HYBRIDGE

Distributed Control and Stochastic Analysis of Hybrid Systems
Supporting Safety Critical Real-Time Systems Design

WP8: Accident risk decomposition

Risk Decomposition and Assessment methods

Jaroslav Krystul[1], Arun Bagchi[1], Henk Blom[2]

27th June 2003

Version: *1.0*
Task number: *8.1*
Deliverable number: *D8.1*
Contract: *IST-2001-32460 of European Commission*

[1] Twente University, NL

[2] National Aerospace Laboratory NLR, NL

DOCUMENT CONTROL SHEET

Title of document: *Risk Decomposition and Assessment methods*

Authors of document: *J. Krystul, A. Bagchi, H.A.P. Blom*

Deliverable number: *D8.1*

Contract: *IST-2001-32460 of European Commission*

Project: *Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design (HYBRIDGE)*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
0.1	21 Nov. 2003	2, 3	1st draft
0.2	11 Dec. 2003	2, 3, 4	2nd draft
0.3	15 Jan. 2003	2, 3, 4, 5	3rd draft
0.4	23 Jan. 2003	All	4th draft
0.5	27 Jan 2003	1,2,3	5th draft
0.6	05 Feb. 2003	2,5	Draft final
0.7	18 Apr. 2003	2,3	Update draft final
1.0	24 Jun. 2003	2,3	Final

Version 0.6		Organisation	Signature/Date
Authors	Jaroslav Krystul	TWEN	
	Arun Bagchi	TWEN	
	Henk Blom	NLR	
Internal reviewers	François LeGland	INRIA	
	Fabien Campillo	INRIA	

Contents

1 Introduction

Accident risk assessment has been widely studied for various safety-critical operations, such as the nuclear and chemical industries, advanced air traffic management (ATM) and many others. Accident risk assessment for safety critical operations has to be done by an appropriate combination of stochastic analysis and Monte Carlo simulations. Unfortunately at this moment the identification of an appropriate way to combine both approaches is more an art than a science. When the scale of complexity of an operation increases, the art tends to fall short. The aim of work package WP8 is to develop novel methods for the assessment of risk such that extreme low risk values for safety critical operations can be better assessed.

The present report reviews existing risk assessment methods, both analytical ones, numerical and Monte Carlo simulation approaches that are developed for safety critical operations in e.g. nuclear and petrochemical industries. In the following tasks of WP8 we will attempt to develop new risk assessment methods and compare them with the existing ones identified in this report.

In order to carry out the risk assessment of a particular safety critical operation, we build a mathematical model, i.e. describe the dynamic evolution of the operation by a set of coupled and interacting discrete event models and differential equations. The time evolution of such a model can often be represented by hybrid state Markov processes. For example, for accident risk modelling in ATM we describe the aircraft evolution by a hybrid state Markov process composed of a two components: a continuous and a discrete. The continuous component is required to model random motion of aircraft due to e.g. variations in wind, while the discrete component is required to model switches in aircraft operational modes, e.g. switches from a nominal behavior of aircraft to a non-nominal behavior (which can e.g. be hardware failures). This aspect is being studied in Hybridge WP2 ([Blom et al 03]).

Similarly as in [Blom et al 03] we consider two different probabilistic risk measures: the probability of a collision and the in-crossing probability, where in-crossing probability is an ICAO adopted metric.

In order to evaluate the in-crossing probability it is very important to characterize the evolution of the probability-density function of the hybrid state Markov process. Theoretically, it is possible to characterize the forward evolution of the density through an appropriate integro-partial differential equation. Unfortunately, solving this equation analytically or numerically is not realistic when the dimension is as high as it is in ATM. Hence, we need adequate numerical approximation and Monte Carlo techniques. Such numerical approaches are generally based on discretization of either time or space variables or on simultaneous discretization of both. The Monte Carlo methods estimate the safety characteristics from information retrieved from a independently generated sample paths. The main advantage of Monte Carlo method is that it can be applied to any hybrid state Markov process model rather easily. It is almost insensitive to the dimensionality of the problem. However, the standard Monte Carlo methods may occur to be too time-consuming for accident assessment in ATM.

In order to avoid ambiguity, this report presents the relevant literature results (often from physics literature) identified in a stochastic analysis setting.

The report is organized as follows. Section 2 formulates the problem. Section 3 begins with a classification of the hybrid state Markov processes, followed by the characterization of the density functions of some of them. The review of numerical evaluations of probability-density functions is given in section 4. The Monte Carlo simulation approaches are discussed in section 5.

2 Problem formulation

2.1 Notations

In this section we briefly explain some notations used in this report.

Let $(\Omega, \mathcal{F}, P)$ define a given probability space. A *random variable* X is a measurable function $X : (\Omega, \mathcal{F}) \to (\mathbb{R}^n, \mathcal{B})$, in which $\mathcal{B}$ is the Borel σ-algebra on $\mathbb{R}^n$. Let us take $T \subset \mathbb{R}_+ \stackrel{\triangle}{=} [0, \infty)$ as the time-axis. A *stochastic process* defined on $(\Omega, \mathcal{F})$ with values in $(\mathbb{R}^n, \mathcal{B})$ is a family $\{x_t,\, t \in T\}$ (short notation $\{x_t\}$) of $\mathbb{R}^n$ valued random variables. $(\Omega, \mathcal{F})$ is called the base space and $(\mathbb{R}^n, \mathcal{B})$ is the state space. For fixed $t \in T$, random variable $x_t(\omega) = \{x_{1,t}, x_{2,t}, \ldots, x_{n,t}\}^T \in \mathbb{R}^n$ is the state of process at time t. For fixed $\omega \in \Omega$ $\{x_t(\omega); t \in T\}$ is called the sample path (or trajectory) associated with ω.

A filtered probability space $(\Omega, \mathcal{F}, \{\mathcal{F}_t\}, P)$ is a probability space $(\Omega, \mathcal{F}, P)$ with filtration $\{\mathcal{F}_t, t \in \mathbb{R}_+\}$. This filtration is defined as any family of sub-σ-algebras such that $\mathcal{F}_s \subset \mathcal{F}_t$ for $s \leq t$, and it describes the history of some phenomenon. The filtration that we will usually consider are natural filtration of processes. The natural filtration of a process $\{x_t\}$ is the filtration that describes the history of the process $\{x_s\}$ until moment t. It is defined as the smallest σ-algebra in $\mathcal{F}$ with respect to which all the random variables $\{x_s, s \leq t\}$ are measurable, and it is denoted by $\{\mathcal{F}_t^x\}$. A process $\{x_t\}$ is adapted to $\{\mathcal{F}_t\}$ if, for every $t \in \mathbb{R}_+$, x_t is an $\mathcal{F}_t$-measurable random variable. Without loss of generality, we assume that filtration $\{\mathcal{F}_t\}$ is complete, i.e. $\mathcal{F}$ is complete and each $\mathcal{F}_t$ contains all P-null sets of $\mathcal{F}$.

Most processes that we will consider have a hybrid state, that is $\xi_t = (\theta_t, x_t)$, in which θ_t assumes values in a finite discrete state space $\mathbb{M}$ and x_t assumes values in the n-dimensional Euclidean state space $\mathbb{R}^n$. Thus $\xi_t \in \mathbb{M} \times \mathbb{R}^n$ for all $t \in \mathbb{R}_+$. A realization $\omega \in \Omega$ determines a trajectory $\{\xi_t(\omega)\}$. The filtration $\mathcal{F}_t$ that we will generally consider is the natural filtration $\mathcal{F}_t^\xi$ of the process $\{\xi_t\}$.

A stopping time τ on the filtered probability space $(\Omega, \mathcal{F}, \{\mathcal{F}_t\}, P)$ is a random variable $\tau : \Omega \to \mathbb{R}_+$, such that $\{\tau \leq t\} \stackrel{\triangle}{=} \{\omega \in \Omega | \tau(\omega) \leq t\} \in \mathcal{F}_t$ for every $t \in \mathbb{R}_+$.

Every random variable $X : (\Omega, \mathcal{F}) \to (\mathbb{R}^n, \mathcal{B})$ induces a probability distribution P_X on the Borel sets of $\mathbb{R}^n$. For any Borel set $B \in \mathbb{R}^n$, the probability $P_X(B)$ is defined by relation

$$P_X(B) = P(\omega : X(\omega) \in B).$$

If random variable Y takes only a countable (perhaps finite) number of distinct values on set $\mathbb{M} = \{1, 2, \ldots\}$, then the *probability function* of it is the function $p_Y(\cdot)$ defined by the relation

$$p_Y(y) = P(\omega : Y(\omega) = y),$$

where $y \in \mathbb{M}$. Then, for any set $B \subset \mathbb{M}$

$$p_Y(B) = \sum_{y \in B} p_Y(y). \tag{1}$$

In this case a random variable Y is said to have a discrete distribution.

Random variable X has an absolutely continuous distribution if there exists a nonnegative *joint density function* $p_X(x)$, $x \in \mathbb{R}^n$, such that for any Borel set $B \subset \mathbb{R}^n$,

$$P_X(B) = \int_B p_X(x)dx.$$

Now, let consider the hybrid state space process $\{\theta_t, x_t\}$. For any fixed $t \in T$ the component θ_t has a discrete distribution while the x_t has an absolutely continuous distribution. If there exists[1] a joint density function of random variables (θ_t, x_t) then it is convenient to represent it by a function $p_{\theta_t,x_t}(\theta, x)$ which might be called the *joint probability-density function* (for short we will call it the *density function*). It is, of course, essential to keep in mind that probabilities of various events in $\mathbb{M} \times \mathbb{R}^n$ are computed from any joint probability-density function by integrating for some components and summing for the others, for example, for any set $\Theta \subset \mathbb{M}$ and any Borel $B \subset \mathbb{R}^n$

$$P_{\theta_t,x_t}(\Theta, B) = \sum_{\theta \in \Theta} \int_B p_{\theta_t,x_t}(\theta, x)dx$$

One can prove that the following relations for the density functions (if they exist) of the components of the random variables $x_t = (x_{1,t}, x_{2,t}, \ldots, x_{n,t})^T \in \mathbb{R}^n$ and $(\theta_t, x_t) = (\theta_t, x_{1,t}, x_{2,t}, \ldots, x_{n,t})^T \in \mathbb{M} \times \mathbb{R}^n$ hold:

$$p_{\theta_t,x_{k,t}}(\theta, x_k) = \int p_{\theta_t,x_t}(\theta, x)dx_1 \ldots dx_{k-1}dx_{k+1} \ldots dx_n, \ k = 1, \ldots, n \tag{2}$$

$$p_{x_t}(x) = \sum_{\theta} p_{\theta_t,x_t}(\theta, x) \tag{3}$$

$$p_{x_{k,t}}(x_k) = \int p_{x_t}(x)dx_1 \ldots dx_{k-1}dx_{k+1} \ldots dx_n, \ k = 1, \ldots, n \tag{4}$$

We will use them often in this report.

Let A and B be two events and $P(B) > 0$. We define the *conditional probability* of A given that B has occurred as follows.

$$P(A|B) \triangleq \frac{P(A \cap B)}{P(B)}.$$

Suppose for any fixed t, $u \in T$, there exist the joint probability-density functions

[1] Important to note that it is not always the case.

$p_{\theta_t,x_t,\theta_u,x_u}(\theta,x,\theta',x')$ and $p_{\theta_u,x_u}(\theta',x') > 0$, then we can define another density

$$p_{\theta_t,x_t|\theta_u,x_u}(\theta,x|\theta',x') \triangleq \frac{p_{\theta_t,x_t,\theta_u,x_u}(\theta,x,\theta',x')}{p_{\theta_u,x_u}(\theta',x')}.$$

This function is called *conditional joint probability-density function* (for short we will call it the *conditional density function*) of (θ_t, x_t) given (θ_u, x_u).

