Relevance of control theory to design and maintenance problems in time-variant reliability: The case of stochastic viability

C. Rougé, Jean-Denis Mathias, G. Deffuant

Relevance of control theory to design and maintenance problems in time-variant reliability: the case of stochastic viability

Charles Rougé[1,2], Jean-Denis Mathias[1] and Guillaume Deffuant[1]

July 22, 2014

Abstract

The goal of this paper is twofold: 1) to show that time-variant reliability and a branch of control theory called stochastic viability address similar problems with different points of view, and 2) to demonstrate the relevance of concepts and methods from stochastic viability in reliability problems. On the one hand, reliability aims at evaluating the probability of failure of a system subjected to uncertainty and stochasticity. On the other hand, viability aims at maintaining a controlled dynamical system within a survival set. When the dynamical system is stochastic, this work shows that a viability problem belongs to a specific class of design and maintenance problems in time-variant reliability. Dynamic programming, which is used for solving Markovian stochastic viability problems, then yields the set of design states for which there exists a maintenance strategy which guarantees reliability with a confidence level β for a given period of time T. Besides, it leads to a straightforward computation of the date of the first outcrossing, informing on when the system is most likely to fail. We illustrate this approach with a simple example of population dynamics, including a case where load increases with time.

Keywords: Viability theory, Time-variant reliability, Dynamical systems, Dynamic programming, Reliability kernel, Design and maintenance problems

[1] Irstea, UR LISC Laboratoire d'ingénierie des systèmes complexes, 24 avenue des Landais - CS 20085, 63178 Aubière Cedex, F-63172, France

[2] Université Laval, Département de génie civil et de génie des eaux, Pavillon Adrien-Pouliot, 1065 avenue de la Médecine, Québec G1V 0A6, QC, Canada

1 Introduction

This paper connects two lines of research, viability and reliability, that have ignored each other up to now despite strong similarities. Both frameworks study the potential for a system to retain desirable properties. They were developed in different contexts and sometimes tackle different specific technical or conceptual issues in relation with the same type of problems, which makes their confrontation promising. In particular, this work focuses on showing how concepts and methods coming from the so-called stochastic viability framework (Doyen and De Lara, 2010) are applicable to time-variant reliability. Indeed, they foster the resolution of a particular class of design and maintenance problems, that this paper is to describe with accuracy.

Reliability theory initially comes from the field of mechanical and structural engineering (Rackwitz, 2001) and has a wide range of applications, from material science (Mathias and Lemaire, 2012) and industrial maintenance (Rausand, 1998) to ecology (Naeem, 1998), environmental management (Aliev and Kartvelishvili, 1993) and hydrology (Melching, 1992). In these applications, different numerical methods enable the estimation of the response surface and the associated probability of a system to be in the so-called failure set. Reliability methods provide ever-improving approximations of this probability of failure in cases of growing complexity, and have been perfected and tailored to an increasing number of applications (Ditlevsen and Madsen, 1996; Rackwitz, 2001; Lemaire, 2009). Let us cite for instance Monte Carlo methods, First and Second Order Reliability Methods (FORM and SORM), or response surface approximations. A central concern is often with understanding and modeling the correlations between the different variables.

However, many of these developments deal with time-invariant systems, since they are carried out under a single definite period of time. When the system under consideration evolves in time, the reliability problem is referred to as time-variant. The central issue of representing the correlations between variables is then extended to account for the time correlations of the processes of interest. The probability of reaching the failure set during the evolution is called the cumulative probability of failure. Rice's formula (Rice, 1944), which counts the average number of times an ergodic stationary process crosses a given fixed level, serves as a basis for computing the cumulative probability of failure in the outcrossing approach. This approach is based on the computation and time integration of the outcrossing rate, i.e. the rate at which the state reaches the failure set, e.g. Li and Der Kiureghian (1995). It has been applied to simple cases where analytical derivations are tractable (Guedes Soares and Garbatov, 1998; Sudret, 2008a) or alongside approaches from time-invariant reliability such as FORM (Kuschel and Rackwitz, 2000), or finite elements methods (Sudret, 2008b).

Thus, bridges exist between the time-variant and -invariant cases. In fact, some outcrossing algorithms decompose the time-variant problem into a series of time-invariant ones (Hagen and Tvedt, 1991; Andrieu-Renaud et al., 2004; Sudret, 2008a), and conversely, the outcrossing rate has been defined on variables other than time (Sudret, 2008b). Some cases can even be solved both with the outcrossing rate approach, and by having time as a parameter (Burgazzi, 2008). Other studies treat a time-variant problem like a time-invariant one, by considering time as a parameter (Petryna et al., 2002; Schotanus et al., 2004) or as yet another space variable (Wang and Wang, 2013), or by treating a finite number of dates like a series system (Savage and Son, 2011).

Most of the works cited in the two paragraphs above assume a monotonic decrease of performance with time. Such an assumption is perfectly reasonable for structures that deteriorate as they grow old, but recent time-variant reliability studies have questioned its systematic use, and suggest using methods that do not require this hypothesis (Quigley and Walls, 2011; Targoutzidis, 2012; Wang and Wang, 2013). A second limitation of the existing literature, linked with the assumption of a monotonic decrease in performance through time, is the idea that maintenance is the fact of choosing between a limited set of options which essentially are equivalent to rejuvenating the system, e.g. Guedes Soares and Garbatov (1998), Kuschel and Rackwitz (2000), Val and Stewart (2003). Without a monotonic decrease of performance, other types of maintenance need to be taken into account. Besides, there is no framework within the time-variant reliability literature that formally considers design and maintenance together. Nevertheless, design and maintenance are closely related, since a system should be designed in a way that allows for an appropriate maintenance throughout its lifetime.

To address these current limits of time-variant reliability, this work uses a stochastic controlled dynamical system formulation. Non-controlled dynamics can be found in the time-variant reliability literature (Sørensen et al., 2005; Biondini and Frangopol, 2009; Targoutzidis, 2012), and the use of controls leads to a general formulation for design and maintenance problems by linking the acceptability of a design to the existence of a maintenance strategy such that reliability is guaranteed with a confidence β, i.e., such that the cumulative probability of failure is smaller than $1 - \beta$.

The link between the initial configuration of a system and the existence of strategies that keep it out of a failure state are central to viability theory (Aubin, 1991; Aubin et al., 2011). This is a control theory that deals with controlled dynamic systems under state constraints, and whose original focus is on controlled deterministic systems. An emphasis is put on finding the viability kernel, the set of all initial states which can be controlled so that their trajectory is maintained within the constraint set at all times. Viability algorithms generally yield both the viability kernel and the associated viable controls at once, e.g. Saint-Pierre (1994), Bonneuil (2006), Deffuant et al. (2007). Viability tools have been successfully applied to a variety of fields such as finance, robotics, or ecology, e.g. Deffuant and Gilbert (2011). Recent work has extended the framework of viability theory in discrete time by considering uncertainties in the dynamics, leading to the definition of the stochastic viability kernel (De Lara and Doyen, 2008), a set of states for which the respect of the constraints can be guaranteed with a desired minimal probability and for a desired time frame. Dynamic programming can compute stochastic viability kernels and determine the control strategy that maximizes the probability to maintain the system in the constraint set during that period (Doyen and De Lara, 2010). This is the specific development which applicability to reliability problems we propose to demonstrate throughout this work.

The paper is organized as follows. Section 2 introduces the notion of reliability kernel to describe a time-variant design problem. Then Section 3 extends this notion to a coupled problem of design and maintenance through a controlled dynamical system formulation. After that, Section 4 shows how the framework of viability theory applies to a specific case of this coupled design and maintenance problem, and solves it in the Markovian case. Section 5 proposes an application in order to illustrate how dynamic programming can be applied to a reliability problem. The discussion of Section 6 further argues about the potential of confronting reliability with control theories such as viability. Finally, Section 7 summarizes the findings.

2 A design problem in time-variant reliability

This section proposes a general formulation for design problems in time-variant reliability, which comes from a similar problem in time-invariant reliability.

2.1 Time-invariant reliability

Let us consider a system and a vector of n random variables $\mathbf{X}$ which represents the system's state variables and their uncertainty. Reliability is concerned with the performance function $g(\mathbf{X})$, and with the so-called limit-state (or failure) surface defined by (Ditlevsen and Madsen, 1996; Lemaire, 2009):

$$g(\mathbf{X}) = 0 \tag{1}$$

The limit-state surface separates the failure domain F (where $g(\mathbf{X}) < 0$) from the survival domain S (where $g(\mathbf{X}) \geq 0$). The object of reliability is to determine the probability of failure p_f of the system :

$$p_f = \mathbb{P}(\mathbf{X} \in F) = \mathbb{P}(g(\mathbf{X}) < 0)). \tag{2}$$

A diversity of methods have been developed to compute or approximate the limit-state surface and the probability of failure in the time-invariant case (Ditlevsen and Madsen, 1996; Lemaire, 2009).

