

# Analysis of sequential failures for assessment of reliability and safety of manufacturing systems

Angela Adamyán, David He\*

*Intelligent System Modeling and Analysis Laboratory, Department of Mechanical and Industrial Engineering,  
The University of Illinois at Chicago, 842 West Taylor Street, 3049 ERF, Chicago, IL 60607, USA*

Received 30 June 2001; accepted 15 January 2002

## Abstract

Assessment of reliability and safety of a manufacturing system with sequential failures is an important issue in industry, since the reliability and safety of the system depend not only on all failed states of system components, but also on the sequence of occurrences of those failures. Methods that are currently available in sequential failure analysis always start with given sequences of the failures in the system, which is not the case in real life situations; therefore, the sequences of the failures should be identified and the probability of their occurrence should be determined. In this paper, we represent a methodology that can be used for identifying the failure sequences and assessing the probability of their occurrence in a manufacturing system. The method employs Petri net modeling and reachability trees constructed based on the Petri nets. The methodology is demonstrated on an example of an automated machining and assembly system. © 2002 Elsevier Science Ltd. All rights reserved.

*Keywords:* Reliability; Manufacturing systems safety; Sequential failures; Petri nets

## 1. Introduction

Rapid technology evolution and increasing complexity of manufacturing systems attract the attention towards multiple failure analysis of the systems. The reliability and safety analysis and assessment of complex systems is becoming more and more difficult task due to the fact that the reliability and safety of manufacturing systems depend not only on all failed states of system components, but also on the sequence of occurrences of those failures. Assessment of the reliability and safety of manufacturing systems that takes sequential failures into consideration is a more realistic view on system failure analysis.

In the past, researchers referred to the system failures caused by the occurrence of sequential failures of the components as sequential failure logic (SFL). Fussel et al. [1] performed one of the pioneer works in this area. In Ref. [1] the authors analyzed a non-repairable electric supply system with main and standby power units and switch controls. The authors provided both an exact and an approximate method for calculating the probability of occurrence of the output event from priority-AND SFL. The assumptions made in their paper were that basic events (inputs to

the priority-AND failure logic) were stochastically independent, exponentially distributed, and non-repairable.

The necessity of SFL for the quantitative analysis of the dynamic systems like space satellites is emphasized in Ref. [2]. SFL has been applied to the risk analysis of a human–robot system [3], to the field of product liability prevention [4], and some other applications.

A domino model has been used for investigating failure process that could occur in the units of an insulator string [5]. Domino failure model assesses cascade process where a failure triggers consecutive failures at later times. The author extended the standard independent failure reliability assessment to the case of the sequential failures, where failure of one unit increases the probability of failure of the neighbor units. To express this domino effect in a mathematical form, the author made an assumption that the failure of one unit increases the failure rate of its two immediate neighbors by a given factor.

A solution for determining the mean time to system failure of a consecutive  $k$ -out-of- $n$  system with single repair, where the components of the system were subject to sequential failures can be obtained from Ref. [6]. The authors evaluated the mean time to system failures by using the relationship between reliability function of the system and the probability of the first passage time to system failure.

Although useful, the applications of current research on

\* Corresponding author. Tel.: +1-312-996-3410; fax: +1-312-413-0447.  
E-mail address: davidhe@uic.edu (D. He).

SFL are rather limited, because the sequences of the failures are assumed given for estimating the system failures. Therefore, it is obvious that there is a need for more work in this field.

In this paper, we present an approach that overcomes the limitations of the SFL. The method can be used as a comprehensive reliability and safety assessment tool for managers to analyze hazardous operations for improving safety of the workers and the overall safety of the manufacturing systems. The novel feature of our approach is in utilizing Petri net techniques for modeling the system dynamics, identifying possible failure sequences, and assessing the reliability and safety of manufacturing system with sequential failures. The Petri net modeling provides the ability of assessing the quality and reliability impacts caused by the combination of unplanned failures and the sequence of these failures. The Petri net graphical representation is used to construct the cause and effect relationship among the events. The Petri net allows performing comprehensive failure and reliability analysis of the system.

The remainder of the paper is organized as follows. In Section 2, we provide the definition of SFL and present quantification methods and the general idea of Petri net modeling. In Section 3, we provide the framework for identification of sequences of the failures. Section 4 presents the mathematical formulation of the method. Section 5 demonstrates the proposed methodology with an example of an automated machining and assembly system. Section 6 concludes the paper.

**2. Background**

Until now, the research on SFL has been mainly based on fault tree analysis (FTA). A fault tree (FT) arises from the logic diagram that is used to analyze the probabilities associated with the various causes and their effects. FTA starts by identifying a problem (catastrophic accident or other undesirable result) and all possible ways that the problem (or failure) occurs. FTs have been widely used for obtaining reliability information about complex systems since 1960. The importance of FTA was pointed out in the safety study

of the US Nuclear Regulatory Commission [7]. In addition, FTs are powerful design tools that can help to meet product performance objectives.

It is well known that FT is equivalent to the minimal cut set tree with all minimal cut-AND structures. A minimal cut set is a set of components in which the repair of any failed component will result in functioning of the failed system. Long et al. [8] defined a minimal cut structure as an AND conjunction of an output and all inputs that compose the minimal cut set. For the minimal cut-AND structure, the failed states of the output become true when all states of the inputs exist simultaneously. Therefore, it is very important to estimate the output of the minimal cut-AND structure in order to quantify the top event of the FT.

Even though it is believed that the top event of a FT arises when all basic elements of the minimal cut set that is derived from the tree exist simultaneously, there are many cases where the occurrence of the top event depends not only on the simultaneous existence of all basic elements, but also on the sequences of their occurrence [9]. Sequential occurrence of the failures very often happens in micro-electronic systems [3,10]. Therefore, the main objective in SFL research is to compute the probability of sequential occurrence of failures. In the context of SFL, a basic failure cause is defined as an input of the system failure (the output) caused by the sequential occurrence of the basic failures.