The *conditional transition probability* from $\theta_s = \eta$ to $\theta_t = \theta$, given $x_s = x$ is:

$$p_{\theta_t|\theta_s,x_s}(\theta|\eta,x) = P(\omega : \theta_t(\omega) = \theta|\theta_s(\omega) = \eta, x_s(\omega) = x),\ t > s.$$

Let K be a set of real numbers with a limit point a. Let $f, g : K \to \mathbb{R}$ be some functions on K. Then we define the following asymptotic estimate:

$$f(x) = o(g(x)) \quad (x \to a,\ x \in K)$$

$$\text{if} \quad \lim_{x\to a,\ x\in K} \frac{f(x)}{g(x)} = 0.$$

2.2 Mathematical modeling of complex systems

Very often we want to find out how safe is a particular system. But before we start assessing the risk of occurrence of undesirable events, we try to represent a complex dynamic system by a set of ordinary (stochastic) differential equations (ODEs/SDEs). The term "dynamic" emphasizes the fact that the system can evolve dynamically and many different factors can influence the dynamics.

Suppose the state of the system at time t is described by the process $\{\xi_t\}$. One can consider a more general setting when process $\{\xi_t\}$ can be decomposed into a discrete and a (piecewise) continuous components: $\xi_t = \{\theta_t, x_t\}$, where $\theta_t \in \mathbb{M} = \{1, 2, \ldots, N\}$ and $x_t \in \mathbb{R}^n$. The discrete component θ_t describes the mode of the system. This mode variable represents discrete valued process changes under sudden impacts such as failures or changes of environment or control. The continuous valued component x_t of the process describes the evolution of the system between mode switches. The components of the vector $x(t) = (x_1(t), x_2(t), \ldots, x_n(t))^T$ may for example represent temperature, velocity, pressure and so on.

In section (3) we provide the classification of different types of hybrid state processes that can be used for modelling of stochastic systems.

2.3 The concept of risk

There are multiple concepts of risk [Roya92]. Hence, it is important to specify what do we mean by *risk*. In this report we use the following definition of risk adopted by [Roya92]. We treat the *risk* as the probability that a particular adverse event occurs during a stated period of time. As a probability in the sense of statistical theory risk obeys all the formal laws of combining probabilities.

Explicitly or implicitly, it must always relate to the 'risk of (a specific event or set of events)' and where appropriate must refer to an exposure to hazard specified in terms of its amount or intensity, time of starting or duration. Such a definition allows one to calculate a numerical value of *risk*.

2.4 In-crossing probability

As we already have mentioned, in order to perform the analysis of a complex dynamic system we describe its states by stochastic process $\{x_t\}$. In particular we are interested in determining the probability that $\{x_t\}$ will cross the boundary of some domain D in time interval $[t_1, t_2]$ and also in determining the expected number of crossings of this boundary during $[t_1, t_2]$.

Let closed and connected set $D \subset \mathbb{R}^n$ denote the collision domain of $\{x_t\}$. If at some time moment τ the process $\{x_t\}$ hits the boundary of D then we say that an in-crossing has occurred at stopping (hitting) time τ. The first in-crossing of D by the process $\{x_t\}$ on the interval $[t_0, t_1]$ is called collision on $[t_0, t_1]$. Furthermore, we denote by $\left\{\chi_t^+\right\}$ (see [Blom94]) the process which counts the number of in-crossings of $\{x_t\}$ into D.

Next we define two different probabilistic risk metrics: the probability of a collision and the probability of an in-crossing. The in-crossing probability is defined by [BlomBakk02]

$$P_{in}(t_0, t_1) \stackrel{\triangle}{=} 1 - \exp\left\{-I_{in}(t_0, t_1)\right\}$$

where $I_{in}(t_0, t_1)$ is the expected number of in-crossings on $[t_0, t_1]$, i.e.

$$I_{in}(t_0, t_1) = E\left[\int_{t_0}^{t_1} d\chi_s^+\right].$$

This ICAO adopted safety metric arose from the studies of Rice [Rice45] and Reich [Reich64] and its development was continued by Blom et al [BlomBakk02], [Bakk93] and [Blom94]. The main feature of this metric is that it is based on the evaluation of the expected number of in-crossings and closed-form formulae are available under particular conditions and assumptions (see [Rice45], [Reich64] and [BlomBakk02]).

The probability of a collision in time period $[t_0, t_1]$ is defined as follows

$$P_{coll}(t_0, t_1) \stackrel{\triangle}{=} P(\exists \text{ at least one in-crossing on } (t_0, t_1])$$

We can also write this as

$$P_{coll}(t_0, t_1) = P(\chi_{t_1}^+ \neq \chi_{t_0}^+)$$

For particular types of Markov processes $\{x_t\}$, this risk metric can be numerically evaluated through solving a backward Kolmogorov partial differential equation with Dirichlet boundary conditions [Gihm&Skor72], [Freid84] pp.102-107. However, the complexity of a numerical evaluation of such a boundary-valued PDE becomes dramatically large when applied to the kind of problems as considered in air traffic.

2.5 Top and Rare events

In this report we often use the term "top event" and "rare event". Here we provide the mathematical definition of these terms.

The event $\chi_t^+ \neq \chi_{t-}^+$ is called a *top event*. If respectively $P_{coll}(t_0, t_1) \leq \varepsilon$ or $P_{in}(t_0, t_1) \leq \varepsilon$ where ε - some small number, then this top event is called a *rare event*. The particular choice of the ε value depends on the situation and context considered. In air traffic management several ε values for collision risk are accepted, e.g. [Blom et al 03].

In safety critical operations top events by their very nature are rare events. The estimation of the probability of occurrence of top events sometimes may be reduces to estimation of a density function $p_{x_t}(x)$ (if exists), for all $t \in (t_0, t_1]$.

2.6 Accident risk assessment in Air Traffic Management

In this section we give a brief illustration of the risk assessment in ATM. For detailed description of the model we refer to [Bakk93], [BlomBakk02] and [Blom et al 03].

We illustrate how one can evaluate the risk of collision between a pair of aircraft. We assume that each aircraft is represented as a box having a fixed orientation. And we assume that evolution of the pair of aircraft is represented by stochastic differential equations, one for each aircraft, i.e. for $i = 1, 2$,

$$dx_t^i = a^i(x_t)dt + b^i(x_t)dw_t^i,$$

with $x_t = \{x_t^1, x_t^2\}^T$, $w_t = \{w_t^1, w_t^2\}$, w_t^i an n-dimensional standard Brownian motion, $\{x_t^i\}$ assumes values in $\mathbb{R}^n$. Some elements of x_t^i form a 3D position s_t^i of aircraft i,

$$s_t^i = Hx_t^i,$$

with H a $3 \times n$-matrix. To avoid the Brownian motion behavior in positions, the following assumption is adopted

$$Hb^i(x_t) = 0 \text{ for } i = 1, 2.$$

Hence

$$ds_t^i = v_t^i dt \text{ with } v_t^i \triangleq Ha^i(x_t).$$

Next, let s_t^1 and s_t^2 represent the positions of centres of aircraft pair. Then by

$$s_t = s_t^1 - s_t^2$$

we denote the relative position. The relative velocity is represented in a similar

way

$$v_t = v_t^1 - v_t^2.$$

Hence

$$ds_t = v_t dt.$$

Let define the collision domain $D \equiv D_1 \times D_2 \times D_3$ ($D_k = [-m_k, m_k]$) as a box of a size of two aircraft with center in the origin of axis. If the relative position $\{s_t\}$ enters D then we say an in-crossing event (top event) occurred.

The probability of in-crossing of the pair of aircraft during the time period $[0, T]$ is given by

$$P_{in}(0,T) = 1 - \exp\left\{-E\left[\int_0^T d\chi_s^+\right]\right\}.$$

In [Blom94] it is shown that under some technical conditions:

$$E\left[\int_0^T d\chi_s^+\right] = \int_0^T \phi(s)ds$$

with $\phi(t)$ the in-crossing rate, which is defined, if the limit exists, as

$$\phi(t) \stackrel{\triangle}{=} \lim_{\Delta \downarrow 0} \frac{P(s_{t-\Delta} \notin D, s_t \in D)}{\Delta}.$$

In [Bakk93] and [BlomBakk02], characterizations of the in-crossing rate $\phi(t)$ have been derived under very general conditions. In [Bakk93] the following characterization for in-crossing rate has been developed:

$$\phi(t) = \sum_{k=1}^{3} \int_{\underline{D}_k} \left\{ \int_0^\infty v_k p_{s_t, v_{k,t}}(\underline{s}_k, -m_k, v_k) dv_k + \int_{-\infty}^0 -v_k p_{s_t, v_{k,t}}(\underline{s}_k, m_k, v_k) dv_k \right\} d\underline{s}_k \tag{5}$$

where

$$\begin{array}{lll} \underline{D}_1 \equiv D_2 \times D_3, & \underline{D}_2 \equiv D_1 \times D_3, & \underline{D}_3 \equiv D_1 \times D_2 \\ \underline{s}_1 \equiv (s_2, s_3), & \underline{s}_2 \equiv (s_1, s_3), & \underline{s}_3 \equiv (s_1, s_2) \end{array}$$

This model with the characterization for the in-crossing (5) is referred to as the generalized Reich collision risk model. It assumes that the process $\{s_t, v_t\}$ admits a density function $p_{s_t, v_t}(\cdot)$. For numerical evaluation of $\phi(t)$ there is a need to characterize the probability density function $p_{s_t, v_t}(\cdot)$. Characterizing this probability density thus is an important part of the accident risk assessment problem.

3 Hybrid state Markov processes

3.1 Types of hybrid state space processes

In the sequel we will consider processes $\{\xi_t\}$ that assume values in a hybrid state space, i.e. $\mathbb{M} \times \mathbb{R}^n$, where $\mathbb{M} = \{1, 2, \ldots, N\}$. This covers a rich family of processes. By varying the size of $\mathbb{M}$, the dimension of $\mathbb{R}^n$ and the type of randomness we get many combinations. These are depicted in the next table

Table 1: Types of hybrid state space processes. n stands for dimension of continuous component $\{x_t\}$, and $|\mathbb{M}|$ denotes the dimension of the state space of discrete component $\{\theta_t\}$.

Code	Characteristics
A.1	$n = 0, \theta \in \mathbb{M}$
A.2	$\lvert\mathbb{M}\rvert = 1, n \geq 1$
A.2.1	Drift only
A.2.2	Drift + diffusion
A.2.3	Drift + diffusion + Poisson jumps
A.2.4	Drift + diffusion + Poisson jumps + boundary hitting
A.3	$\lvert\mathbb{M}\rvert > 1, n \geq 1$, switching coefficients
A.3.1	Drift only
A.3.2	Drift + diffusion
A.3.3	Drift + diffusion + Poisson jumps
A.3.4	Drift + diffusion + Poisson jumps + boundary hitting
A.4	$\lvert\mathbb{M}\rvert > 1, n \geq 1$, switching coefficients, Hybrid jumps
A.4.1	Drift only
A.4.2	Drift + diffusion
A.4.3	Drift + diffusion + Poisson jumps
A.4.4	Drift + diffusion + Poisson jumps + boundary hitting

In the accident risk assessment literature it appears that type A.3.1 hybrid state space processes are the most complex equations studied. For air traffic this is not sufficient [Blom et al 03].

3.2 Characterization of the density of a diffusion process

Suppose the evolution of the vector processes $\{x_t\} \in \mathbb{R}^n$ obeys the equations of type **A.2.2**

$$dx_t = a(x_t)dt + b(x_t)dw_t \tag{6}$$

where $a(x) : \mathbb{R}^n \to \mathbb{R}^n$, $b(x) : \mathbb{R}^n \to \mathbb{R}^{n \times n}$ and $\{w_t\}$ is a Wiener process in $\mathbb{R}^n$.

