P-Safety and Stability

Bujorianu, Manuela L.; Wisniewski, Rafael; Bouloughouris, Evangelos

Published in:
IFAC-PapersOnLine

DOI (link to publication from Publisher):
10.1016/j.ifacol.2021.06.127

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 54-9 (2021) 665–670

p-Safety and Stability

Manuela L. Bujorianu * **Rafael Wisniewski** **
Evangelos Boulougouris *

* *Maritime Safety Research Center, Department of Naval Architecture, Ocean & Marine Engineering, University of Strathclyde, Scotland, UK (e-mail: luminita.bujorianu, evangelos.boulougouris@strath.ac.uk),*
** *Section of Automation & Control, Aalborg University, 9220 Aalborg East, Denmark (e-mail: raf@es.aau.dk)*

,

Abstract: This paper focuses on the formal integration of stability and safety of complex systems. We present the initial developments of a holistic modelling framework, which will be flexible enough to allow us to formulate the integration of safety and stability problems and the design of decision and control algorithms for the maintenance of the appropriate levels of safety and stability required by the system specifications.

Keywords: p-Safety, stability, Markov models, transition semigroup, Green kernel, barrier certificates.

1. INTRODUCTION

We present an approach to ensure safety and stability properties of stochastic systems. Usually, the analyses of both properties are performed in isolation. In this work, we consider analyzing both properties in a single integrative framework. Safety verification is an instrument of analyzing whether a system works according to its requirements. A system is called to be safe if it does not violate any system constraints, i.e., if some dangerous states cannot be reached. The concept of stability has many facets: local/global stability, asymptotic/exponential stability, strong/weak stability, and so on. For dynamical systems, the concept of stability focuses on equilibrium points and is addressed mostly using Lyapunov functions. For a controlled stochastic system, one should expect that the trajectories starting from some region around an equilibrium point converge to it. Alternatively, a set for which arbitrarily small surrounding regions are invariant (or at least viable) is a good candidate for stability. Therefore, the issue of stability may be addressed via invariance/viability techniques. In this paper, we define stability as an invariance property of an initial set of states. Both safety and stability properties are characterized using stochastic barrier certificates. We continue the research line initiated in Bujorianu and Wisniewski (2019) and Wisniewski and Bujorianu (2017), and introduce safety and stability concepts up to a probability threshold p.

The main novelty developed in this paper is that our stochastic barrier functions are now defined as potentials of measures, i.e., integrals of the Green function with respect to probability measures. Historically, Greens original work was conducted with reference to the solution of electrostatic problems in bounded regions. In this context, the Green function $g(r, r')$ is the potential at the point r produced by a unit point charge at r'. For Markovian processes, the Green function appears in the characterization of the solutions of the partial differential equations associated to the infinitesimal generator of the process (Laplace operator for the Brownian motion). In this context, the Green function is the density of the Green operator/kernel, which is in some sense the inverse of the generator. For a Markov chain, $g(r, r')$ can be interpreted as the number of chain visits to the state r' starting with the state r. For a continuous space Markov process, the Green kernel is interpreted as an occupation kernel. In the stochastic framework, the importance of the Green function is coming from the connection between the solutions of electrostatic problems and the hitting/reachability problem for Markov processes Doob (2001). Since our safety/stability concepts are defined in terms of reachability/invariance problem, the use of Green function is natural. The integration of the Green function with respect to a probability measure gives rise to the concept of Green potential, which is the perfect way to build up barrier certificates. Moreover, Green potentials represent a special class of stochastic Lyapunov functions and therefore the connection with dynamical systems is clear (see Hmissi (1989), for potential concepts for deterministic dynamical systems).