Fig. 1 shows the relationships among failures of the inputs  $x_1, x_2, \dots, x_n$  and the output for the SFL. The failure  $x_1$  occurs at  $\tau_1$  and the failed state lasts over  $\tau_n$ ; the failure  $x_2$  occurs at  $\tau_2$  and the failed state lasts over  $\tau_n$ ; finally, the failure of  $x_n$  occurs at  $\tau_n$ . Here, all failed states of inputs become true. The failure of output is generated, given that the occurrences of input failures meet the sequential requirement. The failed state of output is kept until any one of the failed states of inputs disappears.

Sequential logic is easy to express using priority AND gate of a FT. Fig. 2 is a FT representation of the SFL. Failures in this case occur in the following sequence:  $x_1, x_2, \dots, x_n$ . In other words, the failed state of the output happens if and only if the failures of inputs occur in the sequence of  $x_1, x_2, \dots, x_n$ .

Two methodologies have been applied for the

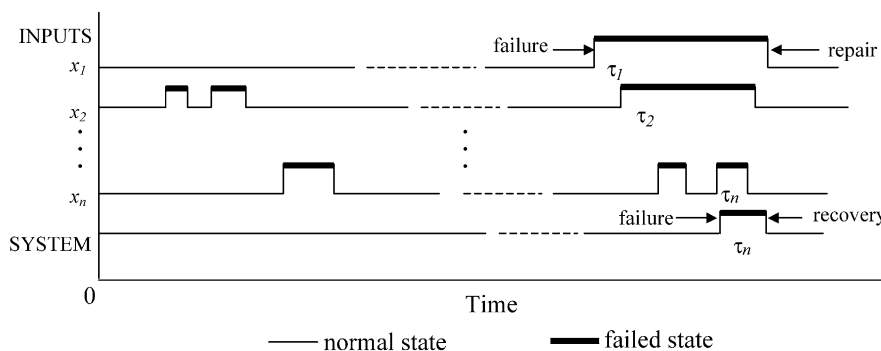


Fig. 1. Relationship among the inputs and the output in SFL.

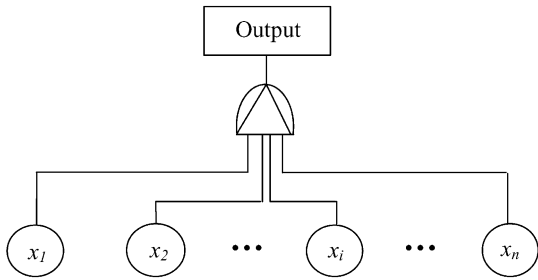


Fig. 2. Graphic representation of SFL using a priority AND gate.

quantification of the SFL, or the priority AND gate. One is the application of the Markov model [11,12], and the other is the application of priority AND gate quantification (PAQ) [1]. The Markov model is applicable for special cases only and gives no analytical solution for an arbitrary number of inputs. The PAQ model is an approximate approach by its nature; however, it allows an analytical solution regardless of the number of inputs. Long and Sato [9] and Long et al. [13] performed a comparison between two methodologies. They concluded that the quantification of the priority AND gate method has an advantage over Markov methodology when  $\lambda/\mu \ll 1$ , where  $\lambda$  and  $\mu$  are failure and repair rates consequently. The authors also came to the conclusion that the PAQ model gives much more simpler and easier algorithm than the Markov model for different failure and repair rates.

As discussed earlier, the assessment of the reliability of the systems with sequential failure is very important issue in industry. However, methods that are currently available in sequential failure analysis always start with given sequences of the failures in the system, which is not the case in real life situations; therefore, the sequences of the failures should be identified and the probability of their occurrence should be determined. Developing new methodology that can be used to identify the failure sequences is essential. For identification of the sequences of the failures and assessment of the probability of their occurrence, current research uses Petri net modeling and reachability trees constructed based on Petri nets.

Petri nets are widely used as a tool for analyzing system safety and reliability of the complex systems. They can be used as visual communication aid similar to flow charts, block diagrams, FTs, and networks. The use of Petri nets augments the ability of understanding the interaction between various effects. First developed by Adam Petri in the early 1960s, Petri nets have become a powerful and generic tool for modeling and simulation [14–18]. The Petri nets where random delays are exponentially distributed are referred to as stochastic timed Petri nets (SPNs) [19–22]. General-purpose software packages are available for solving SPN models, including GreatSPN [23] and SPNP [24].

Incorporating Petri net modeling into system reliability and safety analysis provides an ability to assess the quality

and reliability impacts caused by combination of unplanned failures and their sequences. Petri net allows to analyze combined failure modes and to predict their potential severity, as well as to estimate the probability of occurrence of failure modes. With this knowledge, engineers can put into place effective means to prevent the impacts of the failures. The Petri net graphical representation can be used to construct the cause and effect relationship among the events. Petri nets can be used to replace logic gate functions in an FT for failure analysis [18]. Transition of the FT to the Petri net representation allows performing thorough failure and reliability analysis of the system, as well as provides an efficient way for obtaining path sets and minimal cut sets.

Petri net modeling is superior over traditional Markov chain modeling in that the number of places and transitions increases slightly as the system complexity increases, whereas the number of states in the Markov chain increases exponentially [25]. In addition, Petri net modeling provides a general and formal procedure to generate all possible states for analysis.