Assuming that all appropriate conditions of pathwise existence and uniqueness are satisfied, one can prove that the transition density function $p_{x_t|x_s}(x|y)$ exists [Gihm&Skor82]. Suppose, the derivatives

$$\frac{\partial(a_i(x)p_{x_t|x_s}(x|y))}{\partial x_i},$$

$$\frac{\partial^2(\sigma_{ij}(x)p_{x_tx_s}(x|y))}{\partial x_i \partial x_j},\ i,j=1,2,\ldots,n,$$

exist and are continuous, where $\sigma_{ij}(x)=\sum_{r=1}^{n} b_{jr}(x)b_{ir}(x)$. Then, $p_{x_t|x_s}(x|y)$ satisfies the following partial differential equation

$$\frac{d}{dt}p_{x_t|x_s}(\cdot|y)=\mathcal{L}^\star p_{x_t|x_s}(\cdot|y),\ s\le t \tag{7}$$

where the operator $\mathcal{L}^\star$ is the adjoint of the generator of the Markov process $\{x_t\}$. Writing $\mathcal{L}^\star f(\cdot)$ will denote that operator $\mathcal{L}^\star$ acts on the function $f(\cdot)$ ($f:\mathbb{R}^n\to\mathbb{R}$). The formal adjoint of the generator of the process $\{x_t\}$ as solution of SDE (6) is given by [Gihm&Skor72]:

$$\mathcal{L}^\star f(x)\triangleq -\sum_{i=1}^{n}\frac{\partial(a_i(x)f(x))}{\partial x_i}+\frac{1}{2}\sum_{i,j=1}^{n}\frac{\partial^2(\sigma_{ij}(x)f(x))}{\partial x_i\partial x_j}.$$

3.3 Characterization of the density function of a diffusion with switching coefficients

Now, let us consider the situation when the evolution of the process $\{\theta_t,x_t\}\in\mathbb{M}\times\mathbb{R}^n$ is governed by the equations of type **A.3.2**:

$$dx_t = a(\theta_t,x_t)dt+b(\theta_t,x_t)dw_t, \tag{8}$$

$$p_{\theta_{t+\delta}|\theta_t,x_t}(\theta|\eta,x) = \lambda_{\eta\theta}(x)\delta+o(\delta),\ \eta\neq\theta. \tag{9}$$

Here $\lambda_{\eta\theta}(x)\ge 0$, $(\eta\neq\theta)$ is the conditional rate at which the process $\{\theta_t\}$ switches from state η to state θ given $x_t=x$. Note that in (9) the process $\{\theta_t\}$ is a pure jump finite state process with state-dependent transition rates $\lambda_{\eta\theta}(x)$. It may be represented as a stochastic integral with respect to a Poisson random measure. Indeed, let $\Delta_{\eta\theta}$ be consecutive (with respect to the lexicographical ordering on $\mathbb{M}\times\mathbb{M}$)[2], left closed, right open intervals of the real line each having length $\lambda_{\eta\theta}(x)$. Define a function $h:\mathbb{M}\times\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$ by

$$h(\theta,x,u)=\begin{cases}\eta-\theta, & \text{if } z\in\Delta_{\eta\theta}\\ 0, & \text{otherwise.}\end{cases} \tag{10}$$

[2]For details see [Ghosh93] or [Ghosh97]

Then

$$d\theta_t = \int_{\mathbb{R}} h(\theta_{t-}, x_t, u)p(dt, du) \tag{11}$$

where $p(dt, du)$ is a Poisson random measure with intensity $dt \times du$. Thus the process $\{\xi_t\} = \{\theta_t, x_t\}$ governed by equations (8-9) may be represented as the $\mathbb{M} \times \mathbb{R}^n$-valued process given by the following stochastic differential equations [Ghosh93]

$$\begin{aligned} dx_t &= a(\theta_t, x_t)dt + b(\theta_t, x_t)dw_t & (12)\\ d\theta_t &= \int_{\mathbb{R}} h(\theta_{t-}, x_t, u)p(dt, du) & (13) \end{aligned}$$

for $t \geq 0$, where

1. the initial value x_0 is a prescribed $\mathbb{R}^n$-valued random variable
2. the initial value θ_0 is a prescribed $\mathbb{M}$-valued random variable
3. $w = [w_1, \ldots, w_n]^T$ is an n-dimensional standard Wiener process independent of x_0 and θ_0.
4. $p(\cdot, \cdot)$ and w are independent.

Given that all appropriate conditions of pathwise existence and uniqueness are satisfied, the solution of SDE (12-13) is a Markov process and the transition probability has a density $p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y)$ [Gihm&Skor82]. Again, assume that the derivatives

$$\frac{\partial(a_i(\theta, x)p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y))}{\partial x_i},$$

$$\frac{\partial^2(\sigma_{ij}(\theta, x)p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y))}{\partial x_i \partial x_j},\ i, j = 1, 2, \ldots, n,\ \theta, \eta \in \mathbb{M}$$

exist and are continuous, where $\sigma_{ij}(\theta, x) = \sum_{r=1}^{n} b_{jr}(\theta, x)b_{ir}(\theta, x)$. Then, $p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y)$ satisfies the following integro-partial differential equation

$$\frac{d}{dt}p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y) = \mathcal{A}^\star p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y),\ s \leq t, \tag{14}$$

where the operator $\mathcal{A}^\star$ is the adjoint of the generator of the hybrid state Markov process $\{x_t, \theta_t\}$ and is given by

$$\mathcal{A}^\star f(\theta, x) \stackrel{\triangle}{=} \mathcal{L}_\theta^\star f(\theta, x) + \sum_{\eta \in \mathbb{M},\ \eta \neq \theta} \left[\lambda_{\eta\theta}(x)f(\eta, x) - \lambda_{\theta\eta}(x)f(\theta, x)\right], \tag{15}$$

where $\mathcal{L}_\theta^\star$ is the adjoint of the generator of SDE (8) if $\theta_t = \theta$.

$$\mathcal{L}_\theta^\star f(\theta, x) \stackrel{\triangle}{=} -\sum_{i=1}^{n} \frac{\partial(a_i(\theta, x) f(\theta, x))}{\partial x_i} + \frac{1}{2} \sum_{i,j=1}^{n} \frac{\partial^2(\sigma_{ij}(\theta, x) f(\theta, x))}{\partial x_i \partial x_j}. \tag{16}$$

The domain of operators $\mathcal{A}^\star$ and $\mathcal{L}_\theta^\star$ are real valued functions on $\mathbb{M} \times \mathbb{R}^n$ which are twice continuously differentiable on $\mathbb{R}^n$ for each $\theta \in \mathbb{M}$.

Remark 1 *Equations of type* ***A.3.1*** *can be obtained by assuming coefficient* $b(\theta_t, x_t) = 0$ *in equation (8). So, the deterministic behavior between transitions of system states is assumed:*

$$\frac{dx_t}{dt} = a(\theta_t, x_t), \tag{17}$$

$$p_{\theta_{t+\delta}|\theta_t, x_t}(\theta|\eta, x) = \lambda_{\eta\theta}(x)\delta + o(\delta), \ \eta \neq \theta. \tag{18}$$

The adjoint of the generator for this case is obtained by substituting $\sigma(\theta, x) = 0$ *in equation (16).*

Remark 2 *Then the transition density is characterized by the following integro-partial differential equation:*

$$\begin{aligned} \frac{d}{dt} p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y) &= \mathcal{L}_\theta^\star p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y) \\ &\quad + \sum_{\kappa \in \mathbb{M}, \ \kappa \neq \theta} \big[\lambda_{\kappa\theta}(x) p_{\theta_t, x_t|\theta_s, x_s}(\kappa, x|\eta, y) \\ &\qquad - \lambda_{\theta\kappa}(x) p_{\theta_t, x_t|\theta_s, x_s}(\theta, x|\eta, y)\big]. \end{aligned} \tag{19}$$

where

$$\mathcal{L}_\theta^\star f(\theta, x) = -\sum_{i=1}^{n} \frac{\partial(a_i(\theta, x) f(\theta, x))}{\partial x_i}. \tag{20}$$

4 Numerical evaluation of probability-density function

Several attempts have been made at finding analytical solutions of equations (7) and (14) in closed form. This is possible only in some special cases, when these equations are of a very simple form. Classical numerical schemes for a direct solution of the system of integro-partial differential equations also are not efficient, especially when treating systems with large values of n and N.

In the next sections we will review the existing approximate numerical methods for estimation of the density function $p_{x_t|x_s}(x|y)$ or $p_{\theta_t,x_t|\theta_s,x_s}(\theta,x|\eta,y)$. All these appear to apply to equations of type **A.3.1** only.

We consider four approaches:

1. Simultaneous discretization of time and of the space variables ([Alde87], [Alde91], [Hass90] and [Belh96]) in section 4.1
2. Discretization of space variables only ([Tomb96a] and [Tomb96b]) in section 4.2
3. Discrete dynamic event trees (DDETs), where only the time variable is discretized ([Amen84], [Rein87], [Coja93], [AcoSiu93] and [SiuAco90]) in section 4.3.
4. Density function interpolation approach ([LabDev95]) in section 4.4

4.1 Discretization of time and space variables

In what follows, we will consider the cell-to-cell mapping techniques (CCMT) (sometimes referred to as discrete state transition or Markov state-transition models) to the risk analysis of process control systems (PCSs) ([Alde87], [Alde91], [Hass90]). PCSs are frequently used in process plants (e.g. nuclear or fossil fuel power plants, chemical plants) to maintain the magnitudes of continuous process variables such as pressure, temperature and flow rate within allowed ranges.

Historically, CCMT method was introduced as an extension of a classical discrete Markovian treatment of reliability to PCSs, i.e. systems presenting control loops and continuous dynamic variables.

The cell-to-cell mapping approach under consideration regards system evolution in time as probability of transition of the process $\{x_t\}$ variables $x_{i,t}$ $(i = 1,\ldots,n)$ between their specific magnitude intervals. These intervals form n-dimensional cells V_j in the system state-space. The model inputs are the following:

1. a set of equations describing the system dynamics under normal and abnormal operation

$$\frac{dx_t}{dt} = a(\theta_t, x_t), \tag{21}$$

$$p_{\theta_{t+\delta}|\theta_t,x_t}(\theta|\eta,x) = \lambda_{\eta\theta}(x)\delta + o(\delta),\ \eta \neq \theta, \tag{22}$$

where $\{\theta_t, x_t\} \in \mathbb{M} \times \mathbb{R}^n$. The formal solution of equation (21) is given by $x_t = \bar{g}(\theta_t, x_0, t)$, $x_0 = \bar{g}(\theta_0, x_0, 0)$.

2. undesirable events (Top Events) defined in terms of process variables magnitude intervals in the $D \subset \mathbb{R}^n$; boundaries of the area $D^c \triangleq \mathbb{R}^n \backslash D$.

3. boundaries of the cells

$$V_j \equiv V_{j_1,j_2,\ldots,j_n} = \left\{x_{i,t} : \alpha_{i,j_i} \leq x_{i,t} \leq \beta_{i,j_i}; j_i = 1 \ldots J_i; i = 1, \ldots, n\right\}$$

for all t, (i.e. the set of $\alpha_{i,j}$ and $\beta_{i,j}$) that partition D^c (for $j = 1, \ldots, J$) and D (for $j = J+1, \ldots, J+\Gamma$ where Γ - is the number of supplementary cells which cover the complement of D^c). The states V_j ($j = J+1, \ldots, J+\Gamma$) are considered as absorbing states.

4. possible component state combinations (including operator state) and transition probabilities between these state combinations during a specified interval $[t, t+\tau]$.