2. MARKOV MODELS

In this paper, we will consider a special class of Markov processes, namely (Borel) right processes Bujorianu (2012) $(X_t) := (X_t)_{t\geq 0}$ on the underlying probability space $(\Omega, \mathcal{F}, \mathbb{P})$ with values in a Borel space $\mathcal{Y}$ [1]. We associate a family of probabilities $(\mathbb{P}^y) := (\mathbb{P}^y)_{y\in\mathcal{Y}}$ with the property $\mathbb{P}^y[X_0 = y] = 1$; they are called *Wiener probabilities*. The expectation with respect to $\mathbb{P}^y$ is denoted $\mathbb{E}^y$. To $(\mathbb{P}^y)$, we associate a family of transition probabilities $(p_t) := (p_t)_{t\leq 0}$

⋆ The first and the third author wish to acknowledge and thank for the financial support from MSRC research sponsors DNVGL and Royal Caribbean Cruise Ltd.

[1] $\mathcal{Y}$ is a Borel subset of a complete separable metric space.

10.1016/j.ifacol.2021.06.127

with $p_t(y, A) = \mathbb{P}^y[X_t \in A]$. The action of (p_t) on the Banach space $\mathcal{B}_b(\mathcal{Y})$ of bounded measurable real-valued functions $f : \mathcal{Y} \to \mathbb{R}$ is defined by

$$P_t f(y) = \mathbb{E}^y f(X_t) = \int_{\mathcal{Y}} f(x) p_t(y, dx).$$

The *operator resolvent* $\mathcal{G} = (G_\alpha)_{\alpha \geq 0}$ *associated with* P_t *is* its Laplace transform, i.e.,

$$G_\alpha f(y) = \int_0^\infty e^{-\alpha t} P_t f(y) dt,\ y \in \mathcal{Y}.$$

Let G denote the initial operator G_0 of $\mathcal{G}$, which is known as the *kernel/occupation/Green operator* of the Markov process. This kernel records the number of times the underlying Markov process visits any measurable set.

Associated with the semigroup (P_t) is its *infinitesimal generator* which, loosely speaking, is the derivative of P_t at $t = 0$. Let $D(L) \subset \mathcal{B}_b(\mathcal{Y})$ be the set of functions f for which the following limit exists $\lim_{t \searrow 0} \frac{1}{t}(P_t f - f)$, and denote this limit Lf. The limit refers to convergence in the sup-norm $\|\cdot\|$ of the Banach space $\mathcal{B}_b(\mathcal{Y})$. For a measurable set B, τ_B, *the first hitting time* associated to this set is

$$\tau_B := \inf\{t > 0 | X_t \in B\};$$

whereas, *the first exit time* from B is $\zeta_B = \tau_{\mathcal{Y} \setminus B}$ (i.e., the first hitting time of the complement of B).

A non-negative function f is *excessive* (see Davis (1993)) if the following two conditions are satisfied: (1) $p_t f \leq f$ for all $t \geq 0$, and (2) $\lim_{t \searrow 0} p_t f = f$. The excessive functions, called sometimes *superharmonic functions*, play the role of Lyapunov functions for stochastic processes.

3. SAFETY AND STABILITY CONCEPTS

Suppose that (X_t) is a Markov process with the transition probability function $(p_t)_{t \geq 0}$ and state space $\mathcal{Y}$. Let us consider the first exit time ζ_S from $S \in \mathcal{B}(\mathcal{Y})$, with S bounded. Since this is a stopping time, we have the following decomposition of the kernel operator:

$$Gf(y) = \mathbb{E}^y \int_0^{\zeta_S} f(X_t) dt + \mathbf{P}_{\zeta_S} Gf(y), \tag{1}$$

where $\mathbf{P}_{\zeta_S}$ is the hitting distribution corresponding to ζ_S. The first term in this decomposition is called *occupation kernel, or Green kernel* for S, i.e.,

$$G^S f(y) := \mathbb{E}^y \int_0^{\zeta_S} f(X_t) dt. \tag{2}$$

The following hypothesis will be in force for the remainder of this paper.