Formally Petri net is a directed bipartite graph defined by a 6-tuple  $N = [T, P, A, M_0, I(t), O(t)]$ , where  $T = \{t_1, t_2, \dots, t_n\}$  is a set of transitions, each transition representing an event or an action; and  $P = \{p_1, p_2, \dots, p_l\}$  is a set of places, where a place is used to represent either the condition for the event or the consequences of the event. Therefore, before building a Petri net model, the events and their conditions and consequences in a system are first defined, and then are represented by transitions and places in a Petri net. Each place can contain one or more tokens. Movement of tokens through the places in the constructed model simulates the operations of the system and allows identifying and analyzing what can go wrong within the system. A place with (or without) a token indicates that the state represented by the place is true (or false).  $A \subseteq \{T \times P\} \cup \{P \times T\}$  is a set of directed arcs that connect transitions to places and places to transitions.  $M_0$  is the initial marking of the system that represents initial state of the system. A marking  $M$ , can also be represented as a vector  $M = \{m_1, m_2, \dots, m_l\}$ , where  $m_i$  is the number of tokens in place  $p_i$ . Fig. 3 shows the Petri net with initial state  $M_0 = \{2, 1, 0\}$ , indicated by the number of tokens (black dots) in corresponding places.

Places that represent the conditions of a transition are connected to that transition as input places, and places that represent the consequences of the events are connected

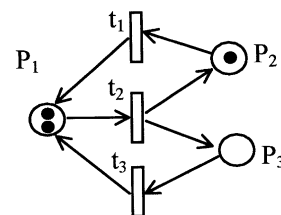


Fig. 3. Petri net with three places and three transitions ( $n = 3, l = 3$ ).

to the transitions as output places. Respectively,  $I(t) = \{p | (p, t) \in A\}$  is the set of input places of a transition  $t$ ; and  $O(t) = \{p | (t, p) \in A\}$  is the set of output places of a transition  $t$ . Directed arcs connect transitions to places and vice versa. A directed arc from place to transition is called an input arc, and an arc from transition to place is called an output arc.

In a Petri net, an action is represented by the ‘firing’ of a transition. The behavior of the Petri net is determined by following firing rules:

1. Tokens in places with arcs towards a transition indicate that conditions are satisfied and the transition is ready to fire (event to occur).
2. Upon firing, transition  $t$  consumes one token along each input arc.
3. Upon firing, transition  $t$  produces one token along each output arc.

Whenever a transition is fired, tokens are taken away from the input places and appear in the output places of the transition. An arc with double arrows indicates that a place serves as both an input place and an output place. A dashed arc with small circle instead of an arrowhead is an inhibitor arc. The inhibitor arc disables the transition when the input place has a token, and enables the transition when the input place has no token and other (normal) input place(s) have a token per arc.

If the firing of the transition results in a new marking  $M'$  from marking  $M$ , then  $M'$  is *immediately reachable* from  $M$ . The marking  $M''$  is *reachable* from marking  $M$  if it is reachable from any marking that is immediately reachable from  $M$ . The reachability tree is the graphical representation of all markings of a net starting from its initial marking. In other words, the reachability tree is the state diagram in which each node represents the unique marking, i.e. state of the system, and edges represent the possible state transitions.

**3. Failures sequences identification framework**

The framework of the methodology for failure sequences identification is shown in Fig. 4. This methodology incorporates dynamic Petri net modeling for identifying all possible failures sequences in order to assess the system reliability.

The methodology starts with identifying potential failures

that could cause functional failure of a process or a product. By definition, a functional failure means unsatisfactory performance (e.g. an item delivering unsatisfactory outputs), occurring during a process such as operation or testing [26]. FTA can be used for identifying those failures.

The sequences of the failures have to be identified for analyzing and quantifying their impacts. Identification of the sequences starts from construction of a Petri net model of the system under normal operating conditions. We assume that failures are stochastically and mutually independent of constant failure and repair rates. In this case, stochastic Petri nets can be used to model the system. When using Petri net concepts, failures should be integrated into the Petri net model for the system in the following way: a failure should be assigned to a transition; failure causes should be assigned to input places of the transition; and failure effects should be assigned to output places of the transition.

Based on the Petri net, the reachability tree can be constructed by firing all possible transitions enabled in all possible reachable markings starting from the initial marking. This procedure continues until all states of the system are represented, so that the entire system representation includes both normal operation flow of the system and all possible failures. Based on the markings representation, the sequence of the failures can be obtained by following the reachability tree starting from the initial marking towards the marking that represents the system failure state. By following the paths that lead to system failure markings, the sequences of the failures are identified. An approximation method for computing the probabilities of the identified failure sequences is presented in Section 4.

**4. Method development**

Define:

- $T = \{t_1, t_2, \dots, t_n\}$  a set of transitions, each transition represents an event or action and can be fired with firing rate  $\lambda_i$  corresponding to transition  $t_i$ ,  $i = 1, 2, \dots, n$
- $M = \{M_1, M_2, \dots, M_l\}$  a set of markings in a reachability tree
- $F_i(\tau)$  probability distribution function of the time interval  $\tau$  between the time at which the transition  $t_i$ ,  $i = 1, 2, \dots, n$  will be able to fire and the time at which the firing of transition  $t_i$  is completed

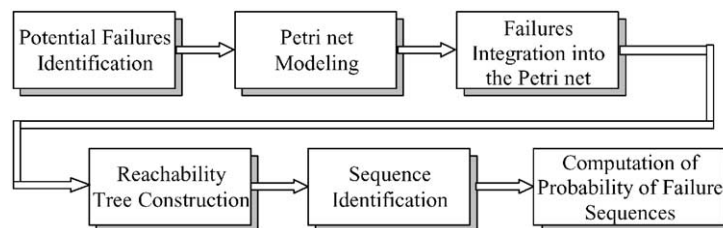


Fig. 4. Failure sequence identification framework.

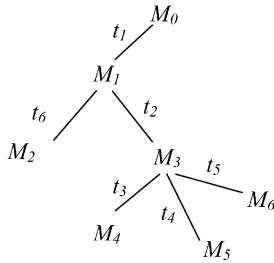


Fig. 5. An example of reachability tree.

