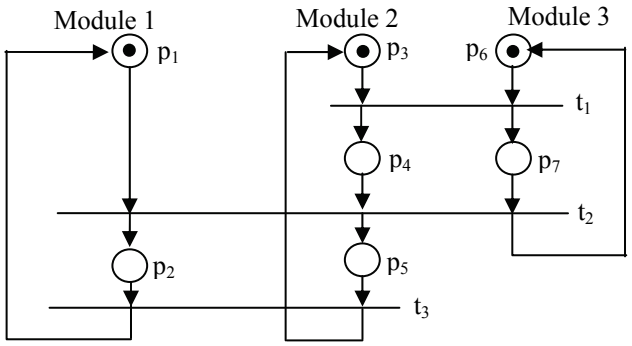


Fig. 1. An example of a modular logic controller

$$C = \begin{matrix} p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \end{matrix} \begin{bmatrix} & t_1 & t_2 & t_3 \\ C_1 & 0 & -1 & 1 \\ & 0 & 1 & -1 \\ C_2 & -1 & 0 & 1 \\ & 1 & -1 & 0 \\ & 0 & 1 & -1 \\ C_3 & -1 & 1 & 0 \\ & 1 & -1 & 0 \end{bmatrix}, M = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \tag{10}$$

The incidence matrix of the system can be constructed using the following equation:

$$C = \begin{bmatrix} C_1^+ & - & C_1^- \\ - & - & - \\ C_2^+ & - & C_2^- \\ - & - & - \\ & \vdots & \\ - & - & - \\ C_k^+ & - & C_k^- \end{bmatrix} = \begin{bmatrix} C_1 \\ - \\ C_2 \\ - \\ \vdots \\ - \\ C_k \end{bmatrix} \tag{11}$$

Where C_i^+ and C_i^- are post and pre – incidence matrices of the i^{th} module respectively and the incidence matrix C is a n x m matrix and $c_{ij} \in \{0,-1,1\}$. The initial places of a modular logic controller are assumed to be the first place of each module and can be represented by an n-dimensional vector. The initial marking is represented by:

$$M_0 \in \{0,1\}^n \tag{12}$$

Here 1 represents the initial places of the modules. This modular construction can be easily modified and reconfigured (i.e. it is suitable for FCRS's representation) by replacing incidence matrix of modules. The dynamic evolution of a modular logic controller can be determined by this incidence matrix and initial marking using the following relation (state equation):

$$M = M_0 + C \cdot f_C \tag{13}$$

Where, f_C is the firing count vector of the firing sequence of transition f in the net. An important parameter of the FCRS's is the resources flow volume. This is determined by the cycle time of a system in normal operation. Generally, performance analysis of event based systems is done by adding time specifications to the Petri net model. The performance analysis of timed Petri nets has been done for the evaluation of the cycle time. For strongly connected timed marked graphs, a classic method for computing the minimum cycle time C_T is given by the following relation (Park 1999), (Tilburg & Khargonekar, 1999):

$$C_T = \underbrace{\max}_{\nu\in\Gamma}\left\{\frac{D(\gamma)}{N(\gamma)}\right\} \tag{14}$$

Where, Γ is the set of directed circuits of the pure Petri net; $D(\gamma) = \sum_{p_i\in\gamma}\tau_i$ is the sum of times of the places in the directed circuit γ; N(γ) is the number of tokens in the places in directed circuit γ. As pointed out in (Zhou & Twiss, 1998), the cyclic behavior of timed Petri nets is closely related to the number of tokens and to the number of states in the directed circuit which decides the cycle time C_T. As we know, model analysis and control algorithms implemented with Petri nets are based on the model state-space, and hence they are adversely affected by large state-space sizes. Thus, in the next section we'll give a bottom-up approach for the state-space size estimation of Petri nets.

5. Size estimation of modular controllers of FCRS's

In order to estimate the state space of Petri nets, they are divided into typical subnets, i.e., subnets with basic interconnections, such as: series, parallel, blocking, resource sharing, failure repair inter-connection, etc. Each subnet is associated with a state counting function (Zaitoon, 1996) (SC-function) that describes the subnet's state-space size when it contains r "flow" tokens. We notice that "flow" tokens (those that enter and leave the subnet via its entry and exit paths) are different from control tokens in a controlled Petri net. Petri nets model the execution of sequential parallel and choice operations, which are abstracted to be subnets (SN). Figure 2 illustrates two subnets in series, where tokens pass from SN_1 to SN_2. The interconnection's SC-function is given by the following relation (Watson & Desrochers, 1994).

$$S_{series}(r) = \sum_{r} S_1(r_1)\cdot S_2(r_2) = \sum_{i=0}^{r} S_1(i)\cdot S_2(r-i) \tag{15}$$