Choices regarding the design of the system may influence the random vector $\mathbf{X}$ or the performance function. Without loss of generality, the problem can be formulated so these choices only affect the former. Let us represent choices by a fixed vector π chosen in a space $\Pi \subset \mathbb{R}^m$ and $m \in \mathbb{N}$. Let us call design this vector: each design leads to a distinct random vector $\mathbf{X}(\pi)$. Then the associated probability of failure $p_f(\pi)$ is:

$$p_f(\pi) = \mathbb{P}(g(\mathbf{X}(\pi)) < 0)). \tag{3}$$

This work focuses on finding values of π such that the system is reliable with a confidence level β (i.e., a significance level $\alpha = 1 - \beta$). In other words, we are interested in finding elements from the set of design choices such that reliability is achieved with a confidence β. Let us introduce this set as the reliability kernel, noted $\text{Rel}_\pi(\beta)$ and formally written as follows:

$$\text{Rel}_\pi(\beta) = \{\pi \in \Pi | p_f(\pi) \leq 1 - \beta\} \tag{4}$$

For instance, $\text{Rel}_\pi(0.99)$ is the set of available designs such that the system has a 99% chance of being in the survival set S. Let us now extend this design problem to the time-variant case.

2.2 Time-variant reliability

We now place ourselves between an initial date $t_0 = 0$ and final date T, so that the problem is studied within a time interval $[0, T]$ called the planning period. The uncertainty and stochasticity of the system are represented at all dates by the vector $\mathbf{X}(t, \pi)$. There is a consensus in the reliability literature that $\mathbf{X}(t, \pi)$ aggregates a vector of random variables like in time-invariant viability, as well as a vector of one-dimensional random processes that may be correlated with one another as well as with the random variables (Kuschel and Rackwitz, 2000; Andrieu-Renaud et al., 2004; Sudret et al., 2005). These processes may also be autocorrelated in time.

The performance of the system may also evolve with time, and is now noted $g(t, \mathbf{X}(t, \pi))$. Likewise, the limit-state surface $g(t, \mathbf{X}(t, \pi)) = 0$ may be dependent on time, and so may the failure domain $F(t)$ (where $g(t, \mathbf{X}(t, \pi)) \leq 0$) and the survival domain $S(t)$ (where $g(t, \mathbf{X}(t, \pi)) \geq 0$).

Time-variant reliability is concerned with the cumulative probability of failure $p_f(t, \pi)$, the probability of reaching the failure set over $[0, t]$:

$$p_f(t, \pi) = \mathbb{P}(\exists \tau \in [0, t], \mathbf{X}(\tau, \pi) \in F(\tau)) \tag{5}$$

From now on, we shall simply call "probability of failure" the cumulative probability of failure $p_f(t, \pi)$, because it is the time-variant equivalent of the probability of failure $p_f(t)$ from equation (5). Much like for the time-invariant case, this work focuses on the problem of finding values of the design vector π such that the system is reliable over the planning period $[0, T]$ with a confidence level β. A very similar problem consists in finding elements from the reliability kernel $\mathrm{Rel}_\pi(\beta, T)$, defined as:

$$\mathrm{Rel}_\pi(\beta, T) = \{\pi \in \Pi | p_f(T, \pi) \leq 1 - \beta\} \tag{6}$$

For instance, $\mathrm{Rel}_\pi(0.99, 100)$ is the set of available designs such that the system has a 99% chance of staying in the survival set $S(t)$ until at least $T = 100$.

Existing time-variant reliability methods aim at finding the value of the probability of failure $p_f(T, \pi)$ given the value of π. In other words, they only aim at iteratively testing which values of π may be acceptable. This is the case for instance for outcrossing (or outcrossing-based) methods (Kuschel and Rackwitz, 2000; Rackwitz, 2001; Andrieu-Renaud et al., 2004; Sudret, 2008a). They are based on the outcrossing rate $\nu^+(t)$ defined as the instantaneous rate at which the system leaves the survival set (Andrieu-Renaud et al., 2004):

$$\nu^+(t) = \lim_{\Delta t \overset{>}{\to} 0} \frac{\mathbb{P}\left(\{g(t, \mathbf{X}(t, \pi)) \geq 0\} \cap \{g(t + \Delta t, \mathbf{X}(t + \Delta t, \pi)) < 0\}\right)}{\Delta t} \tag{7}$$

Time integration of $\nu^+(t)$ throughout the planning period provides an upper bound for the probability of failure:

$$p_f(T, \pi) \leq \int_0^T \nu^+(t) dt \tag{8}$$

and this inequality becomes an equality under the assumption that failure occurs only once. The aim is then to determine when the time-dependent system crosses the limit-state surface.

3 A general design and maintenance problem

Let us now explore the consequences of changing the time-variant design problem of Section 2.2 so as to incorporate the maintenance of the system. Since maintenance is done at discrete dates, it is the values of $\mathbf{X}(t, \pi)$ at these dates that matter. Thus, we first introduce a discrete-time dynamical system formulation, then we add to this formulation the possibility to control the system.

3.1 Discrete-time dynamics

Instead of a representation of the time evolution of a system through its correlation structure, usual within reliability theory, in this work time dependence is expressed explicitly using a dynamical system formulation. Dynamical systems are present in the time-variant reliability literature (Sørensen et al., 2005; Targoutzidis, 2012), and including under discrete time formulations (Biondini and Frangopol, 2009). In this Section, let us assume that reliability assessments focus on $\mathbf{X}(t,\pi)$ at discrete dates $t = 0, 1, \ldots, T-1, T$, where the time interval between two consecutive dates may not be constant. Then, the time correlation structure of the stochastic processes of interest may not be entirely given by the discrete sequence of random vectors $(\mathbf{X}(0,\pi), \mathbf{X}(1,\pi), \ldots, \mathbf{X}(T-1,\pi), \mathbf{X}(T,\pi))$. This is why we introduce another random vector $\mathbf{W}(t)$ which represents how uncertainty and stochasticity affect the system between two consecutive dates[1]:

$$\mathbf{X}(t+1,\pi) = f(t,\pi,\mathbf{X}(t,\pi),\mathbf{W}(t)) \tag{9}$$

where f is the dynamic[2]. Following a convention from De Lara and Doyen (2008), a realization of the sequence $\mathbf{W} = (\mathbf{W}(0), \mathbf{W}(1), \ldots, \mathbf{W}(T-1))$ is called a scenario, and it is an element from the set of all scenarios $\mathbb{S}$. The correlation structure of $\mathbf{W}$ reflects the time correlation structure of the stochastic processes of interest. Thus, the vectors $\mathbf{W}(t_1)$ and $\mathbf{W}(t_2)$ can be correlated for any two dates t_1 and t_2. Only in the Markovian case are $\mathbf{W}(t_1)$ and $\mathbf{W}(t_2)$ statistically independent for all t_1 and t_2 within $[0,T]$.

Through the iterative application equation (9) between the initial date 0 and a later date t, $\mathbf{X}(t,\pi)$ only depends on the design π, the initial value $\mathbf{X}(0,\pi)$ of the random vector $\mathbf{X}(t,\pi)$, and the scenario $\mathbf{W}$. Further assuming, similar to the time-invariant case (Section 2.1), that $\mathbf{X}(0,\pi)$ is only a function of the design π, $\mathbf{X}(t,\pi)$ can be written as a function of the following:

$$\mathbf{X}(t,\pi) = f(t,\pi,\mathbf{W}) \tag{10}$$

and we call trajectory the sequence $(\mathbf{X}(0,\pi), \mathbf{X}(1,\pi), \ldots, \mathbf{X}(T-1,\pi), \mathbf{X}(T,\pi))$.

Then, the probability of failure is computed using the probability distribution of the scenarios. The definitions of $p_f(t,\pi)$ from equation (5) and $\mathrm{Rel}_\pi(\beta,T)$ from (6) apply to the discrete time dynamics from equation (9), the only change being that only a set of discrete dates within $[0,T]$ is now of interest.

3.2 Design and maintenance in time-variant reliability

Still on a planning period $[0,T]$, let us now consider the possibility of acting on the system at each of the discrete dates introduced in Section 3.1. Maintenance actions are represented by a vector u called a *control* or control vector. Similar to the design π, a control vector is a choice fixed by the entity that maintains the system. The set of available controls at a given discrete date t is noted $U(t,\pi)$, and it

[1] Since the dependence of the state on the parameter π is already clear in equation (9), $\mathbf{W}(t)$ can be made independent from the parameter π, which is why we do not use the notation $\mathbf{W}(t,\pi)$.

[2] The different dynamics in the text will always be noted as f, even though they are not the same .

is a subset of $\mathbb{R}^q$. The representation of maintenance actions leads to updating equation (9) into:

$$\mathbf{X}(t+1,\pi) = f(t,\pi,\mathbf{X}(t,\pi),u(t),\mathbf{W}(t)) \tag{11}$$

In control theory terms, this is a stochastic controlled discrete-time dynamical system.

In this work, controls are applied so that the system does not reach the failure set. This is what the reliability literature calls preventive maintenance (Rausand, 1998). To assess how controls affects reliability, the whole sequence of controls applied at the dates $0, 1, \ldots, T-1$ is of interest. We call strategy the sequence $u(.) = (u(0), u(1), \ldots, u(T-1))$. The set of all strategies that can be implemented during the time frame $[0,T]$ is noted $\mathcal{U}(T)$. Notations involved in this formulation are summarized in Table 1. The notion of trajectory introduced by equation (10) can be extended to account for $u(.)$, so that the iterative application of equation (11) between the initial date and a date t leads to:

$$\mathbf{X}(t,\pi) = f(t,\pi,u(.),\mathbf{W}) \tag{12}$$

Given the design π, the strategy $u(.)$ and the scenario $\mathbf{W}$, there is only one sequence of random variables, $(\mathbf{X}(0,\pi), \mathbf{X}(1,\pi), \ldots, \mathbf{X}(T-1,\pi), \mathbf{X}(T,\pi))$.