$Q_{M_i, M_j}(\tau)$  transitional probability, i.e. the probability that marking  $M_i$  changes to  $M_j$  because of firing transition  $t_j$  in an amount of time less than or equal to  $\tau$

$f_{ij}$  probability that starting in marking  $i$  the process will be in marking  $j$  after  $m$  additional transitions in a given sequence

$E = \{\overrightarrow{M_i M_k}, \dots, \overrightarrow{M_h M_j}\}$   $i \neq k \neq h \neq j$  a sequence of events, where  $\overrightarrow{M_i M_j}$  indicates that marking  $M_i$  change to marking  $M_j$ .  $|E| = n$ ,  $n$  is the number of transitions

As mentioned earlier, the reachability tree describes the dynamic behavior of the system, shows all possible markings and possible fairings at each marking. Therefore based on the markings the possible sequences of failures and the probability of occurrence of a particular sequence of the failures can be computed. An example of reachability tree is shown in Fig. 5.

Since the firing times of the transitions are exponentially distributed one can write the probability distribution function as:

$$F_i(\tau) = \int_0^\tau \lambda_i e^{-\lambda_i x} dx$$

In a reachability tree, we can consider three possible branching cases:

**Case 1.** There are no branches. Since the amount of time for firing the transition  $t_i$ , is less or equal to  $\tau$ , the transitional probability that marking  $M_i$  changes to  $M_j$  in general case can be written as following [27]:

$$Q_{M_i, M_j}(\tau) = F_i(\tau) = \int_0^\tau \lambda_i e^{-\lambda_i x} dx$$

In Fig. 1, for example, marking  $M_0$  can be changed only to marking  $M_1$  by firing transition  $t_1$ .

$$Q_{M_0, M_1}(\tau) = F_1(\tau) = \int_0^\tau \lambda_1 e^{-\lambda_1 x} dx$$

**Case 2.** There is only one branch. In the case, when there is an uncertainty, as which transition should be fired we have to exercise a different approach for computing the probability of firing a certain transition. Therefore we

have to estimate the probability that the transition  $t_l$  is fired given that alternative transition  $t_k$  is not fired up to time  $\tau$ . The probability that transition  $t_k$  is not fired up to time  $\tau$  is given by  $\bar{F}_k = 1 - F_k$ . Then we can write the following [27]:

$$Q_{M_i, M_j}(\tau) = \int_0^\tau \bar{F}_k dF_l(\tau) = \int_0^\tau \lambda_l e^{-(\lambda_l + \lambda_k)x} dx$$

For the example shown in Fig. 1, we have an alternative of whether to fire transition  $t_2$  or transition  $t_6$ . The probability that marking  $M_1$  will change to  $M_3$  is:

$$Q_{M_1, M_3}(\tau) = \int_0^\tau \bar{F}_6 dF_2(\tau) = \int_0^\tau \lambda_2 e^{-(\lambda_2 + \lambda_6)x} dx$$

**Case 3.** There is more than one branch. This is a general case where the number of branches is greater than one. Therefore, we have more than one transition to fire. In this case we should estimate the probability that the transition  $t_l$  will be fired given that alternative transition  $t_1, t_k, \dots, t_n$  are not fired up to time  $\tau$ . Then the transitional probability  $Q_{M_i, M_j}(\tau)$  that marking  $M_i$  changes to  $M_j$  is:

$$Q_{M_i, M_j}(\tau) = \int_0^\tau \lambda_l e^{-(\lambda_l + \lambda_k + \dots + \lambda_n)x} dx$$

Based on those three considered cases we can obtain the transitional probabilities of the all-possible changes of markings. The summary is presented below:

$$Q_{M_i, M_j}(\tau) = \begin{cases} F_i(x) = \int_0^\tau \lambda_i e^{-\lambda_i x} dx, & \text{Case 1} \\ \int_0^\tau \bar{F}_k(x) dF_i(x) = \int_0^\tau \lambda_i e^{-(\lambda_i + \lambda_k)x} dx, & \text{Case 2} \\ \int_0^\tau \lambda_l e^{-(\lambda_l + \lambda_k + \dots + \lambda_n)x} dx, & \text{Case 3} \\ 0 & \text{where } M_i = M_j \end{cases}$$

In order to compute the probability of occurrence of sequential failures let us introduce a stochastic process. A *stochastic process* (or random process) is a family of random variables  $\{X(t) : t \in A\}$ , defined over a given probability space, indexed by the parameter  $t$ , where  $t$  varies over the index set  $A$ . The values of random variables are called states. The set of possible states defines the state space  $S = \{s_1, s_2, \dots, s_n\}$ ; although in general it can be continued [28].

Based on the definition of the stochastic process the probability  $f_{ij}$  for all  $i, j \in E$  formally is:

$$f_{ij} = P\{X_n = j, X_{n-1} \neq i, X_{n-2}, \dots, X_1 \neq j | X_0 = i\}$$

Consider a process that is observed at discrete time points to be in any one of possible markings  $M$ , which we numbered  $M_1, M_2, \dots, M_n$ . After observing the state of the process, a

transition to be fired must be chosen, and we let  $T$ , assumed finite, denote the set of all possible transitions.

If process in the marking  $M_l$  at time  $n$  and transition  $t$  is chosen then the next marking of the system is determined according to the transition probabilities  $Q_{M_l, M_j}(t)$ .

If we let  $M_n$  denote the marking of the process at the time  $n$ , then the above is equivalent to stating that:

$$P\{M_{n+1} = j | M_0, t_0, M_1, t_1, \dots, M_n = i, t_n = t\} = Q_{M_i, M_j}(t)$$

Thus, the transition probabilities are functions of only the present marking and the subsequent transition that can be fired.