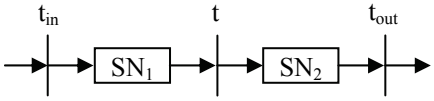


Fig. 2. Series interconnection of two Petri subnets

Analogous with the previous approaches, in the figure 3 we have the basic interconnections for parallel subnets (Fig.3.a); choice among subnets (Fig.3.b); blocking (Fig.3.c), and resource sharing (Fig.3.d).
The SC-functions (Zaitoon, 1996) for the nets in Fig.3.a, b, c, d are given by relations (16), (17), (18), (19), respectively:

$$S_{paralel}(r) = S_1(r)\cdot S_2(r) \tag{16}$$

$$S_{choice}(r) = \sum_{i=1}^{r} S_1(i)\cdot S_2(r-i)\cdot S_3(r-i-1) \tag{17}$$

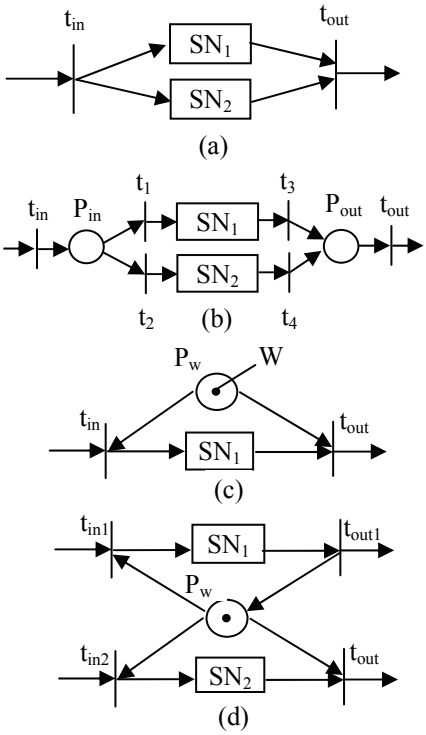


Fig. 3. Basic interconnections of Petri subnets

In relation (16) places P_{in} and P_{out} are considered as a group which forms the third subnet.

$$S_{blocking}(r) = \begin{cases} S_1(r), r \le w \\ 0 \quad , r > w \end{cases} \tag{18}$$

$$S_{share}(r) = \begin{cases} S_1(r_1) \cdot S_2(r_2), & r_1 + r_2 \le w \\ 0 \qquad\quad , & r_1 + r_2 > w \end{cases} \tag{19}$$

For example, in the figure 4 we have a system composed of three interconnections: the innermost is a choice between two subnets (each of the places); the middle interconnection is a resource block with queue; the outermost interconnection is a resource block. The SC-function for the inner choice is:

$$S_{in(r)} = \begin{cases} 1 \ , r = 0 \\ 4 \ , r = 1 \\ 10, r = 2 \end{cases} \tag{20}$$

The SC-function of the middle resource block is:

$$S_{mid(r)} = \begin{cases} 1 \ , r = 0 \\ 5 \ , r = 1 \\ 15 , r \geq 2 \end{cases} \tag{21}$$

The SC-function of the outer resource block is:

$$S_{out(r)} = \begin{cases} 1 \ , r = 0 \\ 5 \ , r = 1 \\ 15 , 2 \leq r \leq 4 \\ 0 \ , r > 4 \end{cases} \tag{22}$$

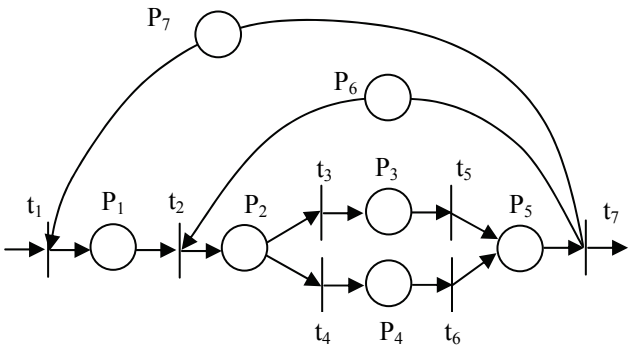


Fig. 4. Example of a multiple interconnection system

Following the above approach for calculating the size of the Petri net models of the modular controllers, we can adjust or modify the models accordingly to a reasonable size or in order to achieve the system requirements. We notice that state-space size estimation provides a tool for the model developer and the resulting data can be used to evaluate detail trade-off. As noted before, the longest directed circuits of the timed Petri net model determine the cycle time. Since for a high volume transfer line, the cycle time is determined by a directed circuit, we can use many of the known results to get more efficient algorithms for finding the critical operations of a timed modular logic controller (Murata, 1989). For example, because all transitions in the Petri net model of a modular controller are synchronized, we can assume that the sequence of transitions for the cyclic behavior is obtained by firing all transitions in the system only at once. Then the markings of the cyclic behavior of the system can be generated by the state equation (4) from the initial marking M_0.