Hypothesis 1. (i) Suppose that the kernel G^S has a density g^S with respect to a reference measure [2] ξ on $\mathcal{Y}$, i.e.,

$$G^S f(y) = \int_S f(z) g^S(y, z) \xi(dz). \tag{3}$$

(ii) The kernel density $g^S(y, z)$ is a lower semicontinuous (l.s.c.) function for $y \neq z$.

For the majority of Markov processes, the Green kernel is the main tool for studying the solutions of the PDEs associated to the infinitesimal generator. For example, for the Brownian motion in the Euclidean space $\mathbb{R}^d$ with $d \geq 3$, the Green function is given via the Newtonian kernel, i.e., $g(y, z) = \frac{c(d)}{||y-z||^{d-2}}$, where $c(d) = \frac{\Gamma(d/2-1)}{2\pi^{d/2}}$, and $\Gamma(x) = \int_0^\infty s^{x-1} e^{-s} ds$ is the Gamma function. For the expression of the Green function associated to Brownian motion killed after a stopping time, the interested reader can consult Morters and Peres (2010), pg. 80-81.

The Green function gives ways to express the solutions of the Dirichlet problem with different boundary values. Also, it provides a method to build some special excessive/superharmonic functions called potentials [3]. The *potential of a measure* ν on S is defined by:

$$G^S \nu(y) := \int_S g^S(y, z) \nu(dz). \tag{4}$$

We can define also the *mutual energy* of two measures μ and ν on S with respect to the Green kernel, as follows:

$$\Lambda(\mu, \nu) := \int g^S(y, z) \mu(dy) \nu(dz). \tag{5}$$

Some notations will be also in force:

$$\Lambda(y, \nu) := \int_S g^S(y, z) \nu(dz);\ \Lambda(\mu, z) := \int g^S(y, z) \mu(dy). \tag{6}$$

Obviously, $G^S \nu = \Lambda(\cdot, \nu)$. In the following, we will work with the process (X_t) killed outside of S, denoted by (X_t^S).

3.1 p-Safety

Let U be an open subset of S. We refer to the set S as the state space, and a point $y \in S$ as a state. Suppose that $\partial U \cap \partial S = \emptyset$. Then $S \setminus U$ is a closed set. For some results, we will work with the closure of U, which we will suppose to be also compact. Let $p \in (0, 1)$, thought of as a permissible probability value. A state y is p-safe if the probability that the process hits U before it leaves S is not greater than p. The above statement can be formalised using the hitting time τ_U of U, and the first exit time ζ_S from S. Let $A \subset S$ be a measurable set of initial states.

Definition 1. A process (X_t) is p-safe w.r.t. (A, U) if

$$\mathbf{P}^y[\tau_U < \zeta_S] \leq p, \forall y \in A. \tag{7}$$

Then the *safety function* is given by:

$$P(y) := P(y; U, S) = \mathbb{P}^y[\tau_U < \zeta_S]. \tag{8}$$

and it can be extended to all measurable initial sets by:

$$P(A) := P(A; U, S) = \sup_{y \in A} P(y).$$

The set of barrier functions w.r.t. U is given by:

$$\mathcal{K}_U := \{h \in \mathcal{E}_X^S |\ h \geq 1 \text{ on } U\}, \tag{9}$$

where $\mathcal{E}_X^S$ is the cone of excessive functions associated to the restricted process (X_t^S).

The following characterization theorem has been proved in Wisniewski and Bujorianu (2017).

Theorem 1. Let (X_t) be a right process. Suppose A, U, $S \in \mathcal{B}(\mathcal{Y})$, and A and U are subsets of S. Then

$$P(A; U, S) = \sup_{x \in A} \inf_{h \in \mathcal{K}_U} h(x) = \inf_{h \in \mathcal{K}_U} \sup_{x \in A} h(x).$$

[2] which is eventually the Lebesgue measure on the Euclidean space

[3] It is known that every excessive function has the so-called *Riesz decomposition* into the sum of a potential and a purely harmonic function (see Blumenthal and Getoor (1968)).