**Theorem.** Given the sequence of events  $E$  the probability  $f_{ij}$  can be computed as:

$$f_{ij} = \prod_{i \in E} Q_{M_i, M_j}, \text{ where } i, j, \in E$$

**Proof.** Define:  $X = \{x_1, x_2, \dots, x_n\}$  is state vector indicating the sequence of transitions.

$$x_i = \begin{cases} 0, & \text{if transition } i \text{ has failed to fire} \\ 1, & \text{if transition } i \text{ is fired} \end{cases}$$

Let us introduce the structural function  $\phi(X)$

$$\phi(X) = \begin{cases} 0, & \text{if the sequence of transitions is not fired when the state vector is } X \\ 1, & \text{if the sequence of transitions is fired when the state vector is } X \end{cases}$$

A sequence of transitions is fired if all transitions in the sequence are fired, thus  $\phi(X)$  assumes the value 1 when  $x_1 = x_2 = \dots = x_n = 1$  and 0 otherwise therefore:

$$\begin{aligned} \phi(X) &= \begin{cases} 0, & \text{if there exists an } i \text{ such that } x_i = 0 \\ 1, & \text{if } x_i = 1 \text{ for all } i = 1, \dots, n \end{cases} \\ &= \min\{x_1, x_2, \dots, x_n\} = \prod_{i=1}^n x_i \end{aligned}$$

Due to the memory less property of the exponential distribution the transitions that fired are independent of each other. Thus the probability  $f_{ij}$  that transitions are fired in the given sequence can be computed as

$$f_{ij} = P[\phi(X) = 1] = P\left[\prod_{i=1}^n x_i = 1\right] = \prod_{i=1}^n P[x_i = 1] = \prod_{i=1}^n p_i$$

where  $p_i$  is the probability that transition  $t_i$  is fired:  $p_i = Q_{M_i, M_j}$ . □

Then the probability that the process will ever make a state transition to state  $j$ , given it starts from state  $i$ , can

be determined by:

$$F_{ij} = \sum_{n=1}^h J_{ij}^n$$

where  $h$  is the number of possible state transitions from state  $i$  to state  $j$ .

Due to the stochastic nature of the process it is not possible to compute the exact duration of the stay in the state  $j$  ( $\tau_j$ ) that is the time between the time at which the transition  $t_i$ ,  $i = 1, 2, \dots, n$  will be able to fire and the time at which the transition  $t_i$  is completed. Therefore, given the sequence of failures some approximation is required to compute the probability that the system will reach the failed state after certain time.

The procedure for finding approximated duration of the stay in the state  $j$  is summarized in the following two steps:

*Step 1.* Normalize all firing rates of the transitions in the given sequence by summing them together, then dividing each by the sum. The result will be weight ( $\omega_j$ ) for computing  $\tau_j$  for each transition.

*Step 2.* Compute  $\tau_j : \tau_j = \omega_j \times T$ , where  $T$  is the total time.

Section 5 presents an example of an automated machining and assembly system.

### 5. Example of an automated machining and assembly system

Development of flexible manufacturing systems requires diverse new skills and sets new challenges for operators. It also increases the possibility of errors due to the organization of the processes and the human factor. That is why we use an automated machining and assembly system to demonstrate the method. The system makes one product type and needs one machining operation and one assembly operation. Fig. 6 shows the system that has one assembly station (A), one robot (R), and one machine (M).

The following steps describe the production procedure:

1. M starts to operate.
2. After M finishes its operations R takes and transfers the part from M to A.
3. R begins the assembly.

At the first step of modeling, an abstract Petri net of the

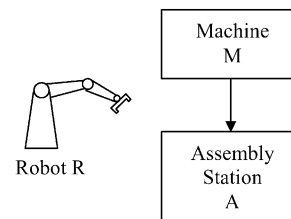


Fig. 6. A simple automated machining and assembly system.

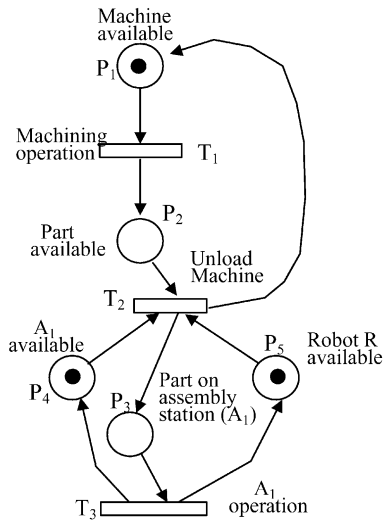


Fig. 7. Petri net model of the machining and assembly system.

system is constructed and shown in Fig. 7, which states that the production procedure needs a machining operation followed by unloading the part, and an assembly operation. Robot transfers parts from machine to the assembly and starts assembling the product.

The automated operation of the robot continues even when the robot drops the part. The part must be recovered by the operator, therefore the operator has to enter into hazardous zone where she/he can be struck by the robot. Robot applications with absolute safety cannot be achieved; therefore, accidents of this type can happen. At the second step of modeling, an abstract Petri net model of the system is

Table 1  
Firing rates of the transitions

Firing rate	$\lambda_1$	$\lambda_2$	$\lambda_3$	$\lambda_4$	$\lambda_5$	$\lambda_6$	$\lambda_7$
	1	0.5	0.5	0.1	0.0005	0.0003	0.5

specified as shown in Fig. 8, which states that the operator is entering the hazardous zone once the part is dropped. The failures of interlock or power source lead to the accident where operator is struck by the robot. The firing rates of the transition are listed in Table 1.

The accident of this type can be caused by the different sequences of failures. To identify the sequences and to compute the probability of their occurrences, the reachability tree of the Petri net model shown in Fig. 8 has to be constructed (third step). Reachability tree is the state diagraph in which each node represents the unique marking, i.e. state of the system, and edges represent the possible state transitions. Therefore, one should start from identifying all possible markings of the system for constructing the reachability tree.