6. The interaction Man-Machine in FCRS's

A characteristic of high level security control systems, such as those used in FCRS's is that an answer to a flaw that makes the man-machine system go to a lower level of security is considered a false answer, namely a dangerous failure, while an answer leading to a higher level of security for the man-machine system is considered an erroneous answer, namely a

non-dangerous failure. That is the reason for the inclusion of some component parts with maximum failure probability towards the erroneous answer and parts with minimum failure probability towards the false answer. One must notice that the imperfect functioning states of the components of the man-machine system imply the partially correct functioning state of the FCRS. In the following lines the notion of imperfection will be named imperfect coverage, and it will be defined as the probability "c" that the system executes the task successfully when derangements of the system components arise. The imperfect reparation of a component part implies that this part will never work at the same parameters as before the derangement (Ciufudean et al., 2008). In other words, for us, the hypothesis that a component part of the man-machine system is as good as new after the reparation will be excluded. We will show the impact of the imperfect coverage on the performances of the man-machine system in railway transport, namely we will demonstrate that the availability of the system is seriously diminished even if the imperfect coverage's are a small percent of the many possible faults of the system. This aspect is generally ignored or even unknown in current managerial practice. The availability of a system is the probability that the system is operational when it is solicited. It is calculated as the sum of all the probabilities of the operational states of the system. In order to calculate the availability of a system, one must establish the acceptable functioning levels of the system states. The availability is considered to be acceptable when the production capacity of the system is ensured. Taking into account the large size of a FCRS, the interactions between the elements of the system and between the system and the environment, one must simplify the graphic representation. For this purpose the system is divided into two subsystems: the equipment subsystem and the human subsystem. The equipment subsystem is divided into several cells. A Markov chain is built for each cell i, where i=1,2,…n, in order to establish the probability that at least k_i equipments are operational at the moment t, where k_i is the least equipment in good functioning state that can maintain the cell i in an operational state. Thus, the probability of good functioning will be established by the probability that the human subsystem works between k_i operational machines in the cell i and k_{i+1} operational machines in the cell (i+1) at the moment t, where i=1,2,…n; n representing the number of cells in the equipment subsystem (Thomson & Wittaker, 1996). Assuming that the levels of the subsystems are statistically independent, the availability of the whole system is:

$$A(t) = \left[\prod_{i=1}^{n} A_i(t) \right] \cdot A_h(t) \tag{23}$$

Where: A (t) = the availability of the FCRS (e.g. the man-machine system); A_i (t) = the availability of the cell i of the equipment subsystem at the moment t; A_h (t) = the availability of the human subsystem at the moment t; n = the number of cells i in the equipment subsystem.

6.1 The equipment subsystem

The requirement for a cell i of the equipment subsystem is that the cell including N_i equipment of the type M_i ensures the functioning of at least k_i of the equipment, so that the system is operational. In order to establish the availability of the system containing imperfect coverage and deficient reparations, a state of derangement caused either by the imperfect coverage or by a technical malfunction for each cell, has been introduced. In order

to explain the effect of the imperfect coverage on the system, we consider that the operation O_1 can be done by using one of the two equipments M_1 and M_2, as shown in the figure 5.

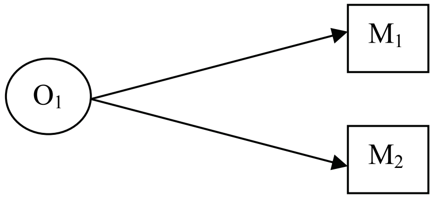


Fig. 5. A subsystem consisting of one operation and two equipments

If the coverage of the subsystem in the figure 1 is perfect, that is c =1, then the operation O_1 is fulfilled as long as at least one of the equipments is functional. If the coverage is imperfect, the operation O_1 falls with the probability 1-c if one of the equipments M_1 or M_2 goes out of order. In other words, if the operation O_1 was programmed on the equipment M_1 which is out of order, then the system in the figure 1 falls with the probability 1-c (Kask & Dechter, 1999). The Markov chain built for the cell i of the equipment subsystem is given in figure 6.

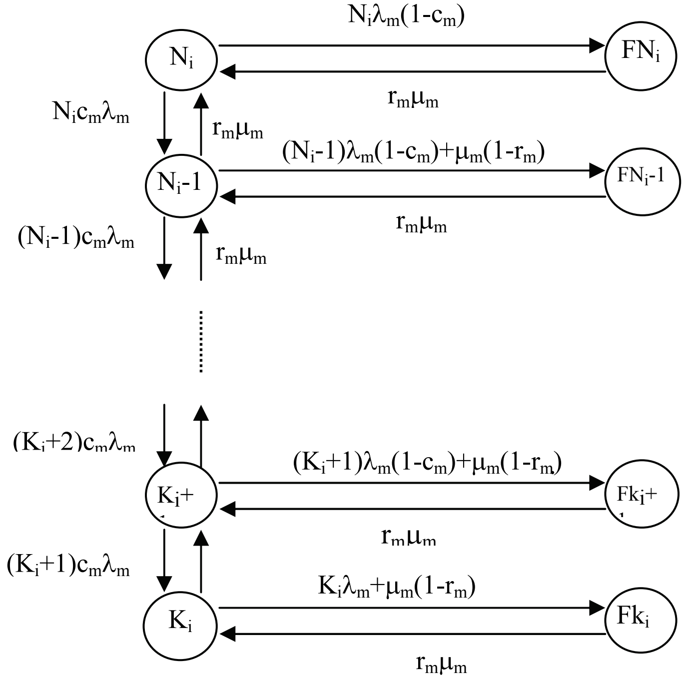


Fig. 6. The Markov model for the cell i of the equipment subsystem

The coverage factor is denoted as c_m, the failure rate of the equipment is λ_m (it is exponential), the reparation rate is μ_m (also exponential), and the successful reparation rate is r_m, where all the equipments in the cell are of the same type. In the state k_i the cell i has only k_i operational equipments. In the state N_i the cell works with all the N_i equipments. The