The safety function is the potential of a special measure with support in U, as follows. This is the optimal measure that minimizes a specific energy called *energy integral* associated to the Green function for the set U, i.e.,

$$I(\mu) := \Lambda(\mu, \mu), \tag{10}$$

where μ is a probability measure with support in U. Let $\mathcal{M}^1(U)$ be the set of probabilities on S with support in U. Now, associated to the class of barrier functions, we can introduce the class of *barrier measures*:

$$\mathcal{KP}_U := \{\mu \in \mathcal{M}^1(U) |\ \Lambda(y, \mu) \geq 1 \text{ for } y \in U\}. \tag{11}$$

Proposition 1. Suppose that U is an open set whose closure is compact. Then, the set of barrier measures $\mathcal{KP}_U$ is a convex metrizable compact set (in the vague topology).

Proof. The convexity of $\mathcal{KP}_U$ is trivial (it follows form linearity of Λ w.r.t. measures). First, let us prove that $\mathcal{KP}_U$ is bounded: For any $\mu \in \mathcal{KP}_U$, we have:

$$\mu(S) = \mu(U) \leq \langle \mu, 1 \rangle,$$

since μ has its support in U. Then, we have to prove that $\mathcal{KP}_U$ is closed: Let (μ_α) a generalized sequence in $\mathcal{KP}_U$ that converges in the vague topology to μ. For each $y \in U$, suppose that (f_n^y) is an increasing sequence of continuous functions with limit $g^S(y, \cdot)$. To this end, we obtain:

$$1 \leq G^S \mu_\alpha(y) = \int g^S(y, z) \mu_\alpha = \lim_n \int f_n^y(z) \mu_\alpha(dz).$$

Then

$$G^S \mu(y) \geq \lim_n \int f_n^y(z) \mu(dz) = \lim_n \lim_\alpha \int f_n^y(z) \mu_\alpha(dz),$$

and

$$G^S \mu(y) = \lim_\alpha G^S \mu_\alpha(y) \geq 1 \text{ for } y \in U.$$

Therefore, $\mu \in \mathcal{KP}_U$.

Concluding, $\mathcal{KP}_U$ is closed and bounded, so it is a compact set w.r.t. the vague topology.

In this case, based on the Krein-Millman theorem we obtain the following consequence.

Corollary 1. The set of the measures of the form

$$\sum_{k=1}^{N} a_k \nu_k,\ a_k \geq 0,\ \sum_{k=1}^{N} a_k = 1,\ \nu_k \in Ex(\mathcal{KP}_U),$$

is dense in $\mathcal{KP}_U$, where $Ex(\mathcal{KP}_U)$ is the set of the extreme points of $\mathcal{KP}_U$.

The set of potentials associated to $\mathcal{KP}_U$ will be called barrier potentials, i.e.,

$$\mathcal{P}_U := \{G^S \mu | \mu \in \mathcal{KP}_U\}.$$

Using the Hunt's theorem for potential functions Doob (2001), we can obtain a characterization of the safety function based on the Green kernel:

Proposition 2. The safety function P w.r.t. (A, U, S) can be expressed as a sweeping out of measure potentials, i.e.,

$$P(y; U, S) = \inf_{\mu \in \mathcal{KP}_U} G^S \mu(y), \forall y \in A. \tag{12}$$

Moreover, there exists a measure σ_U (with support in U), called the *equilibrium measure* of U such that

$$P(y; U, S) = G^S \sigma_U(y).$$

The proof is a consequence of the characterization of the hitting operator developed in Chung (1973). The equilibrium measure[4] is the unique measure that makes the potential $G^S \mu$ constant on U, i.e.,

$$1 = \int_U g^S(y, z) \sigma_U(dz), \forall y \in U. \tag{13}$$

The above concepts are used in the specialized literature to provide characterizations for the boundary value problems Doob (2001). They enter in the characterization of the safety function since this is also solution for the Dirichlet problem associated to the infinitesimal generator L and with boundary conditions $h = 1$ on U and $h = 0$ on S (see Bujorianu and Wisniewski (2019)).