At any given time, the distribution of tokens in places defines the current state of the modeled system, which is represented by corresponding markings. As mentioned earlier, in the Petri net the marking with  $n$  places is represented by  $(n \times 1)$  vector, elements of which are non-negative integers representing the number of tokens in the corresponding places. For the machining and assembly system example, the marking presenting the initial state of the Petri net is  $M_0 = \{1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0\}$ . Starting

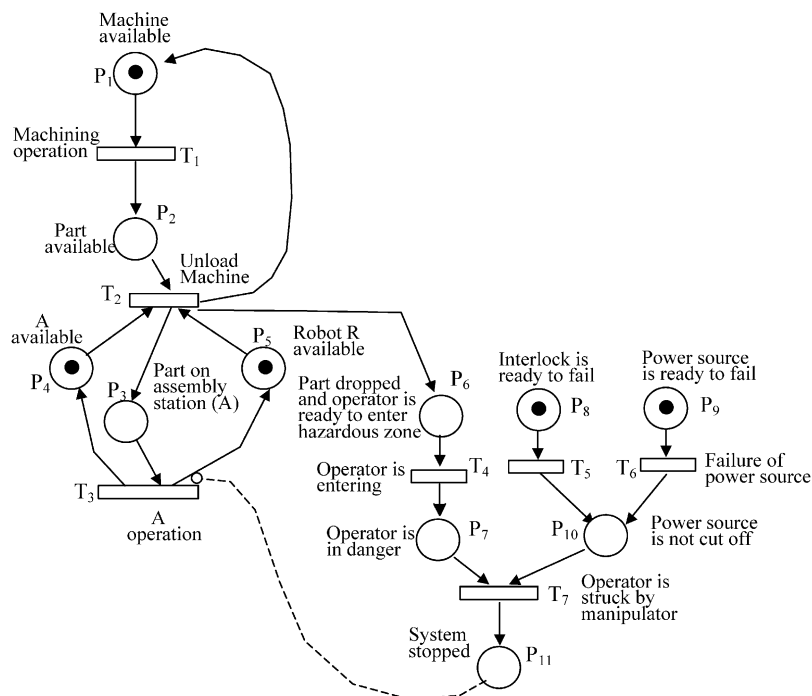


Fig. 8. Petri net model of the machining and assembly system with failures.

Table 2  
List of the markings for the Petri net model shown in Fig. 8

Marking	Place										
	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$	$P_8$	$P_9$	$P_{10}$	$P_{11}$
$M_0$	1	0	0	1	1	0	0	1	1	0	0
$M_1$	0	1	0	1	1	0	0	1	1	0	0
$M_2$	1	0	1	0	0	0	0	1	1	0	0
$M_3$	0	1	1	0	0	0	0	1	1	0	0
$M_4$	1	0	0	1	1	0	0	0	1	1	0
$M_5$	0	1	0	1	1	0	0	0	1	1	0
$M_6$	1	0	1	0	0	0	0	0	1	1	0
$M_7$	0	1	1	0	0	0	0	0	1	1	0
$M_8$	1	0	0	0	0	1	0	0	1	1	0
$M_9$	1	0	0	0	0	0	1	0	1	1	0
$M_{10}$	1	0	0	0	0	0	0	0	1	0	1
$M_{11}$	0	1	0	0	0	1	0	0	1	1	0
$M_{12}$	0	1	0	0	0	0	1	0	1	1	0
$M_{13}$	0	1	0	0	0	0	0	0	1	0	1
$M_{14}$	1	0	0	0	0	1	0	1	1	0	0
$M_{15}$	1	0	0	0	0	0	1	1	1	0	0
$M_{16}$	1	0	0	0	0	0	1	0	1	1	0
$M_{17}$	0	1	0	0	0	1	0	1	1	0	0
$M_{18}$	0	1	0	0	0	0	1	1	1	0	0
$M_{19}$	0	1	0	0	0	0	1	0	1	1	0
$M_{20}$	1	0	0	1	1	0	0	1	0	1	0
$M_{21}$	0	1	0	1	1	0	0	1	0	1	0
$M_{22}$	1	0	1	0	0	0	0	1	0	1	0
$M_{23}$	0	1	1	0	0	0	0	1	0	1	0
$M_{24}$	1	0	0	0	0	1	0	1	0	1	0
$M_{25}$	1	0	0	0	0	0	1	1	0	1	0
$M_{26}$	1	0	0	0	0	0	0	1	0	0	1
$M_{27}$	0	1	0	0	0	1	0	1	0	1	0
$M_{28}$	0	1	0	0	0	0	1	1	0	1	0
$M_{29}$	0	1	0	0	0	0	0	1	0	0	1

with the initial marking  $M_0$ , the reachability tree can be constructed by firing all possible transitions enabled in all possible markings reachable from  $M_0$ . The list of markings for the Petri net in Fig. 8 is presented in Table 2. The reachability tree for the Petri net in Fig. 8 is shown in Fig. 9.

Table 3  
Sequences of transitions that lead to failure of the system

$N$	Interlock fails before operator enters the hazardous zone	$N$	Operator enters the hazardous zone before interlock failures
1	$T_5T_1T_2T_4T_7$	6	$T_1T_2T_1T_4T_5T_7$
2	$T_5T_1T_2T_4T_1T_7$	7	$T_1T_2T_4T_5T_7$
3	$T_1T_2T_5T_4T_7$	8	$T_1T_2T_4T_1T_5T_7$
4	$T_1T_2T_5T_1T_4T_7$		
5	$T_5T_1T_2T_1T_3T_2T_4T_7$		

Markings that have 1 in the place  $P_{11}$  represent the failure of the system and indicate that the operator has been struck by the robot. These markings are  $M_{10}$ ,  $M_{13}$ ,  $M_{26}$ , and  $M_{29}$ . Based on the reachability tree one can easily identify possible sequences of the failures just by following the paths that lead to the system failure markings.

Table 3 lists the sequences of transitions that lead to the failure of the system. First column shows the sequences when interlock failure occurs before the operator enters the system. The second column represents the sequences when the operator enters the system before the failure of the interlock occurs. This could be easily determined by the transition that comes first. The transition  $T_5$  indicates interlock failure and  $T_4$  indicates that the operator entered the system; therefore if  $T_5$  comes before  $T_4$ , then the interlock failure occurs first.