state of the cell i changes from the work state K_i, for $K_i \le k_i \le N_i$, to the derangement state Fk_i, either because of the imperfect coverage $(1-c_m)$ or because of a deficient reparation $(1-r_m)$. The solution of the Markov chain in the figure 6 is the probability that at least k_i equipments work in the cell i at the moment t.
The formula of this probability is:

$$A(t) = \sum_{k=k_i}^{N_i} P_{ki}(t) \tag{24}$$

Where, $A_i(t)$=the availability of the cell i at the moment t; $P_{ki}(t)$=the probability that k_i operational equipments are in the cell i at the moment t, i=1,2,…,n; N_i= the total number of the M_i type equipments in the cell i; K_i=the minimum number of operational equipments in the cell i.

6.2 The human subsystem

The requirement for the human subsystem is the exploitation of the equipment subsystem in terms of efficiency and security. In order to establish the availability of the operator for doing his work at the moment t, we build the following Markov chain, which models the behaviour of the subsystem (Ciufudean et al., 2006):

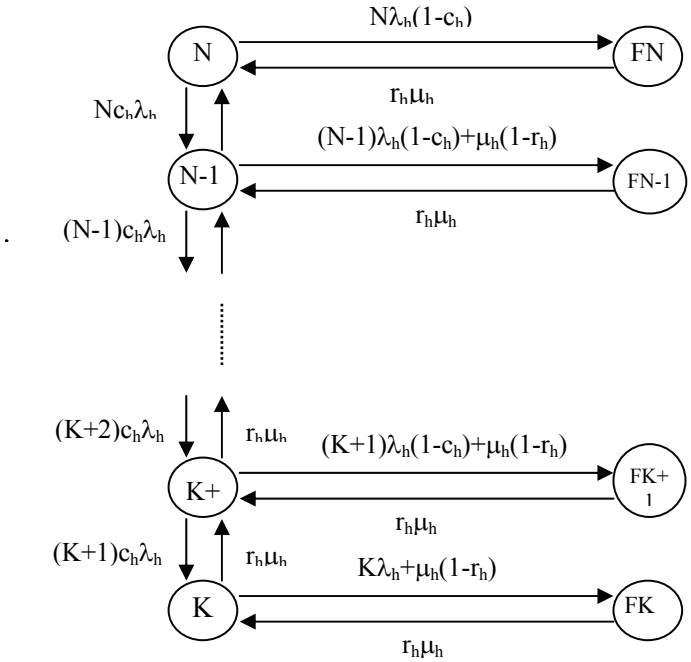


Fig. 7. The Markov chain corresponding to the human subsystem

Where, λ_h = the rate of making an incorrect decision by the operator; μ_h = the rate of making a correct decision in case of derangement; c_h = the rate of coverage for the problems caused

by incorrect decisions or by the occurrence of some unwanted events; r_h = the rate of successfully going back in case of an incorrect decision (Bucholz, 2002).
According to the figure 7, the human operator can be in one of the following states:
The state N = the normal state of work, in which all the N human factors in the system participate in the decisional process;
The state K = the work state in which k persons participate in the decisional process;
The state $F_{(k+u)}$ = the work state that comes after taking an incorrect decision or after an inappropriate repair that can lead to technological disorders with no severe impact on the traffic safety, where u=0,…N-k;
The state F_k =the state of work interdiction due to incorrect decisions with severe impact on the traffic safety.
In the figure 7, the transition between the states of the subsystem is made by the successive withdrawal of the decision right of the human factors who made the incorrect decisions.
The working availability of the human factor under normal circumstances is:

$$A_h(t) = \sum_{x=j}^{m} P_x(t) \tag{25}$$

Where, $P_x(t)$ = the probability that at the moment t the operator is in the working state X; m=the total number of working states allowed in the system; j = the minimal admitted number of working states.
Assigning new working states to the human factor increases the complexity of the calculus. Besides, although the man-machine system continues to work, some technological standards are exceeded, and that leads to a decrease in the reliability of the system.
The highlighting of new states of the human subsystem, that is the development of complex models with higher and higher precision, renders more difficult because of the increasing volume of calculus and the decreasing relevance of these models.
In order to lighten the application of complex models of Markov chains, a reduction of these models is required, until the best ratio precision/relevance is reached.
We notice that it is relatively easy to calculate the probabilities of good functioning for the machines (engines, electronic and mechanic equipments, building and transport control circuits, dispatcher installations etc.), while the reliability indicators of the decisional action of the human operator are difficult to estimate. The human operator is subjected to some detection psychological tests in which he must perceive and act according to the apparition of some random signals in the real system man-machine. However, these measurements for stereotype functions have a low accuracy level.
The man-machine interface plays a great part in the throughput increase of the FCRS's. The incorrect conception of the interface for presenting the information and the inadequate display of the commands may create malfunctions in the system.