Through the latter equation (12), the probability of failure becomes a function of t, π and $u(.)$:

$$p_f(t,\pi,u(.)) = \mathbb{P}(\exists \tau \in [0,t], \mathbf{X}(\tau,\pi) \in F(\tau)) \tag{13}$$

and we can now introduce the reliability kernel of the design problem, in cases where the designer should also be concerned with the system's subsequent maintenance. Then, the goal is to find a design π such that there exists a control strategy $u(.)$ that guarantees the system's reliability with a confidence level β. Its reliability kernel is thus redefined from equation (6) to become $\mathrm{Rel}_{\pi,u}(\beta,T)$, formally defined as follows:

$$\mathrm{Rel}_{\pi,u}(\beta,T) = \{\pi \in \Pi | \exists u(.) \in \mathcal{U}(T), p_f(T,\pi,u(.)) \leq 1-\beta\} \tag{14}$$

Equation (6) correspond to the case where there is no maintenance, which is equivalent to considering that only one strategy is available, and therefore, that it is necessary applied to the system. Conversely, there are cases where there is only maintenance, and the problem is to find whether there is an adequate maintenance strategy: these are maintenance problems. Such cases amount to considering that there is only one possible design ($\Pi = \{\pi\}$), so that either $\mathrm{Rel}_{\pi,u}(\beta,T) = \emptyset$ or $\mathrm{Rel}_{\pi,u}(\beta,T) = \Pi$. Thus, introducing controls in time-variant reliability leads to a coupled design and maintenance problem, and design and maintenance must be considered together. Two other important remarks must be made at this stage.

First, to call a design π reliable, it is necessary to find an adequate strategy, but its search is very challenging because it is necessary to choose among multiple options at each time step. Thus, searching a strategy in $\mathcal{U}(T)$ means searching a space of very high dimensionality. Existing time-variant reliability methods rather aim at computing the probability of failure $p_f(t,\pi,u(.))$ for a given design and maintenance strategy, therefore they are not suited to handle the proposed design and maintenance problem on their own. The general aim of control theories is to find the appropriate controls in a given

Notation	Vector space	Description
$\mathbf{X}(t,\pi)$	$\mathbb{R}^n$	State (random vector) at the discrete date t
$\mathbf{W}(t)$	$\mathbb{R}^p$ $(p \leq n)$	Effect of the stochastic processes between t and $t+1$
$\mathbf{W}$	$(\mathbb{R}^p)^T$	Scenario, sequence $(\mathbf{W}(0), \mathbf{W}(1), \ldots, \mathbf{W}(T-1))$
π	Π	Design (or design choice): fixed
u	$U(t,x) \subset \mathbb{R}^q$	Control (decision): fixed
$u(.)$	$\mathcal{U}(T)$	Strategy (control sequence)

Table 1: Vector notation summary for the general design and maintenance problem in time-variant reliability: with the random vectors in the top half and the decisions to take (deterministic vectors) in the bottom half.

situation, which justifies the idea of exploring how a particular control theory, namely viability theory, may help find reliable designs.

Second, the reliability kernel depends heavily on the information that is available on the system at each date when action must be undertaken. Indeed, information on $\mathbf{X}(t,\pi)$ may lead to adapt the control to that information. Although some reliability studies use bayesian updating to empirically update reliability estimates, e.g. Hsiao et al. (2008), Quigley and Walls (2011), they do not provide a formal framework to deal with the issue of information. Control theory did formalize the importance of information on the state of the system when it comes to controlling it so it avoids failure (Aubin, 1991; Clarke et al., 1995; Doyen and De Lara, 2010; Aubin et al., 2011). Thus, open-loop feedbacks designate predetermined control strategies that are applied without taking information collected at t on $\mathbf{X}(t,\pi)$ into account. Closed-loop feedbacks indicate, to the contrary, that the control is chosen based on the acquisition of new knowledge on $\mathbf{X}(t,\pi)$. In fact, viability theory applies to both types of feedbacks, but the developments from stochastic viability that are to be discussed in the next Section use closed-loop feedbacks.

4 Relevance of stochastic viability in time-variant reliability

The relevance of stochastic viability to solve design and maintenance problems in time-variant reliability is now demonstrated. We use closed-loop feedbacks, so that the control u at date t also depends on information about the system. We will explore how this changes the general design and maintenance problem of Section 3.2, first in the full information case in Section 4.1, and then in the more general partial information case in Section 4.2. Following that, Section 4.3 presents stochastic viability and the associated stochastic viability kernel, which it relates to the reliability kernel of the problem of Section 4.2. This relationship enables the introduction of dynamic programming to solve that problem, as detailed in Section 4.4. This method also leads to approximations of the outcrossing rate as in Section 4.5.

4.1 Closed-loop feedbacks with full information

Full information means that at date t, we have access to complete knowledge of the state $x(t,\pi)$, which is a realization of the random variable $\mathbf{X}(t,\pi)$. The existence of closed-loop feedbacks means that the choice of u at date t depends on the state $x(t,\pi)$. Within a closed-loop formulation, a strategy $u(.)$ (as introduced in Section 3.2) associates a maintenance decision $u(t, x(t, \pi))$ to each date t and state y.

Since we are working with realizations rather than with the random vector $\mathbf{X}(t, \pi)$ itself, equation (11) becomes:

$$x(t+1, \pi) = f(t, \pi, x(t, \pi), u(t, x(t, \pi)), w(t)) \tag{15}$$

where $w(t)$ represents the realization of $\mathbf{W}(t)$ in equation (15). It represents the randomness in updating the state from date t to $t{+}1$, and we also call scenario the sequence $w(.) = (w(0), w(1), \ldots, w(T{-}1))$.

Let us now introduce $y(t) = (x(t, \pi), \pi)$, a vector which aggregates the state and design vectors. The framework of so-called stochastic viability theory[1] De Lara and Doyen (2008) and Doyen and De Lara (2010) focuses on the dynamic of $y(t)$ instead of that of $x(t, \pi)$. The dynamic (15) becomes:

$$y(t+1) = f(t, y(t), u(t, y(t)), w(t)) \tag{16}$$

Stochastic viability then calls $y(t)$ the state vector, and closed-loop feedbacks are determined by $y(t)$. Yet, if neither x nor f depend on the design, setting $y(t) = x(t)$ puts equation (15) under the form of equation (16) (see Section 5).

4.2 Closed-loop feedback with partial information

In many cases, there is no direct access to the realization $x(t, \pi)$. In this paper, we assume that this partial information is a realization $z(t, \pi)$ of a known random variable $\mathbf{Z}(x(t, \pi), \pi)$. Under this assumption, the dynamics of this realization $z(t, \pi)$ can be deduced from that of $\mathbf{X}(t, \pi)$:

$$z(t+1, \pi) = f(t, \pi, z(t, \pi), u(t, z(t, \pi)), w(t)) \tag{17}$$

where u depends on the vector $z(t, \pi)$ because we still are in the closed-loop feedback case. The full information case of Section 4.1 corresponds to the case $\mathbb{P}[\mathbf{Z}(x(t, \pi), \pi) = x(t, \pi)] = 1$, Then, setting $y(t) = (z(t, \pi), \pi)$ yields the same equation as (16):

$$y(t+1) = f(t, y(t), u(t, y(t)), w(t)) \tag{18}$$

where $y(t)$ is again called the state of the system from a stochastic viability perspective. Yet again, if z and f do not explicitly depend on π, then using $y(t) = z(t)$ turns equation (17) into (16).

Working with the dynamics of equation (16) only makes sense if the knowledge of $y(t) = (z(t, \pi), \pi)$ helps in assessing the reliability of the system. Therefore, in the remainder of this article, we also assume that it is possible to compute the conditional probability $\mathbb{P}(\mathbf{X}(t, \pi) \in S(t) | y(t))$. This assumption holds in the full information case because then, $\mathbb{P}(\mathbf{X}(t, \pi) \in S(t) | y(t)) = 1$ if $y(t) = (x(t, \pi), \pi)$ where $x(t, \pi)$ is the realization of $\mathbf{X}(t, \pi)$, and 0 otherwise.

Since π is fixed beforehand and does not depend on time, it is given by the initial state $y_0 = y(0)$. As for equation (12), for a given initial state y_0, a given strategy $u(.)$ and a given scenario $w(.)$, there is a unique trajectory $y(y_0, u(.), w(.)) = (y(0), y(1), \ldots, y(T-1), y(T))$. With these notations, and since probabilities then take into account all the scenarios, we can then write the probability of failure as a

[1] As a matter of fact, “probabilistic” may be a more accurate word than “stochastic”.

function of t, y_0 and $u(.)$:

$$p_f(t, y_0, u(.)) = \mathbb{P}\left[\exists \tau \in [0,t], \mathbf{X}(t,\pi) \in F(\tau) | y_0, u(.)\right] \tag{19}$$

The search of reliable designs can be turned into that of initial states y_0 such that there is a control strategy $u(.)$ which guarantees that the system is reliable with a confidence level β during the planning period. The corresponding reliability kernel, derived from equation (14), is simply noted $\mathrm{Rel}(\beta, T)$ (instead of $\mathrm{Rel}_{\pi,u}(\beta, T)$). It is the following set:

$$\mathrm{Rel}(\beta, T) = \{y_0 \in \mathbb{Y} | \exists u(.) \in \mathcal{U}(T), p_f(T, y_0, u(.)) \leq 1 - \beta\} \tag{20}$$

where the set $\mathbb{Y}$ is the state space. In order to compute this kernel, let us now relate it to a mathematical object from stochastic viability theory, the stochastic viability kernel.