Suppose that we would like to compute the probability that the system will fail in 200 h, given that the interlock fails before the operator enters the hazardous zone. Once the sequences of transitions are identified, the next step is to compute the transitional probabilities. Let us consider the sequence 1 listed in Table 3 for identifying all possible transitional probabilities. The sequence of events  $E = \{M_iM_k, \dots, M_hM_j\}$   $i \neq k \neq h \neq j$  for transitions  $T_5 T_1 T_2 T_4 T_7$  is:  $E = \{M_0M_4, M_4M_5, M_5M_8, M_8M_9, M_9M_{10}\}$ .

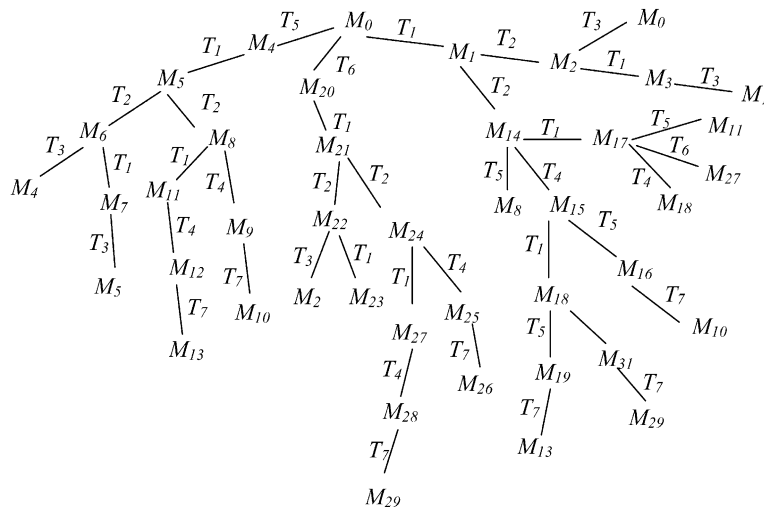


Fig. 9. Reachability tree of the Petri net shown in Fig. 8.

The next step is to compute the approximate time interval between the time at which the transition in the sequence will be able to fire and the time at which the same transition is fired. Then the approximated duration of the stay in the state  $j$  is computed by the following two steps:

*Step 1.* Normalize all transitions firing rates, i.e. summing all firing rates then dividing each by the sum, the results are the weights  $\omega_j$ ;

Weight	$\omega_1$	$\omega_2$	$\omega_4$	$\omega_5$	$\omega_7$
	0.47607712	0.2380385	0.04760771	0.000238	0.23803856

*Step 2.* Compute  $\tau_j$ :  $\tau_j = \omega_j \times T$ , where  $T = 200$  as follows:

Time	$\tau_1$	$\tau_2$	$\tau_4$	$\tau_5$	$\tau_7$
	95.21542	47.60771	9.521542	0.47608	47.60771

At this point we have all information available to compute the transitional probabilities:

$$p_1^1 = Q_{M_0M_4}(\tau) = \int_0^{\tau_5} \lambda_5 e^{-(\lambda_2 + \lambda_5 + \lambda_6)x} dx = 2.324118 E - 05$$

$$p_2^1 = Q_{M_4M_5}(\tau) = \int_0^{\tau_1} \lambda_1 e^{-\lambda_1 x} dx = 1$$

$$p_3^1 = Q_{M_5M_8}(\tau) = \int_0^{\tau_2} \lambda_2 e^{-\lambda_2 x} dx = 0.5$$

$$p_4^1 = Q_{M_8M_9}(\tau) = \int_0^{\tau_4} \lambda_4 e^{-\lambda_4 x} dx = 0.09$$

$$p_5^1 = Q_{M_9M_{10}}(\tau) = \int_0^{\tau_7} \lambda_7 e^{-\lambda_7 x} dx = 1$$

The superscript  $k$  in  $p_i^k$  is the index of the transition sequences that could lead to the failure of the system. Here we present the computation for the first sequence

Table 4  
Probabilities of transferring form marking  $i$  to marking  $j$

Sequence	Equation	Value
$T_5T_1T_2T_4T_7$	$f_{010}^1 = \prod_{i=1}^n p_i^1$	$1.05612 \times 10^{-6}$
$T_5T_1T_2T_4T_1T_7$	$f_{013}^2 = \prod_{i=1}^n p_i^2$	$3.4289 \times 10^{-6}$
$T_1T_2T_5T_4T_7$	$f_{010}^3 = \prod_{i=1}^n p_i^3$	$5.01685 \times 10^{-8}$
$T_1T_2T_5T_1T_4T_7$	$f_{013}^4 = \prod_{i=1}^n p_i^4$	$3.4773 \times 10^{-6}$
$T_5T_1T_2T_1T_3T_2T_4T_7$	$f_{010}^5 = \prod_{i=1}^n p_i^5$	$3.50555 \times 10^{-7}$

listed in Table 3. The subscript  $i$  indicates the number of the events in  $E$ . For example,  $E = \{\overrightarrow{M_0M_4}, \overrightarrow{M_4M_5}, \overrightarrow{M_5M_8}, \overrightarrow{M_8M_9}, \overrightarrow{M_9M_{10}}\}$  has five events, hence,  $i = 1, \dots, 5$ .

The probabilities  $f_{ij}^n$  that starting in marking  $i$  the process will be in marking  $j$  after  $n$  additional transitions in a given sequence are listed in Table 4.

The probabilities that the system will fail in 200 h given

that the interlock fails before the operator enters the hazardous zone is computed as  $\sum_{n=1}^5 f^n = 0.00000731$ .

### 6. Conclusions

The assessment of system reliability and safety with sequential failures plays an important role in improving the reliability and safety of the manufacturing systems, which in turn enhances the usability of the systems and increases overall competitiveness of a manufacturing company.