The equation (21) describing the system dynamics may incorporate complex control laws and may be available in the form of a computer code (simulator) rather than in the analytical form. The modeling of transitions between possible system modes requires the following assumptions:

- If $x_t \in V_j$, then it can be anywhere within V_j at time t with equal probability. In other words the density function $p_{\theta_t,x_t}(\theta, x)$ is uniform over cell V_j at each time step $t = k\tau$, k-integer number and τ-the size of time step.
- The system should not change during a time step $[t, t+\tau]$, but possibly at the end of it.
- The cell boundaries should to be chosen such that

$$\bigcup_{j=1}^{J} V_j = D^c, \quad \bigcup_{j=J+1}^{J+\Gamma} V_j = D \text{ and } V_i \cap V_j = 0 \text{ for } i \neq j.$$

If the probability of change in the system states $\{\theta_t\}$ only depends on the current and future values of the process variables $\{x_s, s \geq t\}$ and the system states $\{\theta_s, s \geq t\}$, and not on the history of system operation, then the process $\{\theta_t, x_t\}$ has the Markov property. The Markov property can be expressed through the Chapman-Kolmogorov equation as

$$\begin{aligned} p_{\theta_w,x_w|\theta_u,x_u}(\theta, x|\eta, y) \quad = \quad & \int dv \sum_{\theta'} \int dx' p_{\theta_w,x_w|\theta_v,x_v}(\theta, x|\theta', x') \qquad (23) \\ & \times p_{\theta_v,x_v|\theta_u,x_u}(\theta', x'|\eta, y),\ 0 \leq u \leq v \leq w \end{aligned}$$

where u, v, w denote the time. Letting $w = t + \tau$, $v = t'$ in equation (23) and integrating over all possible $0 \leq u \leq t$, y and η yields

$$p_{\theta_{t+\tau},x_{t+\tau}}(\theta, x) = \int dt' \sum_{\theta'} \int dx' p_{\theta_{t+\tau},x_{t+\tau}|\theta_{t'},x_{t'}}(\theta, x|\theta', x') \times p_{\theta_{t'},x_{t'}}(\theta', x'). \tag{24}$$

Next, we perform a time discretization and define a new process $\left\{\tilde{\theta}_t, \tilde{x}_t\right\}$ as follows:

$$\begin{aligned} \tilde{\theta}_t(\omega) &\stackrel{\triangle}{=} \theta \quad \text{for } \{\omega : \theta_{k\tau}(\omega) = \theta\},\ t \in [k\tau, (k+1)\tau),\ k = 0, 1, \ldots, K \\ \tilde{x}_t(\omega) &\stackrel{\triangle}{=} j \quad \text{for } \{\omega : x_t(\omega) \in V_j\},\ t \in [k\tau, (k+1)\tau),\ k = 0, 1, \ldots, K \end{aligned}$$

We regard the process $\left\{\tilde{\theta}_t, \tilde{x}_t\right\}$ as an approximation to process $\{\theta_t, x_t\}$. Then, taking in account the assumptions stated above, equation (24) yields the forward Kolmogorov equation for the Markov chain $\left\{\tilde{\theta}_t, \tilde{x}_t\right\}$:

$$p_{\tilde{\theta}_{(k+1)\tau},\tilde{x}_{(k+1)\tau}}(\theta, j) = \sum_{\eta=1}^{N} \sum_{i=1}^{J+\Gamma} \lambda_{\eta i,\theta j}(k\tau) p_{\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(\eta, i) \tag{25}$$

where $\lambda_{\eta i,\theta j}(k\tau)$ are the elements of transition matrix and $p_{\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(\theta, j) = P(\omega : \theta_{k\tau}(\omega) = \theta, x_{k\tau}(\omega) \in V_j)$ is the probability at time $t = k\tau$ of being in state θ with process variables in cell V_j. The elements of transition matrix can be found from

$$\begin{aligned} \lambda_{\eta i,\theta j}(k\tau) &= g_{\tilde{x}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(j|\eta, i) \\ &\quad \times h_{\tilde{\theta}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau},\tilde{x}_{(k+1)\tau}}(\theta|\eta, i, j) \end{aligned} \tag{26}$$

where[3]

$$g_{\tilde{x}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(j|\eta, i) = \begin{cases} \frac{1}{m(V_i)} \int_{V_i} e_j(\bar{g}(\eta, x', \tau)) dx' \text{ if } V_i \subset D^c \\ \\ 1 \text{ if } i = j = J+1, \ldots, J+\Gamma \\ \\ 0 \text{ if } i = J+1, \ldots, J+\Gamma \\ \quad \text{and } j \neq J+1, \ldots, J+\Gamma \end{cases} \tag{27}$$

with

$$e_j(x) = \begin{cases} 1 & \text{if } x \in V_j \\ \\ 0 & \text{if } x \notin V_j \end{cases} \tag{28}$$

[3] $m(V_j)$ in formula (27) denotes the volume of cell V_j

denotes the conditional probability that $x_{(k+1)\tau} \in V_j$, given that $x_{k\tau} \in V_i$ and $\theta_{k\tau} = \eta$, and $h_{\tilde{\theta}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau},\tilde{x}_{(k+1)\tau}}(\theta|\eta,i,j)$ denotes the conditional probability of being in state θ at time $(k+1)\tau$, given that $\theta_{k\tau} = \eta$, $x_{k\tau} \in V_i$ and $x_{(k+1)\tau} \in V_j$. The integral in (27) determines the portion of the cell V_i that leads to cell V_j.

In practice, the construction of the transition matrix

$$G(j,\tau) = (g_{\tilde{x}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(j|\eta,i))$$

is not performed by using equation (27). The integral appearing in the expression of $g_{\tilde{x}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(j|\eta,i)$ is approximated in the following way: the cell V_i is divided into S_i equal-volume subcells; the evolution of the system is calculated on the time interval τ from the center of each subcell; if $\bar{S}_i$ of these trajectories end up in cell V_j, $g_{\tilde{x}_{(k+1)\tau}|\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(j|\eta,i)$ is taken equal to the ratio $\bar{S}_i/S_i$.

The discrete Markov chain so constructed is then given by:

$$\bar{\pi}(k\tau) = \bar{Q}\bar{\pi}((k-1)\tau) = \bar{Q}^k(\bar{\pi}(0)) \tag{29}$$

where $\bar{\pi} = (p_{\tilde{\theta}_{k\tau},\tilde{x}_{k\tau}}(\theta,j))$ and $\bar{Q} = (\lambda_{\eta i,\theta j}(k\tau))$.

The strength of this approach for treating PCSs is that it allows the use of efficient computational techniques available in Markov chain theory. One of the useful characteristics is that it calculates results for rare event sequences as easily as it does for likely event sequences. An important weakness of this approach is that the dimension of system is strongly limited due to the size of the transition matrix that has to be handled and stored. The number of cells defining the partitioning of the safety domain can be reduced, but this will cause the decrease of accuracy. The number of process variable can hardly exceed 3 or 4. Several methods ([Hass90] and [Belh96]) were proposed to improve on the size limitations. For example, some computational improvements can be achieved through a vectorization of the method and use of a sparse matrix techniques [Belh96]. But even these improvements do not solve the dimensionality problem. The number of process variables remains a major limitation of the CCMT. Another weakness concerns the choice of mapping time step τ and the partitioning of the space $\mathbb{R}^n$ into cells. The mapping time step and the cells are not completely independent of each other. This dependency between time and state-space discretization require several trials with different discretization schemes to achieve the suitable results.

4.2 Discretization of the space variables

The continuous cell-to-cell mapping technique (CCCMT) was proposed as an alternative to CCMT [Tomb96a], [Tomb96b]. This approach, as well as the previous one, assumes that a physical system, described by n variables, can evolve according to N different modes of the dynamics:

$$\begin{aligned} \frac{dx_t}{dt} &= a(\theta_t, x_t), . \\ p_{\theta_{t+\delta}|\theta_t,x_t}(\theta|\eta, x) &= \lambda_{\eta\theta}(x)\delta + o(\delta),\ \eta \neq \theta \end{aligned}$$

here $\{\theta_t, x_t\} \in \mathbb{M} \times \mathbb{R}^n$.

In what follows we will briefly describe the CCCMT approach [Tomb96a].

Given that the density function $p_{\theta_t,x_t}(\theta, x)$ is sufficiently smooth, then it can be characterized by the following integro-partial differential equation [DevSmi94]:

$$\frac{dp_{\theta_t,x_t}(\theta, x)}{dt} = -\sum_{k=1}^{n} \frac{\partial(a_k(\theta, x)p_{\theta_t,x_t}(\theta, x))}{\partial x_k} + \sum_{\eta\in\mathbb{M}} \lambda_{\eta\theta}(x)p_{\theta_t,x_t}(\eta, x) \qquad (30)$$

where $\lambda_{\eta\theta}(x) \geq 0$ $(\eta \neq \theta)$ is the conditional rate at which the process $\{\theta_t\}$ switches from state η to state θ given $x_t = x$. For $\eta = \theta$ we define

$$\lambda_{\theta\theta}(x) \stackrel{\triangle}{=} -\sum_{\eta\in\mathbb{M},\eta\neq\theta} \lambda_{\theta\eta}(x).$$

One can also consider the case when the transition rates $\lambda_{\eta\theta}(x)$ depend on the control laws [Tomb96a].

Now, we again divide the state-space region into cells V_j $(j = 1, \ldots, J + \Gamma)$ as in the previous section. Note that $p_{\theta_t,x_t}(\theta, x \in V_j) = \int_{V_j} p_{\theta_t,x_t}(\theta, x)dx$ is the probability at time t that the process variables are in the cell V_j and the system is in state θ. Then, by integrating equation (30) on a cell V_j, we obtain, using Stokes theorem:

$$\begin{aligned} \frac{dp_{\theta_t,x_t}(\theta, x \in V_j)}{dt} &= -\oint_{S_j} \hat{n}(x_s) \cdot a(\theta, x_s)p_{\theta_t,x_t}(\theta, x_s)dx_s \qquad (31) \\ &\quad + \int_{V_j} \sum_{\eta} \lambda_{\eta\theta}p_{\theta_t,x_t}(\eta, x')dx' \end{aligned}$$

where S_j denotes the surface of V_j, x_s is a point on this surface and $\hat{n}(x_s)$ denotes the outward normal to S_j at x_s. The surface integral in equation (31) can be written as

$$\oint_{S_j} \hat{n}(x_s) \cdot a(\theta, x_s) p_{\theta_t, x_t}(\theta, x_s) dx_s \quad = \tag{32}$$

$$\int\limits_{\substack{\hat{n}(x_s)\cdot a(\theta,x_s)>0 \\ x_s \in S_j}} \hat{n}(x_s) \cdot a(\theta, x_s) p_{\theta_t, x_t}(\theta, x_s) dx_s$$

$$+ \int\limits_{\substack{\hat{n}(x_s)\cdot a(\theta,x_s)<0 \\ x_s \in S_j}} \hat{n}(x_s) \cdot a(\theta, x_s) p_{\theta_t, x_t}(\theta, x_s) dx_s.$$

Assuming again that $\{\theta_t, x_t\}$ is uniformly distributed on each cell, we can write, i.e.

$$p_{\theta_t, x_t}(\theta, x) = \frac{p_{\theta_t, x_t}(\theta, x \in V_j)}{m(V_j)} \text{ for all } x \in V_j,$$

and therefore equations (30-32) yield, taking x_s in the cell from which the probability comes

$$\begin{aligned} \frac{dp_{\theta_t, x_t}(\theta, x \in V_j)}{dt} &= \sum_{\eta, i} L_{\eta i, \theta j} p_{\theta_t, x_t}(\eta, x \in V_i) \qquad (33) \\ &= \sum_{\eta} L^c_{\eta, \theta}(j) p_{\theta_t, x_t}(\eta, x \in V_j) + \sum_i L^{\varphi}_{i,j}(\theta) p_{\theta_t, x_t}(\theta, x \in V_i) \end{aligned}$$

where $L_{\eta i, \theta j}$ are the coefficients of the transition matrix of the whole system,

$$L^c_{\eta, \theta}(j) \triangleq \frac{1}{m(V_j)} \int_{V_j} \lambda_{\eta\theta}(x) dx$$

is the average value of $\lambda_{\eta\theta}(x)$ over the cell V_j, and

$$L^{\varphi}_{i,j}(\theta) \triangleq \begin{cases} -\frac{1}{m(V_j)} \int\limits_{\substack{\hat{n}(x_s)\cdot a(\theta,x_s)>0 \\ x_s \in S_j}} \hat{n}(x_s) \cdot a(\theta, x_s) p_{\theta_t, x_t}(\theta, x_s) dx_s & \text{if } i = j \\ \frac{1}{m(V_j)} \int\limits_{\substack{\hat{n}(x_s)\cdot a(\theta,x_s)>0 \\ x_s \in S_j \cap \bar{S}_i}} \hat{n}(x_s) \cdot a(\theta, x_s) p_{\theta_t, x_t}(\theta, x_s) dx_s & \text{if } i \neq j \end{cases}$$

are the coefficients of the transition matrix associated with the discretized physical variables.