4.3 The stochastic viability kernel

Similar to reliability, stochastic viability theory (De Lara and Doyen, 2008; Doyen and De Lara, 2010) focuses on the probability for a system to stay in the survival set during a given time frame. In discrete time, it focuses on the time evolution of a state vector, through a governing equation that is none other than equation (16). Stochastic viability assumes that the state vector $y(t)$ is known at each time step, and that given $y(t)$, the probability of being in the survival set at t is also known.

Thus, stochastic viability focuses on a very similar problem to that described in Section 4.2. One of its central concepts is the so-called stochastic viability kernel, which importance comes from the original deterministic control framework of viability theory (for a quick overview of viability theory and the viability kernel, see Appendix A). It is defined as the set of all states for which there is a strategy such that the system has a probability β or higher of staying in the survival set $S(t)$ for a given time horizon T. It can be formally defined by the following equation in which it is noted $\mathrm{Viab}(\beta, T)$:

$$\mathrm{Viab}(\beta, T) = \{y_0 \in \mathbb{Y} | \exists u(.) \in \mathcal{U}(T), \mathbb{P}(\forall t \in [0,T], \mathbf{X}(t,\pi) \in S(t) | y_0, u(.)) \geq \beta\} \tag{21}$$

Stochastic viability is related to the closed-loop reliability problem of Section 4.2 through the remark that:

$$p_f(T, y_0, u(.)) = 1 - \mathbb{P}(\forall t \in [0,T], \mathbf{X}(t,\pi) \in S(t) | y_0, u(.)) \tag{22}$$

Through equations (20) and (21), the stochastic viability kernel is the reliability kernel of equation (20):

$$\mathrm{Rel}(\beta, T) = \mathrm{Viab}(\beta, T) \tag{23}$$

Yet, by itself, equation (23) does not allow for the computation of the reliability kernel $\mathrm{Rel}(\beta, T)$. Its interest comes from the fact that there exists a dynamic programming algorithm to compute the stochastic viability kernel.

4.4 A dynamic programming solution

In this Section, we are in the Markovian case, meaning that all the $w(t)$ of equation 16 are statistically independent from each other. Then, Doyen and De Lara (2010) establish that the problem of finding the stochastic viability kernel can be solved by dynamic programming, a widespread category of recursive algorithms designed to solve the problem backwards from date T to the initial date. Thus, dynamic programming also allows for solving the reliability-viability problem in the Markovian case.

Let us assume that the continuous bounded sets that form the state and control spaces have been discretized, as is the case in practice. The state is then represented by a finite set of points y_i of the discrete space A_d. Likewise, the discrete control space U_d is represented by points noted u_j, and each control space $\mathcal{U}_d(t, y_i)$ is a subset of U_d. Then the transition equation (16) is given by the probabilities $\mathbb{P}(f(t, y_i, u_j, w(t)) = y_k)$, which we assume to be handily computable. As specified in Section 4.2, we also need to assume that at date t, we know enough about the probability distribution of $\mathbf{X}(t, \pi)$ to compute $\mathbb{P}(\mathbf{X}(t, \pi) \in S(t)|y_i)$, and that we know the value of y_i.

Then, Doyen and De Lara (2010) link $\text{Viab}(\beta, T)$ to a value function $V(t, y_i)$ that is defined both by an initial equation at date T and by a recursive equation. The initial equation is as follows:

$$V(T, y_i) = \mathbb{P}(\mathbf{X}(T, \pi) \in S(T)|y_i) \tag{24}$$

while the latter reads for all t between dates 0 and $T - 1$:

$$V(t, y_i) = \left(\max_{u_j \in \mathcal{U}_d(t, y_i)} \sum_{y_k \in A_d} V(t+1, y_k).\mathbb{P}(f(t, y_i, u_j, w(t)) = y_k) \right) .\mathbb{P}(\mathbf{X}(t, \pi) \in S(t)|y_i) \tag{25}$$

Doyen and De Lara demonstrate that $\text{Viab}(\beta, T)$ is the set of all states such that $V(0, y_i) \geq \beta$. Thus, the states for which there exists a reliable strategy $u(.)$ with a confidence level β are also given by $V(0, y_i) \geq \beta$. Besides, another result from Doyen and De Lara (2010) is that the computation of the value function yields the control strategy $u^*(.)$ that minimizes the probability of failure for a trajectory starting at a state y_0, so that:

$$V(0, y_0) = 1 - p_f(T, y_0, u^*(.)) \tag{26}$$

A major advantage of the stochastic viability approach is that the maintenance controls are not fixed beforehand. It dynamically and simultaneously computes both the optimal maintenance strategy and the associated probability of viability (or reliability) associated to that strategy.

4.5 Approximating the date of first outcrossing

Whereas the outcrossing rate (equation (7)) is usually integrated over a period of time to yield the probability of failure, the dynamic programming algorithm presented above does not compute it directly. Nevertheless, given an initial state y_0 and a strategy $u(.) \in \mathcal{U}(T)$, it is useful to know around which dates the system is most likely to leave the survival set. Noting t_{out} the date at which the system first leaves the survival set for the first time, the probability $\mathbb{P}(t_{out} = t)$ is related to the probability of failure $p_f(t, y_0, u(.))$ defined in equation (19):

$$p_f(t, y_0, u(.)) = \sum_{\tau=0}^{t} \mathbb{P}(t_{out} = \tau) \tag{27}$$

Applying the latter equation at dates t and $t-1$ directly leads to:

$$\mathbb{P}(t_{out} = t) = p_f(t, y_0, u(.)) - p_f(t-1, y_0, u(.)) \tag{28}$$

If we note $\Delta(t)$ the amount of time between dates t and $t+1$, then $\mathbb{P}(t_{out} = t)/\Delta(t)$ is an approximation of the rate of the first outcrossing. Computation of the probability of failure $p_f(t, y_0, u(.))$ for $t < T$ and a fixed maintenance strategy $u(.)$ can be achieved both by backward and forward programming, and both methods are presented in Appendix B.

5 Application

In this Section we apply the dynamic programming techniques from Section 4.4 to a simple dynamical model of controlled population growth. The aim through this is to demonstrate that 1) despite the apparent simplicity of the equations, complex control strategies can and may have to be devised, and 2) that dynamic programming is adequate to do so. The reader should keep in mind that this application does not intend to showcase that dynamic programming is more precise or less computationally demanding than other techniques in time-variant reliability; yet, these techniques are not meant to find appropriate maintenance strategies. This Section also intends to show that dynamic programming also applies to the case, classical in time-variant reliability, of a performance function that decreases with time, and it uses the results from Section 4.5 to compute the outcrossing rate.

5.1 A simple population model

We consider a modified version of a simple model of population growth introduced by Aubin and Saint-Pierre (2002). It is discretized and uncertainty is integrated as an additive term to the population variable at each time step. All quantities being non dimensional for simplicity, the evolution of the state $x = (a, b)$ reads:

$$\left\{ \begin{array}{lcl} a(t+1) & = & a(t) + (a(t)b(t) + w(t))\Delta t \\ b(t+1) & = & b(t) + u(t, a(t), b(t)) \end{array} \right. \tag{29}$$

This is the full information case from Section 4.1. The initial state x_0 represents the system's design, so we can write $\pi = x_0 = (a_0, b_0)$. Since neither the dynamic nor the state vector depend explicitly on x_0, equation (29) is under the form $x(t+1) = f(t, x(t), u(t, x(t)), w(t))$ like in equation (16). Therefore, dynamic programming and other computations can be carried out using $y(t) = x(t)$, and we shall keep the notation $x(t)$ instead $y(t)$ throughout this section.

The state variables are the population $a(t)$ and its growth coefficient $b(t)$. The time interval between two consecutive dates is constant at $\Delta t = 1$. The state variable $b(t)$ is controlled by a unique control variable $u(t, x(t))$. The feedback rule, that is, the control to be associated to each state, is to be determined in order to maximize the system's reliability. The control space is $U = [U_{\min}, U_{\max}]$ and represents the inertia in the evolution of the population. These bounds are taken to be $U_{\min} = -0.5$ and $U_{\max} = 0.5$.

The uncertainty $w(t)$ is a realization of a Gaussian random variable $\mathbf{W}(t)$ of mean 0 and standard deviation 0.25. In the same way as in Section 4.4, we are in the Markovian case, so that the Gaussian random variables $\mathbf{W}(t_1)$ and $\mathbf{W}(t_2)$ at two different dates t_1 and t_2 are statistically independent. In fact, the term $w(t).\Delta t$ from equation (29) reflects in discrete time the hypothesis that in continuous time, the state variable $a(t)$ is disturbed by a white noise process.

The size of the population is constrained, so that the survival set is represented by the following performance function:

$$g(t, x(t)) = g(t, a(t), b(t)) = (a(t) - 0.2)(c(t) - a(t)) \tag{30}$$

so that the survival set is defined by $a(t) \in [0.2, c(t)]$ where $c(t)$ is the carrying capacity of the system ($c(t) \geq 0.2$). In ecology, the carrying capacity is the maximal size of the population that can be sustained by the environment it lives in. For a given expression of $g(t, x(t))$ in equation (30), the design problem is related to assessing reliability at a time horizon T for a given initial state x_0. Since reliability also depends on the way the system is subsequently controlled – or maintained – this problem is a design and maintenance problem as described in Section 3.2.