7. An example of reliability analysis of construction robotized system

In order to illustrate the above-mentioned method, we shall consider a building site equipped with electronic and mechanic equipments consisting of three robot arms for load/unload operations and five conveyors. Two robots (e.g. robot arms) and three conveyors are necessary for the daily traffic of building materials and for the shunting

activity. That means that the electronic and mechanic equipment for two robots and three conveyors should be functional, so that the construction materials traffic is fluent.
The technician on duty has to make the technical revision for the five conveyors and for the three robots, so that at least three conveyors and two robot arms of the building site work permanently (Ciufudean et al., 2008).
On the other side, the construction engineer has to coordinate the traffic and the manoeuvres in such a manner as to keep free at least three conveyors and two robot arms, while the maintenance activities take place on the other two conveyors and one robot.
In this example the subsystem of the human factor consists of the decisional factors: the designer (i.e. architect), the construction engineer and the equipments technician (electro-mechanic). The subsystem of the equipments consists of the three robots and five conveyors (including the necessary devices). This subsystem is divided into two cells, depending on the necessary devices (e.g. electro-mechanisms and the electronic equipment for the conveyors, and respectively the electronic and mechanic equipment for the robots).
All the necessary equipments for the conveyors section are grouped together in the cell A_1, are denoted by $Ap_{1...5}$ and serve for the operation O_1 (the transport of building materials). The rest of the equipments denoted by $E_{1...3}$ are grouped together in the cell A_2 and serve for the operation O_2 (the load/unload operations of building materials by conveyors), according to the figure 8.

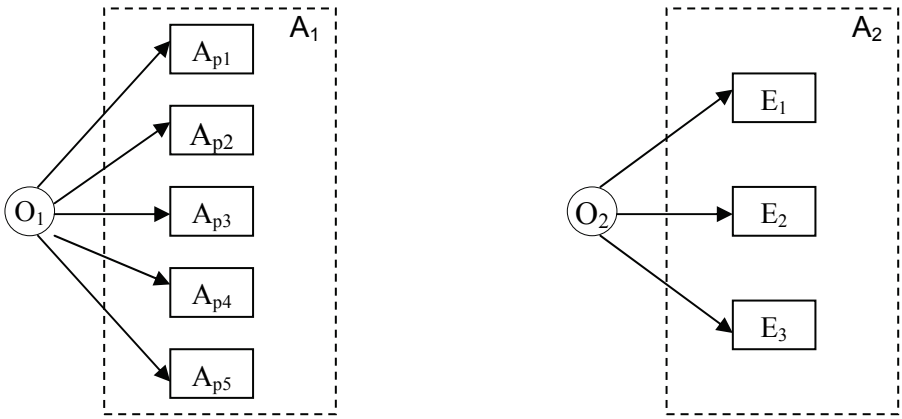


Fig. 8. The cells structure of the equipment subsystem

In the next table the rates of spoiling/repairing of the components are given.

The components of the system	C	μ	λ	r	K_i	N_i
A_{pi}	0.8	1.0	0.03	0.8	3	5
E_i	0.8	0.5	0.025	0.8	2	3
The components of the human subsystem	0.8	0.2	0.01	0.8	1	1,2,3

Table 1. The failing/repairing rates for the components of the system

	3	4	5	F_3	F_4	F_5
3	$-3\lambda+\mu$	$0{,}8\mu$	0	$3\lambda+0{,}2\mu$	0	0
4	$3{,}2\lambda$	$-(4\lambda+\mu)$	$0{,}8\mu$	0	$0{,}8\lambda+0{,}2\mu$	0
5	0	4λ	$-(5\lambda)$	0	0	λ
F_3	$0{,}8\mu$	0	0	$-(0{,}8\lambda)$	0	0
F_4	0	$0{,}8\mu$	0	0	$-(0{,}8\lambda)$	0
F_5	0	0	$0{,}8\mu$	0	0	$-(0{,}8\lambda)$

Fig. 9. The matrix of the state probabilities for the cell A_1 from the equipment subsystem

	2	3	F_2	F_3
2	$-(2\lambda+\mu)$	$0{,}8\mu$	$2\lambda+0{,}2\mu$	0
3	$2{,}4\lambda$	$-(3\lambda)$	0	$0{,}6\lambda$
F_2	$0{,}8\mu$	0	$-(0{,}8\mu)$	
F_3	0	$0{,}8\mu$	0	$-(0{,}8\mu)$

Fig. 10. The matrix of the state probabilities for the cell A_2 from the equipment subsystem

For the equipment subsystem there are two Markov chains, one with six states (cell A_1) and one with four states (cell A_2); the matrix in the figure 9 corresponds to the first one and the matrix in the figure 10 corresponds to the second one. The following Markov chains correspond to the human subsystem:

- with six states (the decisions are made by the three factors: the designer, the construction engineer and the electro-mechanic);
- with four states (the decisions are made only by two of the above-mentioned factors);
- with two states (the decisions are made by only one human factor).