The differential equation (33) is usually a stiff equation and it may take long to solve this to obtain results with a given accuracy. Tombey and Aldemir [Tomb97] have investigated the computational efficiency of CCCMT depending on a various integration schemes.

The CCCMT differs from the previous CCMT in that it leads to set of ordinary differential equations that yield the probability density in continuous

time of the system being in a given cell. Although a time step still needs to be chosen for the integration of the differential equations, the choice of this time step is independent of the state-space discretization used. This allows the use of an integration scheme with variable step size. The main advantages of the CCCMT are: substantial reduction in computer memory requirements, the failure rate data can be used as is without the need to convert the data to failure probabilities during $k\tau < t \leq (k+1)\tau$ under the assumption that the components maintain their states during this interval, and finally, one does not have to conduct the experimentations with the time and space discretization schemes to assure the validity of the results.

4.3 Discrete dynamic event trees

Discrete dynamic event tree (DDET) approach is a discretization technique where only the time variable is discretized. At this time there exist different versions of DDET approach ([Amen84], [Rein87], [Coja93], [AcoSiu93] and [SiuAco90]), but all have the following common features. They track possible branching in modelled system at specified time intervals following an initiating event through simulations. The simulations stop when a specified number of time intervals or a Top Event is reached. The sum of event sequence probabilities leading to a Top Event gives the probability that this Top Event will occur during the specified time interval. In what follows we discuss the principal steps and features of the DDET analysis procedure.

To start with, one should construct a physical model for the system. The physical model should predict the response of system process variables to changes in system component status (e.g. hardware failures). It is constructed by linking physical models for system components, where the component models predict the change in process variables due to changes in component states. For example, the system contains m different components. Among these, for example, may be Valve, Pump-1, Pump-2, ... and so on. Suppose, each j-th component may be in h_j $(j = 1, 2 \ldots, m)$ states. Thus, the whole system can be in one of the $N = h_1 \times h_2 \times \cdots \times h_m$ modes. We can number them from 1 to N and denote by $\mathbb{M} = \{1, 2, \ldots, N\}$ the set of all possible modes. Then, the system dynamics is usually described by the following system of equations (A.3.1):

$$\frac{dx_t}{dt} = a(\theta_t, x_t), \tag{34}$$

$$p_{\theta_{t+\delta}|\theta_t, x_t}(\theta|\eta, x) = \lambda_{\eta\theta}(x)\delta + o(\delta), \ \eta \neq \theta, \tag{35}$$

where $\{\theta_t, x_t\} \in \mathbb{M} \times \mathbb{R}^n$.

The next step is to define the undesired system states. These are defined in terms of process variable levels, rather than system (hardware) modes, and are used to determine when a particular accident sequence simulation should be terminated. Finally, one should define the probability parameters characterizing states and possible state transitions. These are defined through the equation (35).

Next, we perform the time discretization and define a new process $\left\{\bar{\theta}_t, \bar{x}_t\right\}$ through the following system of equations:

$$\frac{d\bar{x}_t}{dt} = a(\bar{\theta}_t, \bar{x}_t), \tag{36}$$

$$p_{\bar{\theta}_{(k+1)\Delta t}|\bar{\theta}_{k\Delta t},\bar{x}_{k\Delta t}}(\theta|\eta, x) = \lambda_{\eta\theta}(x)\Delta t,\ \eta \neq \theta,\ k = 1, 2, \ldots. \tag{37}$$

After the system model is defined, we use it to simulate all possible accident sequences. Starting at time $t = 0$ and some known initial state (θ^0, x^0), the system model is used to determine the change in process variable levels in the next Δt. The time step Δt is fixed and therefore transitions (branching) either on demand or stochastic may happen only at discrete times $k \cdot \Delta t$, $k = 1, 2, \ldots$. Between these transitions the dynamics of the system is described by the system of ODEs (36). The time step Δt must be adequate to the time constants of the system under consideration. Moreover, it must be less than the minimum mean life-time of each state of the system. At the end of the first time interval $[0, \Delta t]$, all possible combinations of system component states are identified and their likelihood calculated. These states are then used to provide boundary conditions for the next round of process variable updating. The generation of an event sequence continues in this manner until an absorbing state or the final time of analysis T_{MAX} is reached. Then, the sum of event sequence probabilities leading to a top event gives the probability that this top event will occur during the specified time interval. Actually, this probability is only an approximation of the true collision probability $P_{coll}(0, T_{MAX})$ defined in section (2.4).

In order to practically apply DDET to realistic problems, rules for limiting the event tree expansion are introduced. The probability of simultaneous multiple failures (switches) of components is assumed to be zero when these events are independent of each other. Sequences with probability falling under a predefined threshold (P_{lim}) are discarded. Absorbing conditions are defined: when the system reaches a particular state, further branching is not considered for that sequence.

Let us consider very simple example to illustrate the DDET approach. Suppose a system contains two components: 1st component - C_1 and 2nd component - C_2. Assume that each of these two components may be in two different states: *on* or *off*. Thus, the whole system may be in 4 different modes:

$$\begin{aligned}
\theta^1 &= \{C_1 \text{ on}, C_2 \text{ on}\},\\
\theta^2 &= \{C_1 \text{ on}, C_2 \text{ off}\},\\
\theta^3 &= \{C_1 \text{ off}, C_2 \text{ on}\},\\
\theta^4 &= \{C_1 \text{ off}, C_2 \text{ off}\}.
\end{aligned}$$

The system dynamics is described by system of ODEs (36). The system modes (their transition probabilities) are characterized by equation (37). We

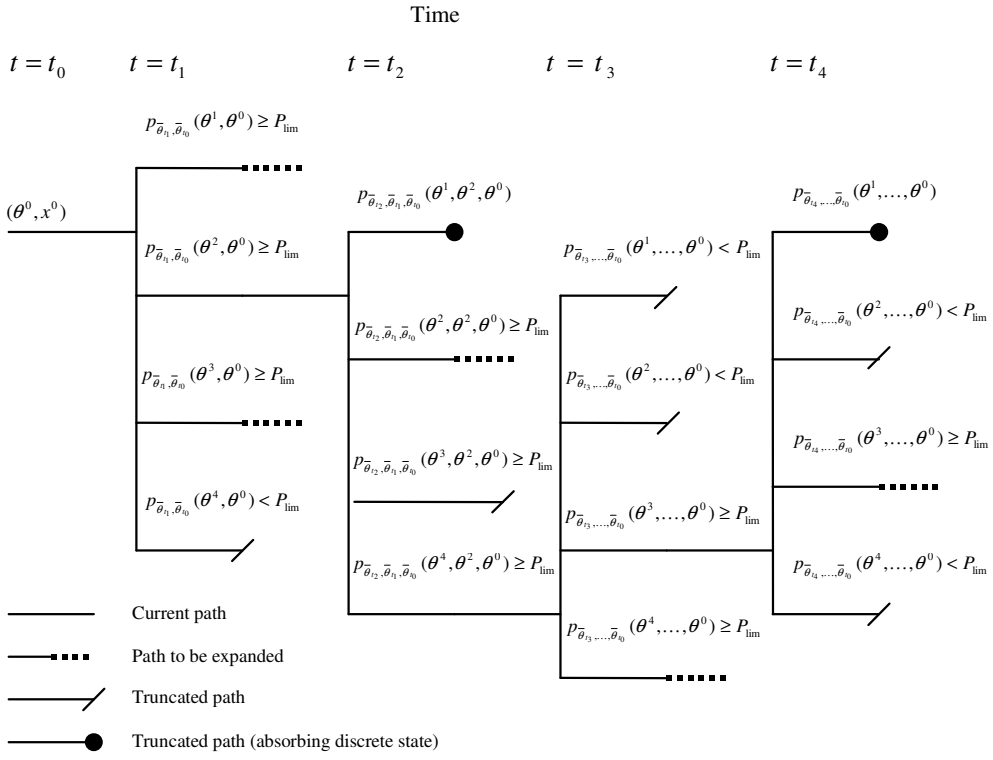

Figure 1: Example application of DDET

assume that the probability of multiple switches of system components is zero. Thus the following transition probabilities are defined to be equal to zero:

$$\begin{aligned} p_{\bar{\theta}_t|\bar{\theta}_u,\bar{x}_u}(\theta^1|\theta^4, x^{4,u}) &= 0, \\ p_{\bar{\theta}_t|\bar{\theta}_u,\bar{x}_u}(\theta^4|\theta^1, x^{1,u}) &= 0, \\ p_{\bar{\theta}_t|\bar{\theta}_u,\bar{x}_u}(\theta^2|\theta^3, x^{3,u}) &= 0, \\ p_{\bar{\theta}_t|\bar{\theta}_u,\bar{x}_u}(\theta^3|\theta^2, x^{2,u}) &= 0. \end{aligned}$$

The top events are defined in terms of process variable x levels. Figure 1 illustrates the logical branching in an application of DDET to our example.

The probability of a particular event sequence is obtained using the following

iterative formula:

$$\begin{aligned} & p_{\bar{\theta}_{t_k},\bar{\theta}_{t_{k-1}},\ldots,\bar{\theta}_0}(\theta^{i_k},\theta^{i_{k-1}},\ldots,\theta^0) \\ & \quad = p_{\bar{\theta}_{t_{k-1}},\ldots,\bar{\theta}_0}(\theta^{i_{k-1}},\ldots,\theta^0)\, p_{\bar{\theta}_{t_k}|\bar{\theta}_{t_{k-1}},\bar{x}_{t_{k-1}}}(\theta^{i_k}|\theta^{i_{k-1}},x^{i_{k-1}}) \\ & \quad = p_{\bar{\theta}_{t_k}|\bar{\theta}_{t_{k-1}},\bar{x}_{t_{k-1}}}(\theta^{i_k}|\theta^{i_{k-1}},x^{i_{k-1}}) \times \cdots \times p_{\bar{\theta}_{t_1}|\bar{\theta}_{t_0},\bar{x}_{t_0}}(\theta^{i_1}|\theta^0,x^0) \end{aligned}$$

Suppose after conducting the simulation K event sequences led to a top event R. Then the probability of this top event is

$$P(R) = \sum_{k=1}^{K} P(k)$$

where $P(k)$ denotes the probability of k-th event sequence.

One important drawback of DDET is that it is limited to the treatment of accidents where the number of different possible scenarios is relatively small. In cases where the characteristic time scale of important dynamic process is small compared with the duration of the accident scenario, a small Δt must be used and the number of possible scenarios increases geometrically. Thus, the scenario calculations have the potential to be long and costly, this is generally because of treatment of process x dynamics, as well as the potentially large number of scenarios to be treated.

The latest development of DDET [Coja93] allows to takes into account different kinds of probabilistic behaviors. Each component of the system can be characterized by one of six different probabilistic options, namely:

1. *constant probabilities* - each functioning or failed state of the component is characterized by a constant probability value

2. *stochastic transitions* - each component state may change in time according to transition rates between states which are constant

3. *functional dependent transitions* - each component state may change in time according to transition probabilities between the states which depend on the value attained by certain process physical variables, properly discretized. This option treats failures (transitions) on demand and physical dependencies

4. *stochastic and functional dependent transitions* - this is a combination of points 2 and 3, i.e., the component states are subject both to stochastic transitions and to transitions due to effects of process physical variables

5. *conditional probabilities* - for static dependencies among states of different components. This is a generalization of option 1

6. *stochastic transitions with variable transition rates* - in this case the component undergoes stochastic transitions, as in case 2, but the transition rates are not considered constant. The transition rates can be a function of any process variable, properly discretized. The case of time dependent transition rates can also be handled by this option.

One can extend the above approach by including the operator state variables, such as *operator diagnosis* state, *operator quality* state, and *operator planning* state ([AcoSiu93], [SiuAco90]). These states have great impact on generation of branching points. This reduces the role of the process variable x in the branching operations. In the case of highly automated systems (no human interaction), new approach would provide the same dynamic risk analysis as the previous one would (see Figure 1).