In this study, the state space has been discretized, with resolutions $\Delta a = 0.01$ and $\Delta b = 0.05$, and the control space is likewise discretized with a resolution $\Delta u = 0.05$. In this discrete space, the transition function between two time steps was obtained by interpolating from equation (29). In what follows, the relevant range for b was found to be $[-1.5, 2.5]$.

5.2 Constant carrying capacity

Let us assume that the carrying capacity is constant at $c = 3$. Then, the performance function from equation (30) is under the following form g_1:

$$g_1(t, x(t)) = (a(t) - 0.2)(3 - a(t)) \tag{31}$$

Dynamic programming leads to the strategy $u(.)$ that optimizes reliability at any horizon, and the only approximation is that of the discretization. This is showcased for $T = 100$ by Figure 1, which shows that only initial states grouped around $b_0 = 0$ have a good reliability. There is, however, a sizable reliability kernel $\mathrm{Rel}(0.95, 100)$, which shows which initial states – or which system designs – lead to the lowest probability of failure. Such reliability kernels can also be computed at any horizon, which allows for observing the evolution of $\mathrm{Rel}(0.95, T)$ as T increases. Its size decreases very little until it abruptly ceases to exist when T tops 254 (Figure 2).

This stability of the reliability kernel $\mathrm{Rel}(0.95, T)$ as the horizon increases is matched by that of the optimal strategy. Whatever the horizon, the backward sequence of feedback maps $x \mapsto u(t, x)$ from the final date T to the initial date is the same, and what is more, the map becomes constant for $t \leq T - 10$. It is noted u^* and represented on Figure 3. For a given value of a, the value of u^* increases as b increases. Yet the relationship between u^* and b is different for each single value of a, so that the

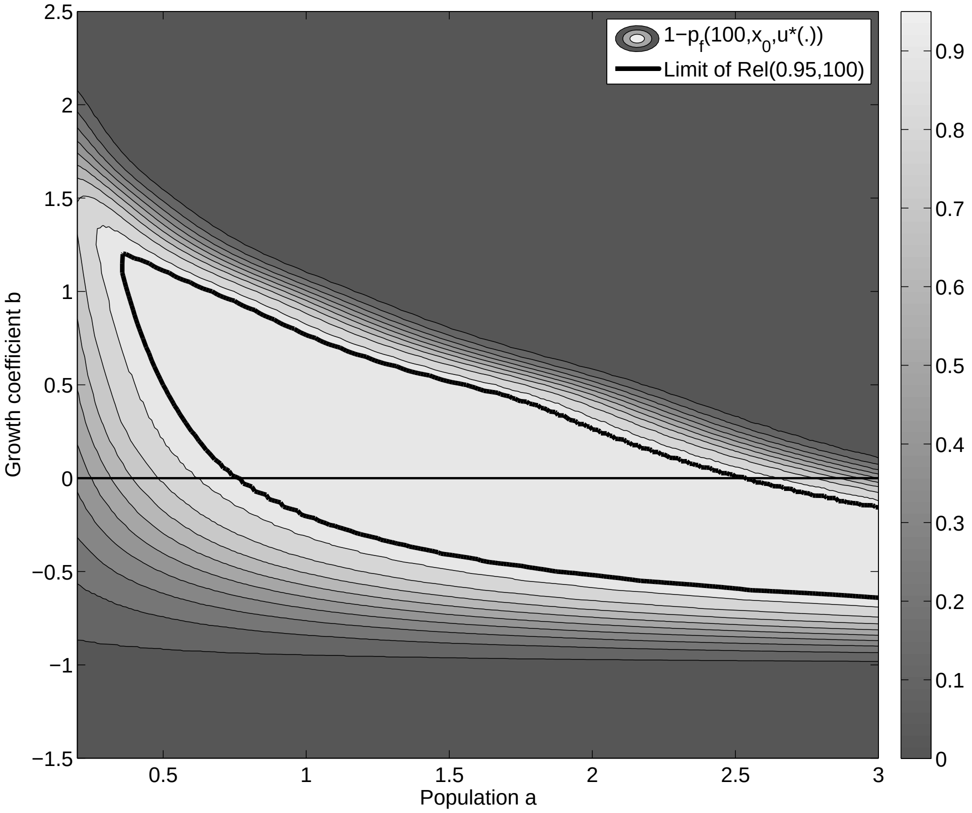

Figure 1: Reliability with the performance function g_1 and a time horizon of a hundred time steps.

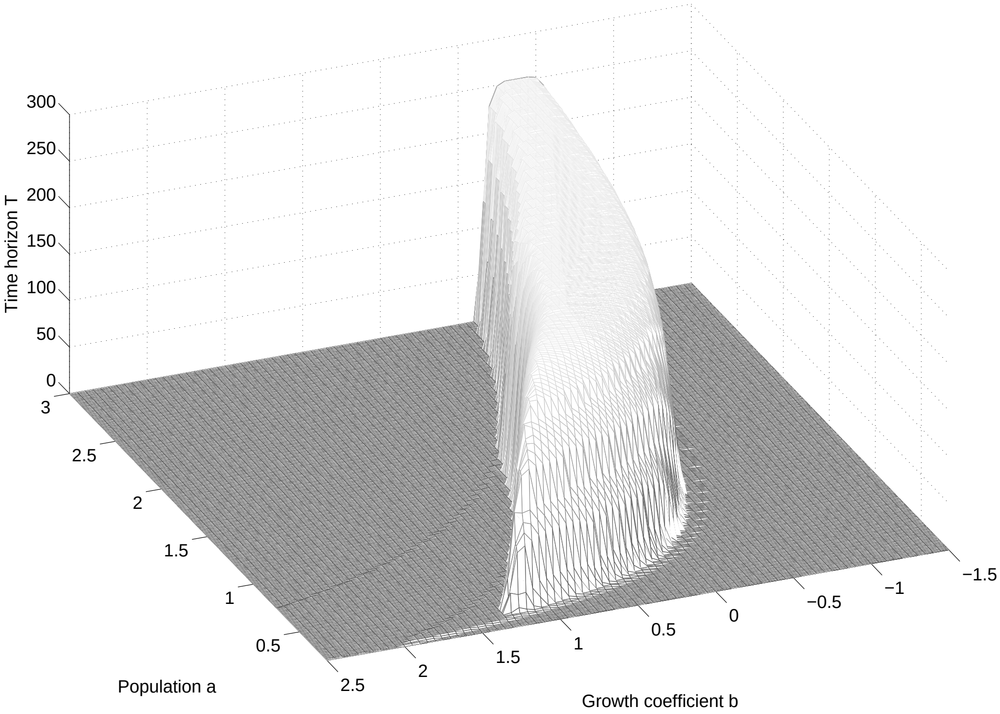

Figure 2: Initial states x_0 belonging to $\mathrm{Rel}(0.95, T)$, for different values of the horizon T and the performance function g_1.

map is very complex. This map has been obtained through the use of dynamic programming, and it is important to recall that usual time-variant reliability kernel are not devised to yield such complex maintenance strategies.

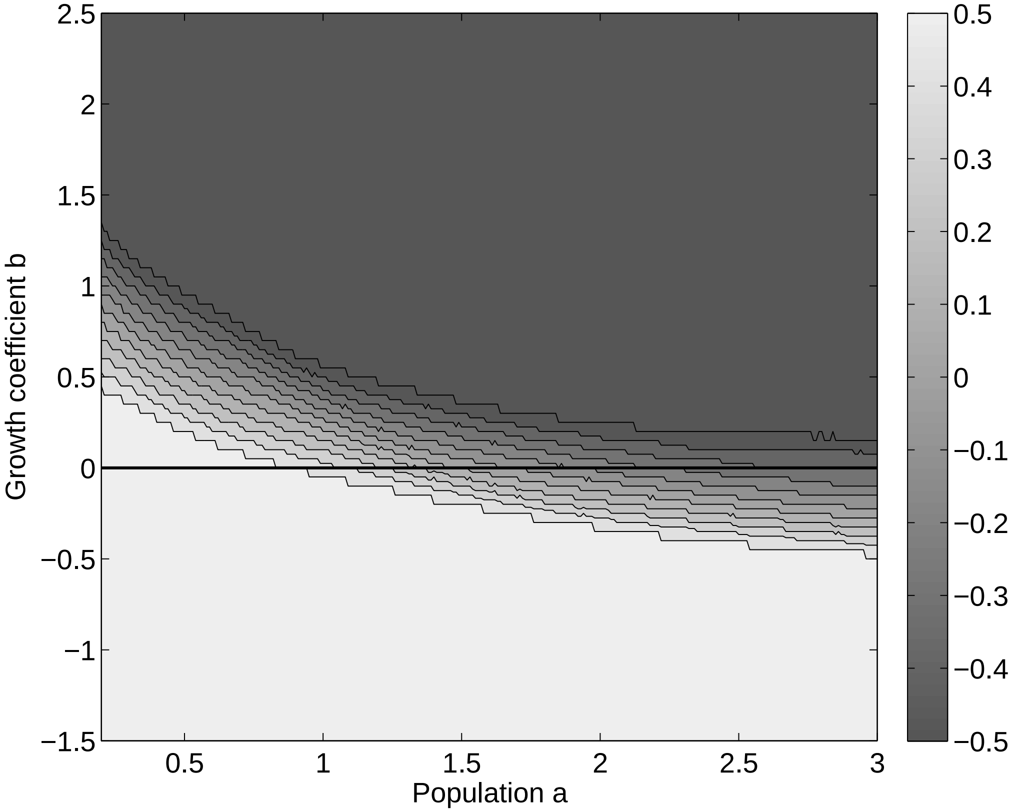

Figure 3: Map of the optimal controls $u^*(x)$ for the performance function g_1, 10 time steps or more from the horizon.