A matrix of the state probabilities corresponds to each Markov chain:

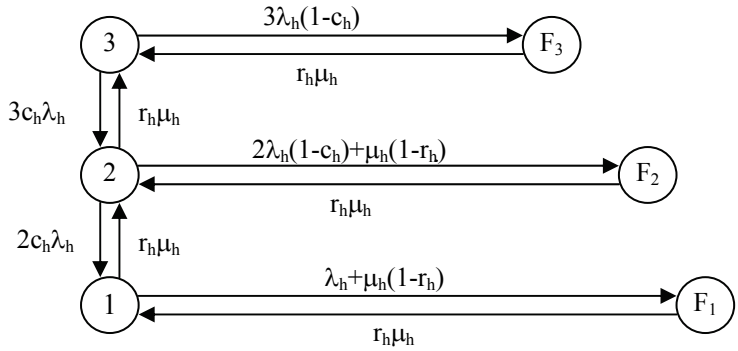


Fig. 11. The Markov chain corresponding to three of the decisional factors

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ F_1 \\ F \\ F_3 \end{array} \begin{bmatrix} 1 & 2 & 3 & F_1 & F_2 & F_3 \\ -(\lambda+\mu) & 0{,}8\mu & 0 & \lambda+2\mu & 0 & 0 \\ 1{,}6\lambda & -(2\lambda+\mu) & 0{,}8\mu & 0 & 0{,}4\lambda+0{,}2\mu & 0 \\ 0 & 2{,}4\lambda & -(3\lambda) & 0 & 0 & 0{,}6\lambda \\ 0{,}8\mu & 0 & 0 & -(0{,}8\mu) & 0 & 0 \\ 0 & 0{,}8\mu & 0 & 0 & -(0{,}8\mu) & 0 \\ 0 & 0 & 0{,}8 & 0 & 0 & -(0{,}8\mu) \end{bmatrix}$$

Fig. 12. The matrix of the state probabilities corresponding to the Markov chain in the Fig.11

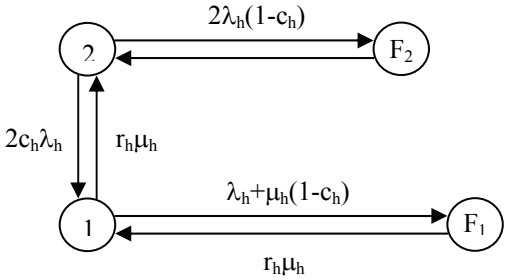


Fig. 13. The Markov chain corresponding to two decisional factors

$$\begin{array}{c} \\ 1 \\ 2 \\ F_1 \\ F_2 \end{array} \begin{bmatrix} 1 & 2 & F_1 & F_2 \\ -(\lambda+\mu) & 0{,}8\mu & \lambda+0{,}2\mu & 0 \\ 1{,}6\lambda & -(2\lambda) & 0 & 0{,}4\lambda \\ 0{,}8\mu & 0 & -(0{,}8\mu) & 0 \\ 0 & 0{,}8\mu & 0 & -(0{,}8\mu) \end{bmatrix}$$

Fig. 14. The matrix of the state probabilities corresponding to the Markov chain in the Fig.13

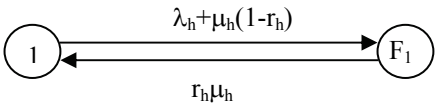


Fig. 15. The Markov chain corresponding to one decisional factor

$$\begin{array}{c} \\ 1 \\ F_1 \end{array} \begin{bmatrix} 1 & F_1 \\ -(\lambda+0{,}2\mu) & \lambda+0{,}2\mu \\ 0{,}8\mu & -(0{,}8\mu) \end{bmatrix}$$

Fig. 16. The matrix of the state probabilities corresponding to the Markov chain in the Fig.15

The equations given by the matrix of the state probabilities are functions of time and by solving them we obtain:

- The expressions of the availabilities for the cell A_1, and respectively A_2 from the equipment subsystem calculated with the relation (18);
- The expression of the availability of the human subsystem calculated with the relation (19);
- The expression of the availability of the whole system calculated with the relation (17).

The values of these availabilities depending on time are given in the table 2.

Time [hours]	Cell A_1	Cell A_2	The human subsystem A_h	The availability of the railway system A
0	1.000000	1.000000	1.0000000	1.00000000
1	0.980013	0.985010	0.9548293	0.92171802
4	0.947011	0.951341	0.8645392	0.77888946
8	0.933510	0.933468	0.8061449	0.70247605
12	0.933010	0.927481	0.7809707	0.67581225
16	0.933129	0.926133	0.7701171	0.66553631
20	0.933060	0.925951	0.7654364	0.66131243
24	0.932891	0.925600	0.7647893	0.65970171
28	0,932762	0,925012	0,7635876	0.65876005
32	0.932132	0.924910	0.7631243	0.65781145
36	0.931902	0.924830	0.7625786	0.65716133
40	0.931819	0.924690	0.7621289	0.65640272
44	0.931791	0.924600	0.7619786	0.65640272
48	0.931499	0.924582	0.7619456	0.65618425