Another advantage of the approach proposed in [AcoSiu93] and [SiuAco90] is that the user is free to define the basis for branching and the number of branches at any time step.

4.4 Interpolation of a density function

Let us consider the situation where system evolution is described by continuous valued process $\{x_t\} \in \mathbb{R}^n$. For example, suppose that process $\{x_t\}$ is governed by equation of type **A.2.1**, i.e.

$$\frac{dx_t}{dt} = a(x_t),$$

here we assume that the initial value x_0 is a random variable. Assuming the existence, continuity and differentiability of a density function $p_{x_t}(x)$ we can write the partial differential equation describing its evolution in time.

$$\frac{d}{dt}p_{x_t}(x) = -\sum_{k=1}^{n} \frac{\partial(a_k(x)p_{x_t}(x))}{\partial x_k}.$$

In what follows we will outline a semi-analytic approach for the estimation of a multivariate density developed by P.E. Labeau and J. Devought [LabDev95]. The estimation is based on the moments of the process and densities of its components. Calculation of the moments is discussed in [DevLab95].

Let us presume that the support of density $p_{x_t}(x)$ is finite. Next, we assumed that we know n densities $p_{x_{k,t}}(x_k)$, $k = 1 \ldots n$. The objective is to find an interpolated density $\hat{p}_{x_t}(x)$, preserving the relation (4) and conserving as many moments as possible. The idea is similar to usual function interpolation when only finite number of function values are known. But in this case we have some restrictions: the interpolated function must be again a density function and possess all properties of density functions. This requires a special interpolation scheme.

Using the techniques of Gordon's projections [LabDev95] the aim is to work with the following interpolation formula:

$$\begin{aligned}\hat{p}_{x_t}(x) &= \sum_{i=1}^{n} p_{x_{i,t}}(x_i) \prod_{k\neq i} g_{x_{k,t}}(x_k) - (n-1) \prod_{j=1}^{n} g_{x_{j,t}}(x_j) \\ &\quad - \sum_{i=1}^{n} \sum_{j\neq i} d_{ij} (p_{x_{i,t}}(x_i) - g_{x_{i,t}}(x_i)) \\ &\quad \times (p_{x_{j,t}}(x_j) - g_{x_{j,t}}(x_j)) \prod_{k\neq i,j} g_{x_{k,t}}(x_k)\end{aligned} \tag{38}$$

where d_{ij} some coefficients and $g_{x_{k,t}}(\cdot)$ are some auxiliary functions satisfying the relation $\int g_{x_{k,t}}(x_k) = 1$. Because of this we call them auxiliary densities. It seems quite logical to take auxiliary densities with the same support as the densities $p_{x_{k,t}}(x_k)$ have. The most well-known example of density with a bounded support is the density of β distribution. The auxiliary densities $g_{x_{k,t}}(x_k)$ and coefficients d_{ij} should be chosen in a special way in order to preserve the covariances of process $\{x_t\}$. Hence define the different moments of the distribution:

$$\begin{aligned}\mu(m_1 \dots m_n) &= \int x_{1,t}^{m_1} \dots x_{n,t}^{m_n} p_{x_t}(x) dx \\ \mu_k(l) &= \int x_k^l p_{x_{k,t}}(x_k) dx_k,\ \mu_k(0) = 1,\ k = 1 \dots n \\ \nu_k(l) &= \int x_k^l g_{x_{k,t}}(x_k) dx_k,\ \nu_k(0) = 1,\ k = 1 \dots n.\end{aligned}$$

For simplicity we also define

$$\mu_{ij} = \mu(0 \dots m_i \dots 0 \dots m_j \dots 0)|_{m_i=1; m_j=1}.$$

One can check that equation (38) preserves the relation (4) (i.e. $p_{x_{k,t}}(x_k) = \int \hat{p}_{x_t}(x) dx_1 \dots dx_{k-1} dx_{k+1} \dots dx_n$) and conserves all the moments of one variable (i.e. $\mu_k(l) = \int x_k^l \hat{p}_{x_{k,t}}(x_k) dx_k$, $\mu_k(0) = 1$, $k = 1 \dots n$). In order to insure the conservation of the covariances, and similarly all the moments of two variables, the following equation should be satisfied.

$$\begin{aligned}\mu_{lm} &= \mu_l(1)\nu_m(1) + \mu_m(1)\nu_l(1) - v_l(1)\nu_m(1) \\ &\quad -(d_{lm} + d_{ml}) \left[\nu_l(1)\nu_m(1) - \mu_l(1)\nu_m(1) - \mu_m(1)\nu_l(1) + \mu_l(1)\mu_m(1)\right].\end{aligned} \tag{39}$$

Because of the symmetry of the coefficients d_{ij} (see [LabDev95]) we have $\frac{n(n-1)}{2}$ to be determined coefficients added to the n arbitrary auxiliary moments $v_i(1)$, while we have at our disposal $\frac{n(n-1)}{2}$ relations of the form (39). It is thus possible to find a solution to this problem.

Next let us assume that a physical system, described by n variables $x \in \mathbb{R}^n$, can evolve according to N different modes of the dynamics (**A.3.1**):

$$\begin{aligned} \frac{dx_t}{dt} &= a(\theta_t, x_t), \\ p_{\theta_{t+\delta}|\theta_t,x_t}(\theta|\eta, x) &= \lambda_{\eta\theta}(x)\delta + o(\delta),\ \eta \neq \theta, \end{aligned}$$

here $\{\theta_t, x_t\} \in \mathbb{M} \times \mathbb{R}^n$. The probability density $p_{\theta_t,x_t}(\theta, x)$ that the system is at time t in state (θ, x), for a given initial conditions, obeys the following integro-partial differential equation:

$$\begin{aligned} \frac{d}{dt}p_{\theta_t,x_t}(\theta, x) &= -\sum_{i=1}^{n} \frac{\partial(a_i(\theta, x)f(\theta, x))}{\partial x_i} + \sum_{\eta\in\mathbb{M},\ \eta\neq\theta} [\lambda_{\eta\theta}(x)p_{\theta_t,x_t}(\eta, x) \\ &\quad -\lambda_{\theta\eta}(x)p_{\theta_t,x_t}(\theta, x)]\,. \end{aligned} \tag{40}$$

One can slightly modify equation (38) in order to adopt the above interpolation scheme to $\hat{p}_{\theta_t,x_t}(\theta, x)$:

$$\begin{aligned} p_{\theta_t}(\theta) \cdot \hat{p}_{\theta_t,x_t}(\theta, x) = p_{\theta_t}(\theta) &\sum_{k=1}^{n} p_{\theta_t,x_{k,t}}(\theta, x_k)(1 + 2\sum_{l\neq k} d_{kl}^{\theta}) \prod_{m\neq k} g_{\theta_t,x_{m,t}}(\theta, x_m) \\ - p_{\theta_t,x_t}(\theta, x)^2 &(n - 1 + \sum_{k=1}^{n}\sum_{l\neq k} d_{kl}^{\theta}) \prod_{m=1}^{n} g_{\theta_t,x_{m,t}}(\theta, x_m) \\ - \sum_{k=1}^{n}\sum_{l\neq k} d_{kl}^{\theta} p_{\theta_t,x_{k,t}}(\theta, x_k)&p_{\theta_t,x_l}(\theta, x_l) \prod_{m\neq k,l} g_{\theta_t,x_{m,t}}(\theta, x_m), \end{aligned} \tag{4.21}$$

$\theta = 1, \ldots N$.

Additionally, using this interpolation scheme imposes restrictions on the form of the dynamics and of the transitions rates of process $\{\theta_t\}$. [DevLab95] choice is limited to a quadratic dynamics in the physical variables :

$$a_k(\theta, x) = \sum_{l=1}^{n}\sum_{m=1}^{n} (a_o)_{klm}^{\theta} x_l x_m + \sum_{m=1}^{n} (a_1)_{km}^{\theta} x_m + (a_2)_k^{\theta},\ \theta = 1 \ldots N,\ k = 1 \ldots n \tag{42}$$

and linear transition rates:

$$\lambda_{\theta\theta}(t, x) = \sum_{m=1}^{n} c_m^{\theta} x_m + d^{\theta},\ \theta = 1 \ldots N \tag{43}$$

$$\lambda_{\eta\theta}(t, x) = \sum_{m=1}^{n} h_m^{\theta,\eta} x_m + g^{\theta,\eta},\ \theta \neq \eta = 1 \ldots N \tag{44}$$

where $\lambda_{\theta\theta}(t,x)$ is the total transition rate out of state θ, given x, and $q_{\eta\theta}(t,x)$ is the transition rate between configurations η and θ, given x, such that

$$q_{\theta\theta}(t,x) = -\sum_{\eta\in\mathbb{M},\ \eta\neq\theta} q_{\theta\eta}(t,x).$$

Since the interpolation (4.21) conserve the relation (4), one can find the equation of evolution of density functions $p_{\theta_t,x_{k,t}}(\theta,x_k)$, $k=1\dots n$, by replacing $p_{\theta_t,x_t}(\theta,x)$ in equation (40) by its value in equation (4.21) and by integrating the result over all variables except one. P.E. Labeau and J. Devought [LabDev95] have obtained n systems of N one-dimensional hyperbolic PDEs for the densities $p_{\theta_t,x_{k,t}}(\theta,x_k)$, $k=1\dots n$ in place of a system of N n-dimensional PDEs for the total distributions.

$$\begin{aligned}
&\frac{dp_{\theta_t,x_{m,t}}(\theta,x_m)}{dt} + A^\theta_m(x_m,t)\frac{\partial p_{\theta_t,x_{m,t}}(\theta,x_m)}{\partial x_m} + C^\theta_m(x_m,t)p_{\theta_t,x_{m,t}}(\theta,x_m)\\
&\quad + D^\theta_m(t)g_{\theta_t,x_{m,t}}(\theta,x_m)p_{\theta_t}(\theta) + E^\theta_m(x_m,t)\frac{\partial g_{\theta_t,x_{m,t}}(\theta,x_m)}{\partial x_m}p_{\theta_t}(\theta) \quad (45)\\
&\quad = \sum_{\eta\neq\theta}\left[F^{\eta,\theta}_m(x_m,t)p_{\theta_t,x_{m,t}}(\eta,x_m) + G^{\eta,\theta}_m(t)g_{\theta_t,x_{m,t}}(\eta,x_m)p_{\theta_t}(\eta)\right]
\end{aligned}$$

$\theta=1,\dots,N$, $m=1,\dots,n$.
The different coefficients defined in the previous expression depend only on the coefficients of equations (42),(43) and (44), and on the moments $\mu_k(\theta,t)$ and covariances $\sigma_{kl}(\theta,t)$:

$$\begin{aligned}
p_{\theta_t}(\theta) &= \int p_{\theta_t,x_t}(\theta,x)dx\\
p_{\theta_t}(\theta)\mu_k(\theta,t) &= \int x_k p_{\theta_t,x_t}(\theta,x)dx\\
p_{\theta_t}(\theta)\sigma_{kl}(\theta,t) &= \int (x_k-\mu_k(\theta,t))(x_l-\mu_l(\theta,t))p_{\theta_t,x_t}(\theta,x)dx.
\end{aligned}$$

(see [LabDev95] for more details.) For explanation how to calculate these moments and covariances see [DevLab95].

Remark 3 *Let us note that in case when the system always evolves only in one state*[4] *θ, then the evolution of the density functions $p_{x_{k,t}}(x_k)$, $k=1\dots n$, is described by equation (45) where $\theta=1$, $m=1,\dots,n$. In this case we have only one one-dimensional hyperbolic PDE.*

[4] i.e. if we deal with processes $\{x_t\}$ of type A.2.1 ($|\mathbb{M}|=1$), our first considered case in this section

The obtained hyperbolic PDEs can be solved by a Lie algebraic method [Wein63]. This method performs analytically the integration of the x variable, bringing the calculation of the densities $p_{\theta_t,x_{k,t}}(\theta, x_k)$ back to one or two time quadratures. This considerably reduces the numerical workload. Once the moments and densities $p_{\theta_t,x_{k,t}}(\theta, x_k)$ are evaluated, the density function $p_{\theta_t,x_t}(\theta, x)$ can be approximately found by the interpolation formula.