Outcrossing rates as approximated by $\mathbb{P}(t_{out} = t)/\Delta t$ can be estimated using this feedback map. Since $\Delta t = 1$, using equation (28) the outcrossing rate takes the approximate value of $(\lambda(1-p_f(t, x_0, u^*(.)))$ after less than 10 time steps, where $\lambda \approx 2 \times 10^{-4}$ is the probability of leaving at t conditional on staying in the survival set up to $t-1$. λ is independent on the initial state, so that the differences in reliability displayed in Figure 1 account for the probability of leaving the survival set within these first ten time steps. After $t = 10$, the probability of failure increases very slowly.

5.3 Decreasing carrying capacity

Let us now suppose that the system performance decreases over time. We choose a simple model of linear decrease from Savage and Son (2011) with a diminishing carrying capacity $c(t) = 3 - 0.01t$. Let us note this function g_2, equation (30) becomes:

$$g_2(t, x(t)) = (a(t) - 0.2)(3 - 0.01t - a(t)) \tag{32}$$

As expected, this linear decrease in performance affects reliability, so that $\mathrm{Rel}(0.95, T)$, even though it assumes a similar shape as for g_1, vanishes for $T > 54$ (Figure 4). Besides, unlike for the case of a constant carrying capacity, the optimal control maps change at each time step. This would make them very difficult to find if it were not for dynamic programming.

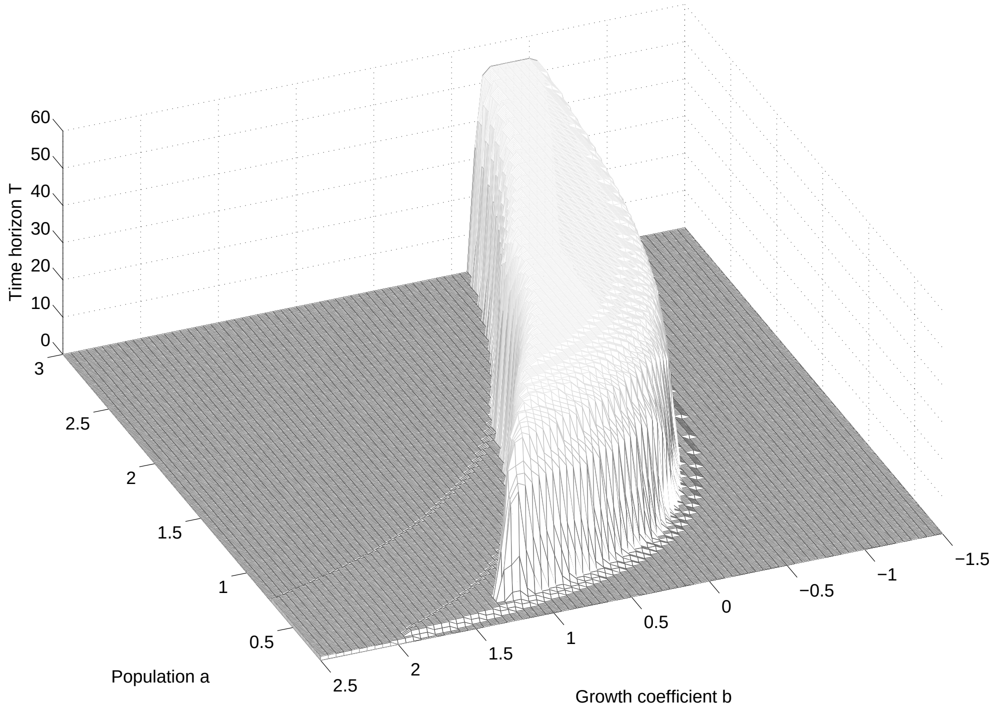

Figure 4: Initial states x_0 belonging to $\mathrm{Rel}(0.95, T)$, for different values of the horizon T and the performance function g_2.

Yet, for $t \leq T - 10$ it seems that the map $u^*(t, .)$ does not depend on the horizon T. Thus, the maps for $T = 100$ and $T = 200$ are identical until the date $t = 92$, while those for $T = 150$ and $T = 200$ are identical until $t = 145$. This makes the computation of the outcrossing rates values computed with the optimal strategy for $T = 200$ applicable to lower time horizons. No matter the initial state, the outcrossing rate is low after the first ten time steps then gradually increases to peak at $t = 124$ (Figure 5). Then, it decreases because the decreasing quantity $(1 - p_f(t, x_0, u^*(.))$ in equation (28) compensates the growth of the probability of leaving the survival set at t conditional on staying in it until $t - 1$. Like for the previous case, the amplitude of the outcrossing rate after $t = 10$ depends on the odds of leaving the survival set within the first few time steps. The cumulative probability of failure through time can be computed alongside the outcrossing rate (Figure 6).

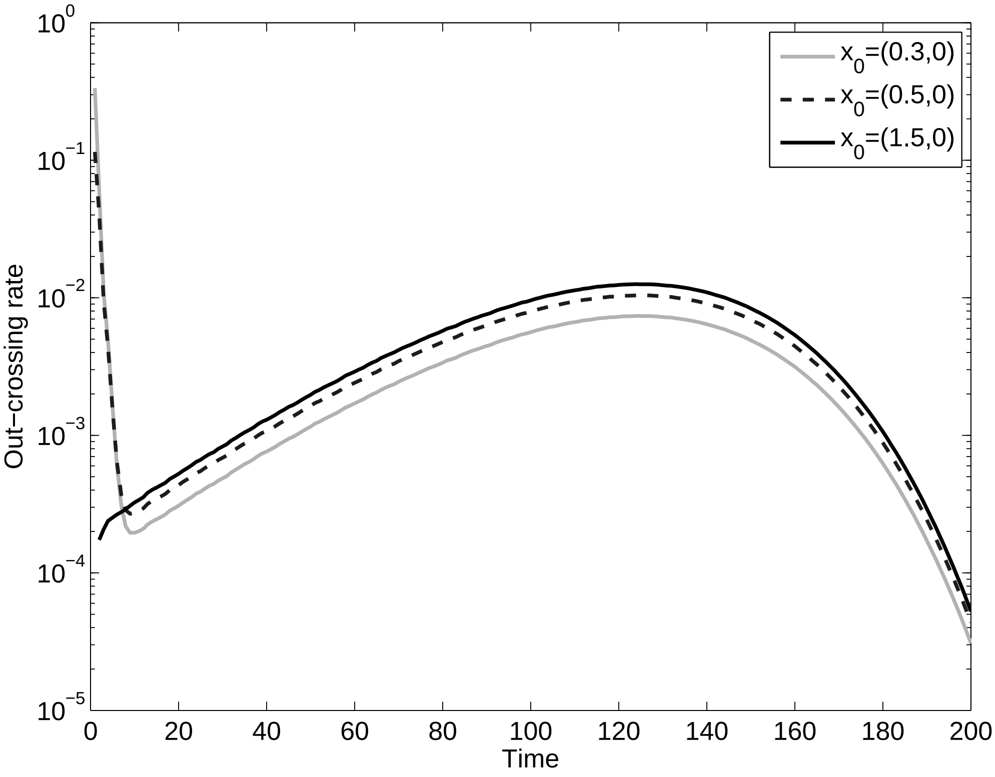

Figure 5: Evolution of the outcrossing rate under the performance function g_2.

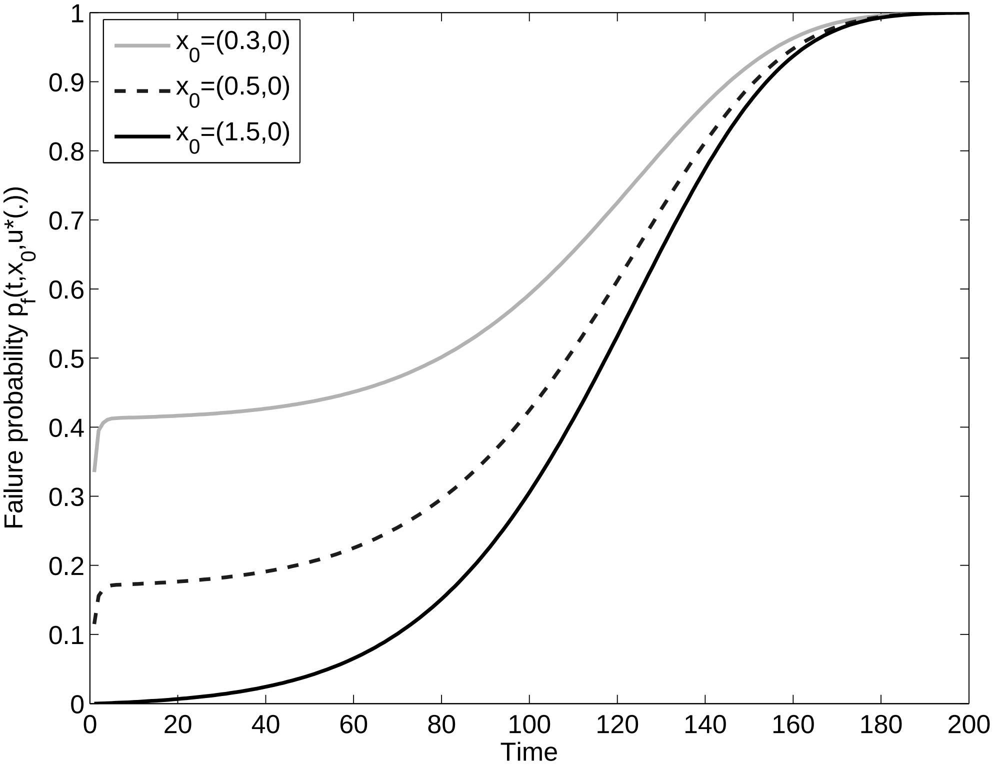

Figure 6: Evolution of the probability of failure under the performance function g_2.