Table 2. The availability values for the elements of the exemplified system

8. Conclusion

An advantage of the above-mentioned calculus method is the easy calculation of the availability of the whole system and of the elements of the system. The availabilities of the exemplified system are drawn in figure 17, depending on time and on the number of decision factors. In figure 17, the numbers x=1,2,3 show the availability of the systems corresponding to the Markov chains in figure 11, figure 13, respectively figure 15. The figure 17 shows that the best functioning of the system can be obtained by using two decisional factors: while the availability of the system in figure 15 is 65% after 12 hours of functioning, the availability of the system in figure 13 is 82%. The availability of the system decreases when the third decisional factor appears, because the diminution due to the risk of imperfect coverage or due to an incorrect decision is greater than the increase due to the excess of information.

In the figure 18 the availability of the system depending on the coverage factors (c_m), and on the successful repairing (r_m) of deficient equipment is illustrated. One may notice that the availability increases with 5 percents when the coverage is perfect (c_m=1). Moreover, when the repairing of a deficient equipment is perfect (r_m=1), the availability increases with 10 percents (we mention that the increases refer to a concrete case where c_m=0.8 and r_m=0.8). An important conclusion that we can draw is that the presumption of perfect coverage and repairing affects the accuracy of the final result. This presumption is made in the literature in the majority of the analysis models of the system availability (Hopkins, 2002).

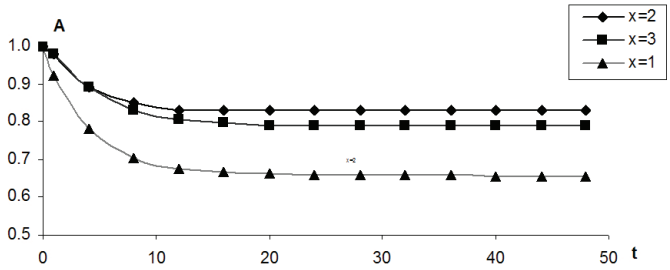


Fig. 17. The availability of the railway system depending on the number of the decisional factors

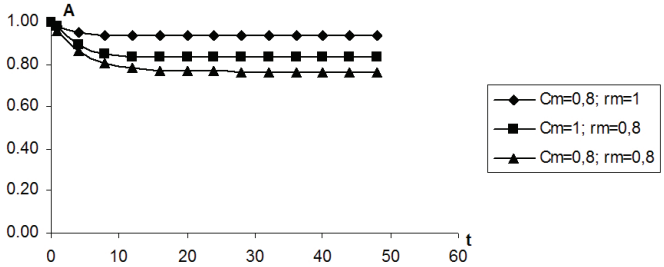


Fig. 18. The variation of the system availability depending on the factors c_m and r_m

The analysis of the availabilities of the operation O_1 and O_2 done by the cell A_1 and respectively by the cell A_2 from the equipment subsystem shows that an increase of the number of the conveyors (from N_i=5 and k_i=3 to N_i=5 and k_i=4) in the cell A_1 would lead to a decrease of the availability of the operator O_1 with 4% (as shown in the figure 19). In the case of the cell A_2, a decrease of the total number of robots (from N_i=3, k_i=2 to N_i=2, k_i=2) would lead to a decrease of the availability of the operator O_2 with 20% (as shown in the figure 20). The conclusion is that an extra robot is critical for the system, because it improves considerably the availability of O_2 and hence, the availability of the system.

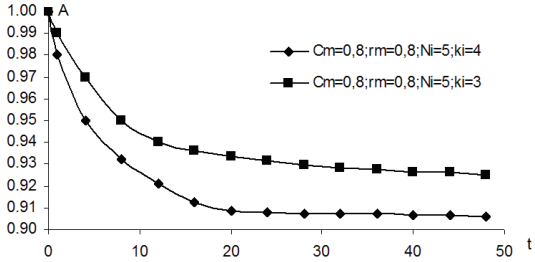


Fig. 19. The analysis of the availability of the cell A_1

The analysis of the availability allows us to establish the lapse of time when changes must be made in the structure of the system (major overhaul, the rotation of the personnel in shifts etc). For example, from the figure 17, if the availability is 70%, the human decisional factor must be replaced every 12 hours (for the system in the figure 15 that is rotating the personnel every 12 hours).