The various benchmarks presented in [LabDev95] show a good accuracy for the densities $p_{\theta_t,x_{k,t}}(\theta, x_k)$. Unfortunately, the interpolated density $\hat{p}_{\theta_t,x_t}(\theta, x)$ is a crude approximation of the real one, depending mainly on how the hyper-rectangular interpolation region fits the real support of the density. This rough approximation of the solution can be used to improve variance reduction techniques of a Monte Carlo method. [Labeau95] have investigated how an a priori knowledge of the support of the density could be used to improve the above interpolation scheme.

5 Monte Carlo simulation

In this chapter we will discuss the application of Monte Carlo (MC) techniques to risk assessment, following [Kloe92].

The main advantage of MC technique is that it is almost insensitive to the dimensionality of the application. MC performs a direct estimation of risk and reliability characteristics expressed as functionals of the densities $p_{\xi_t}(\xi)$. The explicit calculation of these densities is thus bypassed. Nowadays, MC simulation appears to be the only tool likely to cope with high-dimensional realistic problems. However, it suffers from several drawbacks. Since we aim at estimating the risk of very rare events, the MC simulation may be too time-consuming or inaccurate. To overcome this problem different efficient MC techniques have been developed: variance reduction techniques, biased schemes, the acceleration of the integration of the equations of the dynamics etc. In what follows we will review the standard MC and efficient MC algorithms for estimation of rare events.

5.1 Standard Monte Carlo

First, let us consider the situation when the system dynamics is modelled by the following SDE (A.2.2):

$$dx_t = a(x_t)dt + b(x_t)dw_t \tag{46}$$

where $\{x_t\} \in \mathbb{R}^n$, $t \in [0, T]$. Assume that we are interested in the evaluation of functionals of the form

$$Eg(x_T), \tag{47}$$

where g is a given function. If one were able to solve (46) explicitly, the evaluation of (47) would be an easy task. Unfortunately, very few specific SDE's have explicitly known solutions. The well known exceptions are linear Gaussian SDE's.

A widely applicable approach to evaluating functionals like (47) is the simulation of sample paths of time discrete approximations. This is based on a finite discretization of the time interval $[0, T]$ under consideration and generates approximate value of the sample paths step by step at the discretization times. The simulated sample paths can then be analyzed by usual statistical methods to determine how good the approximation is and in what sense it is close to the exact solution. See [Kloe92] for further discussions on this topic.

For a given discretization $0 = \tau_0 < \tau_1 < \cdots < \tau_L = T$ of the time interval $[0, T]$ we should choose an appropriate approximation $\left\{x_t^h\right\}$ to the process $\{x_t\}$. For simplicity one can choose the simplest explicit Euler approximation. This is a discrete time stochastic process $\{x_t^h\} = \left\{x_t^h,\ 0 \le t \le T\right\}$ satisfying the iterative scheme

$$x^h_{\tau_{n+1}} = x^h_{\tau_n} + a(x^h_{\tau_n})(\tau_{n+1} - \tau_n) + b(x^h_{\tau_n})(w_{\tau_{n+1}} - w_{\tau_n}), \tag{48}$$

for $n = 0, 1, \ldots, L-1$ with initial value

$$x^h_0 = x_0.$$

Then, we evaluate (47) with the functional

$$Eg(x^h_{\tau_L})$$

using the estimator

$$\frac{1}{N_h} \sum_{r=1}^{N_h} g(x^h_{\tau_L}(\omega_r)), \tag{49}$$

which is just the arithmetic mean of N_h independent simulations of the random variable $g(x^h_{\tau_L})$. Here $x^h_{\tau_L}$ denotes the rth simulation of $\{x^h_t\}$ at time $\tau_L = T$.

So, in order to find an approximation of the functional $Eg(x_T)$, the following algorithm can be used:

1. Sample the initial state x_0 from the initial distribution $p_{x_0}(x)$.
2. Generate the random independent increments $\Delta w_{\tau_n} = w_{\tau_{n+1}} - w_{\tau_n}$, $(n = 0, 1, \ldots, L-1)$ of the Wiener process $\{w_t\}$.
3. Compute the value of $\{x^h_{\tau_n}\}$ at time $\tau_L = T$ using the recurrence formula (48).
4. Repeat steps 1-3 N_h times.

Note that if we use an implicit approximation scheme, then, in step 3, we will need to solve an additional algebraic equation at each time step. This may increase the computing time significantly. On the other hand, implicit scheme can improve the stability of approximate solutions considerably. (see [Kloe92])

We can represent the difference of the estimator (49) and the desired functional (47)

$$\hat{\mu} = S_{N_h} - Eg(x_T)$$

by the sum of the systematic error

$$\mu_{sys} = E(\hat{\mu}) = Eg(x^h_T) - Eg(x_T)$$

and the statistical error

$$\mu_{stat} = \hat{\mu} - \mu_{sys}.$$

For a large number N_h of independent simulations the Central Limit Theorem says that the statistical error is asymptotically Gaussian with mean zero and variance

$$Var(\mu_{stat}) = Var(\hat{\mu}) = \frac{1}{N_h} Var(g(x_T^h)). \tag{50}$$

The variance (50) determines the size of the confidence interval for the estimator (49). Hence, in order to obtain sufficiently small confidence intervals we should run a large enough number N_h of independent simulations.

5.2 Variance reduction by measure transformation

In order to reduce the necessary number of independent simulations, several variance reduction approaches have been developed. First we will describe a measure transformation method. In section (5.3) we describe an importance and stratified sampling variance reduction approach.

Suppose $\{x_t\}$ satisfies the SDE (46). Our aim is to approximate the functional (47) in an efficient way by constructing an estimator with the same expectation, but with a smaller variance than estimator (49).

Milstein ([Mils95] or see [Kloe92]) proposed the use of a particular Girsanov transformation to transform the underlying probability measure P so that the process $\{\tilde{w}_t\}$ defined by

$$\tilde{w}_t = w_t - \int_0^t \psi(\tilde{x}_s) ds$$

is a Wiener process with respect to the transformed probability measure $\tilde{P}$ with Radon-Nikodym derivative

$$\frac{d\tilde{P}}{dP} = \Theta_t / \Theta_0.$$

Here the process $\{\tilde{x}_t\}$ satisfies the stochastic equation

$$\tilde{x}_t = x + \int_0^t a(\tilde{x}_s) ds + \int_0^t b(\tilde{x}_s) d\tilde{w}_s$$

and the correction process $\{\Theta_t\}$ satisfies the equation

$$\Theta_t = \Theta_0 + \int_0^t \Theta_s \psi(\tilde{x}_s) dw_s$$

with $\Theta_0 \neq 0$, where ψ denotes given n-dimensional vector function.

Obviously, the process $\{\tilde{x}_t\}$ is an Ito process with respect to measure $\tilde{P}$ with the same drift and diffusion coefficient as the Ito process $\{x_t\}$. Thus, it follows that

$$Eg(x_T) = E(g(\tilde{x}_T)\Theta_T/\Theta_0).$$

Hence, we can estimate the expectation of the random variable

$$g(\tilde{x}_T)\Theta_T/\Theta_0 \tag{51}$$

to evaluate the functional (47). Note that we can choose the function ψ arbitrary, so we can use it as a parameter to reduce the variance of the random variable (51).

Assuming that the functions g, a, and b are sufficiently smooth, one can show (see [Kloe92]) that it is possible to obtain a substantial reduction in the variance of the estimator by choosing the parameter function $\psi = (\psi_1, \psi_2, \ldots, \psi_n)$ of the form

$$\psi_j(t,x) = -\frac{1}{\bar{u}(t,x)} \sum_{k=1}^{n} b_{k,j}(x) \frac{\partial \bar{u}}{\partial x_k}(t,x), \ j = 1, \ldots, n$$

where the function $\bar{u}(s,x)$ is sufficiently close to the solution $u(s,x) = Eg(x_T^{s,x})$[5] of the Kolmogorov backward equation:

$$\frac{\partial u(s,x)}{\partial s} = -\sum_{k=1}^{n} a_k(x) \frac{\partial}{\partial x_k} u(s,x) - \frac{1}{2} \sum_{k,l=1}^{n} \sigma_{kl}(x) \frac{\partial^2}{\partial x_k \partial x_l} u(s,x)$$

where $\sigma_{kl}(x) = \sum_{r=1}^{n} b_{lr}(x) b_{kr}(x)$.

5.3 Variance reduction by importance and stratified sampling

In this section we will consider other variance reducing estimators which are derived using the theory of Monte Carlo integration. The results in this section apply to n-dimensional diffusion processes

$$x_t = x + \int_0^t a(x_s)ds + \int_0^s b(x_s)dw_t$$

with diffusion term $b : \mathbb{R}^n \to \mathbb{R}^{n\times 1}$ and with scalar Wiener process: $\{w_t\} \in \mathbb{R}^1$.

[5] $\{x_t^{s,x}\}$ denotes the process starting at x at time $s \in [0,T)$. Here we should also assume that $u(s,x)$ is strictly positive. The extension to general case is straightforward.

Again, let

$$Eg(x_T) \tag{52}$$

be the quantity of interest. Suppose that we are given a time discretization $0 = \tau_0 < \tau_1 < \cdots < \tau_L = T$ of the time interval $[0, T]$. Using the Markov property and the Chapman-Kolmogorov equation, one can represent the functional (52) in the form

$$Eg(x_T) = \int_{\mathbb{R}^n} \cdots \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} \prod_{i=1}^{L} p_{x_{\tau_i}|x_{\tau_{i-1}}}(x^i|x^{i-1}) g(x^L) p_{x_0}(x^0) dx^1 \dots dx^L, \tag{53}$$

where x^i denotes the value of process $\{x_t\}$ at time $t = \tau_i$ $(i = 0, 1, \dots, L)$.

If we set

$$d\mu(\zeta) = p_{x_0}(x^0) dx^1 \dots dx^L$$

and

$$F(\zeta) = \prod_{i=1}^{L} p_{x_{\tau_i}|x_{\tau_{i-1}}}(x^i|x^{i-1}) g(x^L)$$

where $\zeta = (x^0, \dots, x^L) \in \Gamma \stackrel{\triangle}{=} (\mathbb{R}^n)^{L+1}$, then we can write (53) as the finite-dimensional integral

$$Eg(x_T) = \int_{\Gamma} F(\zeta) d\mu(\zeta). \tag{54}$$

A simple Monte Carlo estimator for this integral is

$$\frac{F(\zeta)}{D(\zeta)}, \tag{55}$$

where ζ is a random variable with density $D(\zeta)$ with respect to measure $d\mu$. If we assume that $D(\zeta) > 0$ for all $\zeta \in \Gamma$ with $g(x^L) \neq 0$, then it follows that

$$E\left(\frac{F(\zeta)}{D(\zeta)}\right) = Eg(x_T).$$

Thus the estimator (55) is unbiased. Note that, in general, function F is not known explicitly. Therefore, we should somehow approximate or estimate the finite-dimensional density of the process $\{x_t\}$

$$Q(x^0, x^1, \dots, x^L) = \prod_{i=1}^{L} p_{x_{\tau_i}|x_{\tau_{i-1}}}(x^i|x^{i-1}) \tag{56}$$

by a similar, but known density. For instance, one could use the density of a weak time discrete approximation of the process $\{x_t\}$, the simplest being the Euler approximation. In this case, we can approximate function Q by the following one

$$\tilde{Q}(\zeta) = \prod_{i=1}^{L} \tilde{p}_{x_{\tau_i}|x_{\tau_{i-1}}}(x^i|x^{i-1})$$

where $\tilde{p}_{x_{\tau_i}|x_{\tau_{i-1}}}(x^i|x^{i-1})$ is the known density for Gaussian increments.

Then we can define the variance reducing *Euler estimator* as

$$\frac{\tilde{Q}(\zeta)}{D(\zeta)} g(x^L) \tag{57}$$

where $\zeta = (x^0, \ldots, x^L) \in \Gamma$ is a random variable with density D with respect to $d\mu$. Here, D is a free parameter, thus an appropriate choice of it provides a means for reducing the variance of the estimator.