Current method for assessing reliability and safety of manufacturing systems with sequential failures, known in the literature, is SFL. Although useful, the applications of current research on SFL are rather limited, because the sequences of the failures are assumed to be given for estimating the system failures. Therefore, in this paper we present a method that identifies the sequences of the failures, quantifies the probability of the failures occurring in a sequence, hence, overcomes the limitations of the SFL.

The novel feature of our approach is in utilizing Petri net techniques for modeling the system dynamics, identifying possible failure sequences, and assessing the reliability and safety of the manufacturing systems with sequential failures. The Petri net modeling provides the ability of assessing the reliability and safety impacts caused by the combination of unplanned failures and the sequence of these failures. The Petri net graphical representation is used to construct the cause and effect relationship among the events. The Petri net allows performing comprehensive failure and reliability analysis of the system and approximation of the probability of failures in a sequence.

The method can be used as a comprehensive risk assessment tool for managers to analyze hazardous operations for improving safety of the workers and the overall safety of the systems. Data can also be used for helping the industry to meet safety requirements and to improve the efficiency of new manufacturing system implementations. The results obtained can contribute to the safety and ergonomic aspects in designing and operating manufacturing systems.

An example of an automated machining and assembling system is presented for demonstration of the concept. It is shown that based on reachability tree derived from Petri net model, the sequences of the failures and minimum cut set can be identified. Finally, the probabilities of the sequences of the failures are computed with an approximation method.

### Acknowledgements

This research has been supported by the research grant EPA 82854101 from the US Environmental Protection Agency (EPA).

### References

- [1] Fussel J, Alber E, Rahl R. On the quantitative analysis of priority-AND failure logic. *IEEE Trans Reliab* 1976;25:324–6.
- [2] Ngom L, Cabarbaye A, Barpm C. Taking into account of dependency relations in the Monte Carlo simulation of non-coherent fault trees. *Proceeding of the PSAM-4*. vol. 3, 1998. p. 2067–72.
- [3] Sato Y, Henley E, Inoue K. An action-chain model for the design of hazard control system for robots. *IEEE Trans Reliab* 1990;39:151–7.
- [4] Shibata Y, Sato YA. Case study of risk assessment for product liability prevention. *Proceeding of the PSAM-4*. vol. 2, 1998. p. 1215–20.
- [5] Pickles JH. Stochastic domino model for a sequential failure process. *Reliab Engng* 1986;6(3):219–36.
- [6] Elias S, Mokhles N, El-Sayed E. Consecutive  $k$ -out-of- $n$  system with sequential failures and single repair. *Microelectron Reliab* 1994;34(1):39–51.
- [7] US Nuclear Regulatory Commission. An assessment of accident risk in US commercial nuclear power plants reactor safety study. WASH-1400 (NUREG-75/014): Washington, DC, 1975.
- [8] Long W, Sato Y, Horigone M. Quantification of sequential failure logic for fault tree analysis. *Reliab Engng Syst Saf* 2000;67:269–74.
- [9] Long W, Sato Y. A comparison between probabilistic models for quantification of priority-AND gates. *Proceedings of the PSAM-4*. vol. 2, 1998. p. 1215–20.
- [10] Sato Y. The design of hazard control systems and its PSA for advanced mechatronics. *Proceeding of the PSAM-3*. vol. 3, 1996. p. 1959–64.
- [11] Modares M. *Reliability and risk analysis*. New York: Marcel Dekker, 1993.
- [12] Henley E, Kumamoto H. *Probabilistic risk assessment*. New York: IEEE Press, 1993.
- [13] Long W, Sato Y, Zhang H. Monte Carlo simulation for analysis of sequential failure logic. *IEICE Trans Fundam* 2000;E83-A(5):812–7.
- [14] Peterson J. *Petri net theory and the modeling of systems*. Englewood Cliffs, NJ: Prentice-Hall, 1981.
- [15] Holliday M, Vernon M. A generalized timed Petri net model for performance analysis. *IEEE Trans Software Engng* 1987;SE-13(12):1297–310.
- [16] Murata T. Petri nets: properties, analysis, and applications. *Proc IEEE* 1989;77(4):541–79.
- [17] Ramaswamy V. Extended Petri net-based modeling, analysis and simulation of an intelligent materials handling system. *J Intell Robot Syst: Theory Applic* 1994;10(1):79–108.
- [18] Liu T, Chiou B. Application of Petri nets to failure analysis. *Reliab Engng Syst Saf* 1997;57:129–42.
- [19] Zhou M, Zurawski R. In: Zhou R, editor. *Introduction to Petri nets in flexible and agile automation in Petri nets in flexible and agile automation*. Norwell, MA: Kluwer, 1995. p. 1–42.
- [20] Molloy M. Performance analysis using stochastic Petri nets. *IEEE Trans Comput* 1982;3(9):913–7.
- [21] Molloy MK. Discrete time stochastic Petri nets. *IEEE Trans Software Engng* 1985;SE-11(4):417–23.
- [22] Florin G, Fraize C, Natkin S. Stochastic Petri nets: properties, applications, and tools. *Microelectron Reliab* 1991;31(4):669–97.
- [23] Chiola GA. Graphic Petri net tool for performance analysis. *Proceedings of International Workshop on Modeling Techniques and Performance Evaluation*, France. 1987. p. 323–33.
- [24] Ciardo G. *Manual for the SPNP package*. NC: Duke University, 1989.
- [25] Al-Jaar R, Desrochers A. Performance evaluation of automated manufacturing systems using generalized stochastic Petri nets. *IEEE Trans Robotics Automn* 1990;6(6):621–39.
- [26] Yellman T. Failures and related topics. *IEEE Trans Reliab* 1999;48:6–8.
- [27] Nakada K, Yoneyama T. A method to abstract Petri net. *Mathl Comput Model* 2000;31:251–60.
- [28] Ross S. *Probability models*. 4th ed. Boston: Academic Press, 1989.