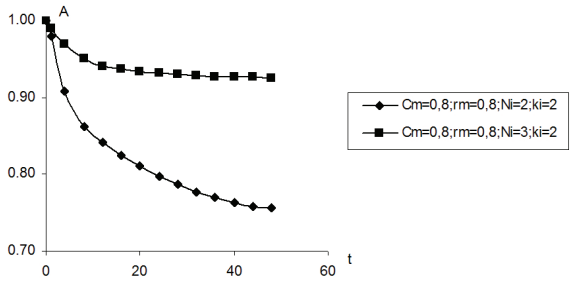


Fig. 20. The analysis of the availability of the cell A_2

9. References

Aven, T. (2004). Risk Analysis and Science, *International Journal of Reliability, Quality and Safety Engineering*, vol. 11, no. 1, pp. 1-15

Ferrarini, L. (1992). An incremental approach to logic controller design with Petri nets, *IEEE Trans. Syst. Man. Cybern*., vol. 22, pp. 461-473

Ferrarini, (1994). L. A new approach to modular liveness analysis conceived for large logic controllers design, *IEEE Trans. Robot. Automat*, vol. 10, pp.169-184

Zaitoon, J. (1996). Specification and design of logic controllers for automated manufacturing systems, *Robot. Comput-Integr. Man*., vol. 12, no. 4, pp. 353-366

Murata, T. (1989). Petri nets: Properties, analysis and applications, *Proc. IEEE*, pp. 541-580,

Zhon, M. C. & DiCesare, F. (1992). Design and implementation of a Petri net based supervisor for a flexible manufacturing system, *IFAC J. Automatica*, vol. 28, no. 6, pp. 1199-1208

Park, E.; Tilburg D.; Khargonekar, P. (1999). Modular logic controllers for machining systems: formal representation and performance analysis using Petri nets, *IEEE Trans. Rob. and Autom*., vol. 15, no. 6, pp. 1046-1060

Watson J. & Desrochers, A. (1994). State space size estimation of Petri nets: a bottom-up perspective, *IEEE Trans. Rob. and Autom*., vol. 10, no. 4, pp. 555-561

Zhou M. & Twiss, E. (1998). Design of industrial automated systems via relay ladder logic programming and Petri nets, *IEEE Trans. Man. Cyber,*vol.28,pp.137-150

a. Hopkins, M. (2002). Strategies for determining causes of events, *Technical Report R-306*, UCLA Cognitive Systems Laboratory

b. Hopkins, M. (2002). A proof of the conjuctive cause conjecture in causes and explanations, *Technical Report R-306*, UCLA Cognitive Systems Laboratory

Thomson, M. G. & Wittaker, J. A. (1996). Rare Failure State in a Markov Chain Model for Software Reliability, *IEEE Trans. Reliab. 48(2),* pp. 107-115

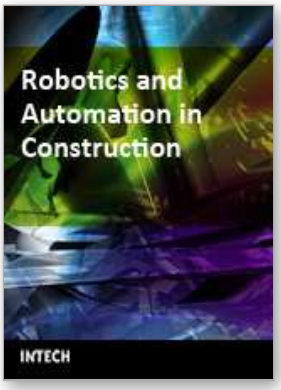
Kask, K. & Dechter, R. (1999). Stochastic local search for Bayesian networks, *In Workshop on AI and Statistics 99*, pp. 113-122

Russell, S. & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach*, J. Willey and Sons, N.Y.

Bucholz, P. (2002). Complexity of memory-efficient Kroneker operations with applications to the solutions of the Markov models, *Informs J. Comp.,* no. 12(3), pp. 203-222

Ciufudean, C. & Graur, A. & Filote, C. (2006). Determining the Performances of Cellular Manufacturing Systems, In *Scientific and Technical Aerospace Reports*, vol.14, Issue 6, NASA, Langley Research Center, USA

Ciufudean, C. & Filote, C. & Amarandei, D. (2008). Scheduling Availability of Discrete Event Systems, *The 14th IEEE Mediterranean Electrotechnical Conference, MELECON'2008*, Palais des Congrès François Lanzi - Ajaccio – France.



Robotics and Automation in Construction

Edited by Carlos Balaguer and Mohamed Abderrahim

ISBN 978-953-7619-13-8
Hard cover, 404 pages
Publisher InTech
Published online 01, October, 2008
Published in print edition October, 2008

This book addresses several issues related to the introduction of automaton and robotics in the construction industry in a collection of 23 chapters. The chapters are grouped in 3 main sections according to the theme or the type of technology they treat. Section I is dedicated to describe and analyse the main research challenges of Robotics and Automation in Construction (RAC). The second section consists of 12 chapters and is dedicated to the technologies and new developments employed to automate processes in the construction industry. Among these we have examples of ICT technologies used for purposes such as construction visualisation systems, added value management systems, construction materials and elements tracking using multiple IDs devices. This section also deals with Sensorial Systems and software used in the construction to improve the performances of machines such as cranes, and in improving Human-Machine Interfaces (MMI). Authors adopted Mixed and Augmented Reality in the MMI to ease the construction operations. Section III is dedicated to describe case studies of RAC and comprises 8 chapters. Among the eight chapters the section presents a robotic excavator and a semi-automated façade cleaning system. The section also presents work dedicated to enhancing the force of the workers in construction through the use of Robotic-powered exoskeletons and body joint-adapted assistive units, which allow the handling of greater loads.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Calin Ciufudean (2008). Risk and Reliability Analysis of Flexible Construction Robotized Systems, Robotics and Automation in Construction, Carlos Balaguer and Mohamed Abderrahim (Ed.), ISBN: 978-953-7619-13-8, InTech, Available from: http://www.intechopen.com/books/robotics_and_automation_in_construction/risk_and_reliability_analysis_of_flexible_construction_robotized_systems

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821