6 Discussion

The limitations of dynamic programming algorithms should be kept in mind. In practice, they can only solve systems which state space has a low dimension. Too high a dimension leads to the so-called "curse of dimensionality" which designates the exponential increase of the needed computational time and memory. There exist approximation and decomposition algorithms that have been used to deal with the dimension problem in dynamic programming, such as the Benders decomposition (Perreira and Pinto, 1985) or dual approximations, e.g. Shapiro (2011), but their applicability lies well outside the scope of this work.

Yet, the confrontation of reliability with control theory looks very promising. In this paper, it led to the formal definition of coupled design and maintenance problems without restrictive hypotheses on the aging of the system with time, nor on the effects of maintenance. While stochastic viability was used, other branches of control theory may be relevant to such design and maintenance problems, both in the closed- and open-loop cases. In fact some works are very close to viability theory, such as the invariance framework (Clarke et al., 1995) or reach-avoid problems in probabilistic hybrid systems, e.g. Abate et al. (2008), Summers and Lygeros (2010). They may help in the formulation and / or the resolution of time-variant reliability problems. Conversely, reliability may be instrumental in solving control problems. For instance, it is necessary to know $\mathbb{P}(\mathbf{X}(t, y(t)) \in S(t))$ in viability problems, but this knowledge may not be easy to get. Time-invariant reliability methods may then provide efficient approximations of these probabilities.

The interest of the confrontation of reliability and viability does not stop with the potential methodological developments. Both theories, since they tackle very similar performance problems, have been used in fields concerned with environmental and resources management. Thus, reliability theory has been used for more than three decades for water resources systems, following the pioneering work by Hashimoto et al. (1982) later completed by Moy et al. (1986) and Kundzewicz and Laski (1995). It has also been used in groundwater management, be it for water quantity (Oviedo-Salcedo, 2012) or quality (Skaggs and Barry, 1997) issues. In ecology, the definition of ecosystem failure byNaeem (1998) has fostered discussions on the link between species redundancy and ecosystem reliability (Naeem and Li, 1997; Rastetter et al., 1999). The goal is to assess whether the performance of the system is consistent or satisfactory over a given time frame, which can be expressed in terms of whether and how reliability may reach or best a threshold value. The stochastic viability framework, which uses the word of viability instead of reliability, has tackled the same type of performance problem for fishery management (Doyen et al., 2007; De Lara and Martinet, 2009; Doyen et al., 2012), with an emphasis on finding management options that maintain both the fish stocks and economic benefits from fishing. Viability has also be used for the aptly named population viability analysis (De Lara and Doyen, 2008) which tries and assesses the risk that a species may go extinct. The simple example of population viability analysis from Section 5 showcases how both stochastic viability and time-variant reliability may be relevant to similar problems.

Finally, both viability and reliability have been used to explore other concepts related to the performance of a system. On the one hand, resilience has been defined as the possibility for the system to recover and get to a set of states robust to uncertainty after a major event dragged it into the failure set, this robust set being the stochastic viability kernel (Rougé et al., 2013). In the same work, stochastic viability methods such as dynamic programming are used to compute the probability of reaching a given stochastic viability kernel within a given time frame after an event. On the other hand, resilience but also vulnerability have been defined alongside reliability as performance indicators for water resources systems (Hashimoto et al., 1982) and further, a method computing all three concepts using FORM also exists (Maier et al., 2001). Thus, bringing viability and reliability methods together may improve the definition and computation of other related concepts such as resilience and vulnerability.

7 Conclusion

Stochastic viability and reliability have the same broad goal of computing the probability for a system to not violate its constraints. This work used stochastic viability to propose new concepts and methods in time-variant reliability.

Conceptually, similarities between stochastic viability and reliability led to the definition of the reliability kernel to deal with design problems: this is an analog of the stochastic viability kernel. Viability being a branch of control theory, the notion of reliability kernel has been extended to cases where both the design and maintenance of the system have to be considered together. This kernel then regroups the possible designs such that the system can be maintained in the survival set with a high probability and for a sufficient amount of time. Besides, its definition relies on a formulation that is independent from the assumption of a monotonic decrease in performance over time, even though the application shows that the framework is well-suited to tackle these cases as well.

As for the method, dynamic programming is applicable to time-variant reliability in the specific cases in which a design and maintenance problem is also a stochastic viability problem, namely when the uncertainty and stochasticity of the system can be summarized at discrete dates by a vector called the state vector, and when the search of the design is related to that of the initial state. If the uncertainty can be expressed by independent random variables, then dynamic programming yields both the reliable designs and the adequate maintenance strategy for these designs.

Acknowledgements

This work has been supported by a Région Auvergne's scholarship. The authors also want to thank an anonymous reviewer, whose constructive remarks on earlier versions of this manuscript considerably improved its content.

A Background on viability theory

In its original deterministic version (Aubin, 1991), viability theory deals with controlled systems such that $w(t) \equiv 0$, and for which full information is available: $y(t) = (x(t), \pi)$. Equation (16) can be simplified into:

$$y(t+1) = f(t, y(t), u(t)) \tag{33}$$

In this framework, a trajectory is defined by an initial state y_0 and a strategy $u(.)$, so the state can be noted $y(t, y_0, u(.))$. The central question of viability is whether that trajectory leaves a survival set $S(t)$, at any given date within the time frame $[0, T]$. An answer to this question is brought about by a central object, the viability kernel, which is the set of all initial states for which the system can be controlled so its trajectory does not leave the survival set:

$$\mathrm{Viab}(T) = \{y_0 \in \mathbb{Y} | \exists u(.) \in \mathcal{U}(T), \forall t \in [0, T], y(t, y_0, u(.)) \in S(t)\} \tag{34}$$

Thus, an initial state can either be viable or not, which we can translate into reliability terms by stating that in a deterministic context, the probability of failure is either 1 when $y_0 \in$Viab(T), and 0 otherwise. Properties of the viability kernel have provided the foundation of viability algorithms. This is for instance the case for algorithms that use the binary nature of a state under deterministic viability (e.g. Saint-Pierre, 1994; Deffuant et al., 2007), or the fact that viable trajectories are tangent to the surface of the viability kernel (Bonneuil, 2006). An interest of these algorithms is that they find both the viable initial states and the associated viable controls.

B Computation of $p_f(t, y_0, u(.))$ for $t < T$ and a fixed $u(.)$

In what follows we assume a predefined value of $u(t, y)$ for each t and y.

B.1 Forward

This is done through the direct computation of the possible trajectories $x(t, y_0, u(.), w(.))$ for all dates $0 < t \leq T$, as long as they do not leave the survival set. We recursively compute the value function $V_1(t, y_0, u(.), y_k)$:

$$V_1(t, y_0, u(.), y_k) = \mathbb{P}\left(\{y(t, y_0, u(.), w(.)) = y_k\} \cap \left\{\forall \tau < t, \mathbf{X}\left(t, \pi\right) \in S(\tau) | y_), u(.)\right\}\right) \tag{35}$$

The value function V_1 gives the probability of transitioning from y_0 at the initial date to y_k at date t, while keeping the system in the survival set. In other words, we have:

$$p_f(t, y_0, u(.)) = 1 - \sum_{y_k \in \mathbb{Y}} V_1(t, y_0, u(.), y_k) \tag{36}$$

The value function V_1 is computed through a forward iterative scheme. Initialization reads:

$$V_1(0, y_0, u(.), y_k) = \begin{cases} \mathbb{P}\left(\mathbf{X}(0, \pi) \in S(0) | y_0\right) & \text{if} \quad y_0 = y_k \\ 0 & \text{if} \quad y_0 \neq y_k \end{cases} \tag{37}$$

then the function V_1 is recursively updated at each date $1 \leq t \leq T$:

$$V_1(t, y_0, u(.), y_k) = \left(\sum_{y_i \in \mathbb{Y}} V_1(t-1, y_0, u(.), y_i).\mathbb{P}(f(t-1, y_i, u(t-1, y_i), w(t-1)) = y_k) \right) \\ .\mathbb{P}(\mathbf{X}(t, \pi) \in S(t) | y_k) \tag{38}$$

The advantage of using the above approach is that it yields the failure probabilities at all dates recursively, in a single run. The inconvenient lies with the large amount of computational memory it requires, since it connects all the points of the successive survival sets with each other.