It is easy to show that the estimator (55) attains the minimum possible variance, which is zero when g is only positive or only negative, and

$$D(\zeta) = D_{opt}(\zeta) = \frac{Q(\zeta)\left|g(x^L)\right|}{E(|g(x_T)|)}.$$

Usually D_{opt} is not known. The method of choosing D close to D_{opt} in the estimator (55) is known as *importance sampling* because the density is high in those regions making the most important contributions to the functional.

When g changes sign, we can write it as the sum of its positive and negative parts and apply the above procedure to each part separately. The optimal choice of the corresponding densities D^+ and D^- is then called *stratified sampling*.

5.4 Monte Carlo for systems with switching coefficients

As before, we suppose that the system consists of m components, and each j-th component may be in h_j $(j = 1, 2, \ldots, m)$ states. Then the whole system possesses $N = h_1 \times h_2 \times \cdots \times h_m$ states. The system dynamics is modelled by the following system of equations (A.3.1) [Mars98], [Labeau98]:

$$\frac{dx_t}{dt} = a(\theta_t, x_t), \tag{58}$$

$$p_{\theta_{t+\delta}|\theta_t, x_t}(\theta|\eta, x) = \lambda_{\eta\theta}(x)\delta + o(\delta),\ \eta \neq \theta, \tag{59}$$

where $\{\theta_t, x_t\} \in \mathbb{M} \times \mathbb{R}^n$, $\mathbb{M} = \{1, 2, \ldots, N\}$.

As we already mentioned above, we are interested in evaluation of the functionals of the form

$$E(g(\theta_T, x_T)), \tag{60}$$

where g is a given function.

The functional (60) can be estimated with the help of the following standard MC algorithm:

1. Sample the initial state θ and process variables x from the initial distribution $p_{\theta_0,x_0}(\theta, x)$.
2. Sample the next transition time t out of θ.
3. Compute the evolution of x in state θ up to t; if the end of the accident duration is reached, the current simulation run is stopped.
4. A new state η is sampled.
5. This procedure is repeated from step 2., η being the new value of θ.

The unbiased estimator $\tilde{s}$ of the functional (60) after N_h independent runs of the above MC algorithm is given by:

$$\tilde{s} = \frac{1}{N_h} \sum_{r=1}^{N_h} g(\theta_T(\omega_r), x_T(\omega_r)),$$

which is just the arithmetic mean of N_h independent simulations of the random variable $g(\theta_T(\omega_r), x_T(\omega_r))$. Here $(\theta_T(\omega_r), x_T(\omega_r))$ denotes the rth simulation of $\{\theta_t, x_t\}$ at time T.

However, the above MC algorithm presents two major drawbacks:

1. For a safe system, most simulation runs do not lead to an accident situation, and consequently do not bring any information (score) on the accident risk. Huge numbers of simulation runs are necessary for an acceptable statistical accuracy.
2. This problem of prohibitively long computer times is reinforced by the need to compute the system's dynamic evolution during each simulation run.

6 Conclusions

The aim of this report was to review existing accident risk assessment methods for safety-critical operations. We have analyzed techniques available in literature and tried to ascertain their applicability to ATM. Two main streams of development have been identified: approximate numerical solution of the integro-partial differential equations and Monte Carlo simulation based approaches. Both developments are largely available from physics literature. All the material that has been gathered from literature we present in a stochastic analysis framework. It has turned out that most of the existing literature considers the situation where the dynamic evolution of safety-critical operation is described mainly by hybrid state Markov processes without jump and diffusion terms. The latter terms seem to be necessary in order to achieve a proper model of ATM operations [Blom et al 03].

The accident risk assessment problem usually reduces to the evaluation of the probability-density function of hybrid state Markov process. It is possible to characterize the forward evolution of the density through a particular integro-partial differential equation. In most cases it is not realistic to solve this equation analytically or even numerically. Some approximate numerical techniques are available, these are the discretization, density interpolation and Monte Carlo. The discretization techniques can be divided into three types: the first one is based on simultaneous discretization of time and of the space variables, in second one only the space variable is discretized, and in the third one the time discretization is done. One of the main weakness of the discretization schemes is their applicability to a low dimensional problem only. The interpolation based approach does not provide the sufficient accuracy, i.e. the interpolated density obtained with help of this method is a crude approximation of the real one. But this rough approximation can be used to improve the variance reduction techniques of a Monte Carlo method. One of the most feasible computational approach for large-scale problems is Monte Carlo simulation. Its main advantages are the applicability to any hybrid state Markov process and insensitivity to the dimensionality of the problem. Unfortunately, the Monte Carlo methods suffer from one important drawback - are too time-consuming when applied to assess the risk of rare events. Thus it is important to develop efficient Monte Carlo techniques which could reduce the computation time significantly. Some of them were already described in this report. Further studies will mainly concentrate on development of efficient Monte Carlo methods feasible for more advanced hybrid state processes, e.g. with diffusion, Poisson jumps and boundary hitting.

References

[AcoSiu93] Acosta C, Siu N. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. Reliability Engineering and System Safety 1993;41:135–54.

[Alde87] Aldemir T. Computer-assisted Markov failure modeling of process control systems. IEEE Transactions in Reliability 1987;R-36:133–44.

[Alde91] Aldemir T. Utilization of the cell-to-cell mapping technique to construct Markov failure models for processed control systems. Proceedings of PSAM, Beverly Hills (USA) 1991;2:1431–6.

[Alde94] Aldemir T, Siu N, Cacciabue P, Gül Göktepe B, Mosleh A. Reliability and safety assessment for dynamic process systems, NATO ASI Series, vol. 120. Berlin: Springer, 1994.

[Amen84] Amendola A, Reina G. Dylam-1, AA software package for event sequence and consequence spectrum methodology. EUR9224 EN, Commission of European Communities, 1984.

[Blom et al 03] Blom, H.A.P., Bakker, G.J., Everdij M.H.C., M.N.J. van der Park, Stochastic analysis background of accident risk assessment for Air Traffic Management, Report Hybridge WP2.2, January 21st 2003.

[BlomBakk02] Blom, H.A.P. and Bakker, G.J., Conflict probability and incrossing probability in air traffic management, Proceedings IEEE Conference on Decision and Control, Las Vegas, NV, December, 10-13, 2002, pp. 2421-2426.

[Blom94] Blom, H.A.P., Klompstra, M.B., Bakker, G.J., Air traffic management as a multiagent stochastic dynamic game under partial state observation, in : Proc. IFAC 7th Symposium on Transportation systems: Theory and application of advanced technology, pp. 249-254, Tianjijn, China, August 1994.

[Bakk93] Bakker, G.J., and Blom, H.A.P., "Air traffic collision risk modelling," 32nd IEEE Conference on Decision and Control, Vol. 2, Institute of Electrical and Electronics Engineers, New York, 1993, pp. 1464-1469.

[Belh96] Belhadj M, Aldemir T. Some computational improvements in process system reliability and safety analysis using dynamic methodologies. Reliability Engineering and System Safety 1996;52(3):339–47.

[Coja93] Cojazzi, G, Cacciabue, P.C., Parisi, P. DYLAM-3, a dynamic methodology for reliability analysis and consequences evaluation in industrial plants, theory and how to use. Commission of the European Communities, JRC, EURATOM, Report EUR 15265 EN, 1993.

[DevSmi92] Devooght J, Smidts C, Probabilistic reactor dynamics. I The theory of continuous event trees. Nuclear Science and Engineering, 1992; 111:229-40.

[DevSmi94] Devooght J, Smidts C, Probabilistic dynamics: The mathematical and computing problems ahead. Reliability and Safety Assessment of Dynamic Process Systems, T.Aldemir at al (Eds.), Springer Verlag, 1994, pp.85-100.

[DevLab95] Devooght J, Labeau PE. Moments of the distributions in probabilistic dynamics. Annals of Nuclear Energy 1995;22(2):97–108.

[Ghosh93] Ghosh M. K., A. Arapostathis and S. I. Marcus, Optimal control of switching diffusions with applications to flexible manufacturing systems, SIAM J. Control Optim, 1993; 31, pp. 1183-1204.

[Ghosh97] M.K. Ghosh, A. Arapostathis, and S.I. Marcus, Ergodic Control of Switching Diffusions, SIAM J.l Control Optim, November 1997; 35, pp. 1952-1988.

[Gihm&Skor72] Gihman, I. I, Skorohod, A.V, Stochastic differential equations, Springer-Verlag Berlin, 1972.

[Gihm&Skor82] Gihman, I. I, Skorohod, A.V, Stochastic differential equations and their applications, Naukova Dumka, Kiev, 1982. (in Russian)

[Elliott82] Elliott, R.J., Stochastic Calculus and Applications, Springer-Verlag, New York, 1982.

[Freid84] Freidlin, M.I., Wentzell, A.D., Random perturbations of dynamical systems, Springer-Verlag, New-York, 1984.

[Hass90] Hassan M, Aldemir T. A data base oriented dynamic methodology for the failure analysis of closed loop control systems in process plants. Reliability Engineering and System Safety 1990;27:275–322.

[Kloe92] Kloeden, P.E., Platen, E., Numerical solution of stochastic differential equations, Springer-Verlag Berlin Heidelberg, 1992, 632 p.

[LabDev95] Labeau PE, Devooght J. Synthesis of multivariate distributions from their moments for probabilistic dynamics. Annals of Nuclear Energy. 1995 ;22(2):109–24.

[Labeau95] Labeau PE. Improvement of probabilistic dynamics calculations by the determination of the support of the distributions. Proceedings of Esrel'95, 1995. p. 431–44.

[Labeau98] Labeau P.E, A survey on Monte Carlo estimation of small failure risks in dynamic reliability. International Journal of Electronics and Communication, 1998; 52(3):205-11.

[Labeau00] Labeau, P.E., Smidts, C., Swaminathan, S., Dynamic reliability: towards an integrated platform for probabilistic risk assessment, Reliability Engineering & Systems Safety, 2000; 68, pp. 219-254.

[Mars98] Marseguerra M, Zio E, Devooght J, Labeau P.E, A concept paper on dynamic reliability via Monte Carlo simulation. Mathematics and Computers in Simulation 1998; 47:371-82.

[Mils95] Milstein, G. N., Numerical Integration of Stochastic Differential Equations, Kluwer, Dordrecht, 1995.

[Rein87] Reina G, Amendola A. DYLAM-2 Description and how to use. Commission of the European Communities, JRC Ispra (Italy), Eura-tom, PER1393/87, Technical Note I.87.128, 1987.

[Reich64] Reich, P.G., A theory of safe separation standards for Air Traffic Control, Technical Report 64041, Royal Aircraft Establishment, U.K., 1964.

[Rice45] Rice, S.O., Mathematical analysis of random noise, Part II, Bell System Technical Journal, 1945; 24, pp. 46-156.

[Roya92] Risk: Analysis, perception and management, Report of a Royal Society Study Group, London, The Royal Society, 1992.

[SiuAco90] Siu N, Acosta C. Modeling the effect of dependency between humans and hardware on overall system performance, NUREG/CP-0114. Proceedings of 18th Water Reactor Safety Information Meeting, Rockville, MD, 22–24 October 1990. p. 149–74.

[Tomb96a] Tombuyses B, Aldemir T. Continuous cell-to-cell mapping and dynamic PSA. Proceedings of the International Conference on Nuclear Engineering ICONE-4, New Orleans (USA) 1996;3:431-8.

[Tomb96b] Tombuyses B, Aldemir T. Dynamic PSA of process control systems via continuous cell-to-cell mapping. Proceedings of Esrel'96-PSAM III, Creete (Greece) 1996;3:1541-6.

[Tomb97] Tombuyses B, Aldemir T. Computational efficiency of the continuous cell-to-cell mapping as a function of integration schemes. Reliability Engineering and System Safety 1997;58:215–23.

[Wein63] Wei J, Norman E. Lie algebraic solution of linear differential equations. Journal of Mathematical Physics 1963;4(4):575–81.