B.2 Backward

Let us introduce a value function V_2 to compute the probability of not failing between the initial date and set a date $t \in [0, T]$. V_2 is to be computed recursively backwards from t to 0. It is initialized through:

$$V_2(t, y_i) = \mathbb{P}(\mathbf{X}(t, \pi) \in S(t) | y_i) \tag{39}$$

and then for $\tau \in [0, \tau[$, the backward transition equation reads:

$$V_2(\tau, y_i) = \left(\sum_{y_k \in \mathbb{Y}} \mathbb{P}(f(t, y_i, u(\tau, y_i), w(\tau)) = y_k).V_2(\tau + 1, y_k) \right).\mathbb{P}(\mathbf{X}(\tau, \pi) \in S(\tau) | y_i) \tag{40}$$

These equations are exact analogous to equations (24) and (25) for the value function V, where there is only one possible control $u(\tau, y_i)$ at each date τ and state y_i. Thus, equation (26) becomes $V_2(0, y_i) = 1 - p_f(t, y_0, u(.))$. This is less expensive than the algorithm for V since there is no need to solve an optimization problem at each date and state to get the feedbacks. However, it is necessary to run this algorithm for each date separately so as to get the probability of failure at multiple dates.

References

Abate, A., Prandini, M., Lygeros, J., Sastry, S., 2008. Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica 44, 2724–2734.

Aliev, T.A., Kartvelishvili, L.N., 1993. Principles of evaluating the ecological reliability of irrigation systems. Hydrotechnical Construction 27, 297–304.

Andrieu-Renaud, C., Sudret, B., Lemaire, M., 2004. The phi2 method: A way to compute time-variant reliability. RESS 84, 75–86.

Aubin, J.P., 1991. Viability Theory. Birkhäuser.

Aubin, J.P., Bayen, A., Saint-Pierre, P., 2011. Viability Theory. Regulation of Uncertain Systems. Springer-Verlag.

Aubin, J.P., Saint-Pierre, P., 2002. An introduction to viability theory and management of renewable resources, in: Coupling Climate and Economic Dynamics. Springer, pp. 55–96.

Biondini, F., Frangopol, D.M., 2009. Lifetime reliability-based optimization of reinforced concrete cross-sections under corrosion. Struct. Saf. 31, 483–489.

Bonneuil, N., 2006. Computing the viability kernel in large state dimension. J. Math. Anal. Appl. 323, 1444–1454.

Burgazzi, L., 2008. About time-variant reliability analysis with reference to passive systems assessment. RESS 93, 1682–1688.

Clarke, F.H., Ledyaev, Y.S., Stern, R.J., Wolenski, P.R., 1995. Qualitative properties of trajectories of control systems: a survey. Journal of Dynamical and Control Systems 1, 1–48.

De Lara, M., Doyen, L., 2008. Sustainable Management of Natural Resources. Springer.

De Lara, M., Martinet, V., 2009. Multi-criteria dynamic decision under uncertainty: A stochastic viability analysis and an application to sustainable fishery management. Math. Biosci. 217, 118–124.

Deffuant, G., Chapel, L., Martin, S., 2007. Approximating viability kernel with support vector machines. IEEE T. Automat. Contr. 52, 933–937.

Deffuant, G., Gilbert, N. (Eds.), 2011. Viability and resilience of complex systems. Kluwer Academic Publishers, London.

Ditlevsen, O., Madsen, H.O., 1996. Structural Reliability Methods. John Wiley & Sons, Chichester.

Doyen, L., De Lara, M., 2010. Stochastic viability and dynamic programming. Syst. Control Lett. 59, 629–634.

Doyen, L., Lara, M.D., Ferraris, J., Pelletier, D., 2007. Sustainability of exploited marine ecosystems through protected areas: A viability model and a coral reef case study. Ecol. Model. 208, 353–366.

Doyen, L., Thébaud, O., Béné, C., Martinet, V., Gourguet, S., Bertignac, M., Fifas, S., Blanchard, F., 2012. A stochastic viability approach to ecosystem-based fisheries management. Ecol. Econ. 75, 32–42.

Guedes Soares, C., Garbatov, Y., 1998. Reliability of maintained ship hull girders subjected to corrosion and fatigue. Struct. Saf. 20, 201–219.

Hagen, O., Tvedt, L., 1991. Vector process out-crossing as parallel system sensitivity measure. J. Eng. Mech. 117, 2201–2220.

Hashimoto, T., Stedinger, J., Loucks, D., 1982. Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation. Water Resour. Res. 18, 14–20.

Hsiao, E., Schuster, M., Juang, C., Kung, G., 2008. Reliability analysis and updating of excavation-induced ground settlement for building serviceability assessment. J. Geotech. Geoenviron. Eng. 134, 1448–1458.

Kundzewicz, Z., Laski, A., 1995. Reliability-related criteria in water supply studies. In: New Uncertainties Concepts in Hydrology and Water Resources. Cambridge University Press, Cambridge, UK.

Kuschel, N., Rackwitz, R., 2000. Optimal design under time-variant reliability constraints. RESS 22, 113–127.

Lemaire, M., 2009. Structural Reliability. John Wiley & Sons, New York.

Li, C., Der Kiureghian, A., 1995. Mean out-crossing rate of nonlinear response to stochastic input, in: Lemaire, M., Favre, J., Mébarki, A. (Eds.), Proceedings of the International Conference on the Application of Statistics and Probability (ICASP7), pp. 295–302.

Maier, H.R., Lence, B.J., Tolson, B.A., Foschi, R.O., 2001. First-order reliability method for estimating reliability, vulnerability, and resilience. Water Resour. Res. 37, 779–790.

Mathias, J.D., Lemaire, M., 2012. Reliability analysis of bonded joints with variations in adhesive thickness. J. Adhes. Sci. Technol. , 1–11.

Melching, C.S., 1992. An improved first-order reliability approach for assessing uncertainties in hydrologic modeling. J. Hydrol. 132, 157–177.

Moy, W., Cohon, J., ReVelle, C., 1986. A programming model for analysis of the reliability, resilience, and vulnerability of a water supply reservoir. Water Resour. Res. 22, 489–498.

Naeem, S., 1998. Species redundancy and ecosystem reliability. Conserv. Biol. 12, 39–45.

Naeem, S., Li, S., 1997. Biodiversity enhances ecosystem reliability. Nature 390, 507–509.

Oviedo-Salcedo, D.M., 2012. Accounting for parameter uncertainty and temporal variability in coupled groundwater-surface water models using component and systems reliability analysis. Ph.D. thesis. University of Illinois at Urbana-Champaign.

Perreira, M.V.F., Pinto, L.M.V.G., 1985. Stochastic optimization of a multireservoir hydroelectric system: a decomposition approach. Water Resour. Res. 21, 779–792.

Petryna, Y.S., Pfanner, D., Stangenberg, F., Krätzig, W.B., 2002. Reliability of reinforced concrete structures under fatigue. RESS 77, 253–261.

Quigley, J., Walls, L., 2011. Mixing Bayes and empirical Bayes inference to anticipate the realization of engineering concerns about variant system designs. RESS 96, 933–941.

Rackwitz, R., 2001. Reliability analysis – a review and some perspectives. Struct. Saf. 23, 365–395.

Rastetter, E.B., Gough, L., Hartley, A.E., Herbert, D.A., Nadelhoffer, K.J., Williams, M., 1999. A revised assessment of species redundancy and ecosystem reliabilityauthor. Conserv. Biol. 13, 440–443.

Rausand, M., 1998. Reliability centered maintenance. RESS 60, 121–132.

Rice, S.O., 1944. Mathematical analysis of random noise. Bell System Tech. J. 23, 282–332.

Rougé, C., Mathias, J.D., Deffuant, G., 2013. Extending the viability theory framework of resilience to uncertain dynamics, and application to lake eutrophication. Ecol. Indic. 29, 420–433.

Saint-Pierre, P., 1994. Approximation of the viability kernel. Appl. Math. Opt. 29, 187–209.

Savage, G.J., Son, Y.K., 2011. The set-theory method for systems reliability of structures with degrading components. RESS 96, 108–116.

Schotanus, M.I.J., Franchin, P., Lupoi, A., Pinto, P.E., 2004. Seismic fragility analysis of 3d structures. Struct. Saf. 26, 421–441.

Shapiro, A., 2011. Analysis of stochastic dual dynamic programming method. Eur. J. Oper. Res. 209, 63–72.

Skaggs, T.H., Barry, D.A., 1997. The first-order reliability method of predicting cumulative mass flux in heterogeneous porous formations. Water Resour. Res. 33, 1485–1494.

Sørensen, J.D., Svensson, S., Stang, B.D., 2005. Reliability-based calibration of load duration factors for timber structures. Struct. Saf. 27, 153–169.

Sudret, B., 2008a. Analytical derivation of the outcrossing rate in time-variant reliability problems. Struct. Infrastruct. Eng. 4, 353–362.

Sudret, B., 2008b. Probabilistic models for the extent of damage in degrading reinforced concrete structures. RESS 93, 410–422.

Sudret, B., Defaux, G., Pendola, M., 2005. Time-variant finite element reliability analysis – application to the durability of cooling towers. Struct. Saf. 27, 93–112.

Summers, S., Lygeros, J., 2010. Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem. Automatica 49, 1951–1961.

Targoutzidis, A., 2012. A monte carlo simulation for the assessment of bayesian updating in dynamic systems. RESS 100, 125–132.

Val, D.V., Stewart, M.G., 2003. Life-cycle cost analysis of reinforced concrete structures in marine environments. Struct. Saf. 25, 343–362.

Wang, Z., Wang, P., 2013. A new approach for reliability analysis with time-variant performance characteristics. RESS 115, 70–81.