Let $\mathcal{M}^1(A)$ be the set of probability distributions supported by A. We define the set of co-safety measures, as:

$$\mathcal{KP}_U^\top := \{\lambda \in \mathcal{M}^1(A) | \Lambda(\lambda, z) \leq 1 \text{ on } S\}. \tag{14}$$

Based on the Green kernel characterization of the safety function, we can obtain a similar result to the one described by the Theorem 1, which is, in this case, equivalent with its weaker version expressed in terms of measures. We define the *safety measure* w.r.t. an initial probability distribution λ supported by A: $\langle \lambda, P \rangle := \int_A P(y) \lambda(dy)$. For each $z \in U$, we define the *co-safety function* by:

$$P^\top(z) := \sup_{\lambda \in \mathcal{KP}_U^\top} \Lambda(\lambda, z), \forall z \in U, \tag{15}$$

which can be understood in the context of reverse process (when the trajectories are followed backwards) as the cost to bring the process from $z \in U$ to the set A. The co-safety function encapsulates information about the inverse of the sweeping problem that appears in the Prop. 2. The following theorem characterizes the largest initial measure that can be swept into the equilibrium measure of U.

Theorem 3. Let (X_t) be a right process. Let $A,\ U,\ S \in \mathcal{B}(\mathcal{Y})$, where A and U are subsets of S. Suppose that the hypothesis (1) holds. Then

$$\sup_{\lambda \in \mathcal{KP}_U^\top} \langle \lambda, P \rangle = \inf_{\mu \in \mathcal{KP}_U} \langle \mu, P^\top \rangle. \tag{16}$$

Proof. Since the Green function is l.s.c., the maps $\mu \mapsto \Lambda(y, \mu)$, $\lambda \mapsto \Lambda(\lambda, z)$ and $(\lambda, \mu) \mapsto \Lambda(\lambda, \mu)$ are also l.s.c. on the corresponding cones of measures equipped with their vague topology. In Fuglede (1965), the author presents two dual ways to define a Greenian capacity (w.r.t. a kernel) for a measurable set U. The first one is using the set of barrier measures $\mathcal{KP}_U$ giving rise to the concept of outer capacity and the second one is using the dual of this set (i.e., $\mathcal{KP}_U^\top$) providing the inner capacity. The two methods give rise to the same capacity for U (i.e., the outer and inner capacities are equal), therefore the following minimax result holds:

$$\sup_{\lambda \in \mathcal{KP}_U^\top} \inf_{\mu \in \mathcal{KP}_U} \Lambda(\lambda, \mu) = \inf_{\mu \in \mathcal{KP}_U} \sup_{\lambda \in \mathcal{KP}_U^\top} \Lambda(\lambda, \mu) \tag{17}$$

Corollary 2. Under the hypotheses of the Th.3, we have the following estimation for the safety measure:

[4] The theory of the equilibrium measure goes back to the work of Gauss (1840), who obtained the sweeping of a measure on a set U in $\mathbb{R}^3$. He used his result to solve the Dirichlet problem for the domain bounded by U. It was Frostman (1935) who formally proved that this measure is minimizing a certain energy functional (see Kallenberg (2006) for more historical aspects).

$$P(A) = \inf_{\mu \in \mathcal{KP}_U} \sup_{y \in A} \Lambda(y, \mu). \quad (18)$$

When the expression of the Green function is available, (18) reduces to the study of barrier measures $\mathcal{KP}_U$. We have proved that $\mathcal{KP}_U$ is compact, metrizable and is the closed convex hull of its extreme measures. To make the computation easier, we will suppose that U is also convex. In this case, the extreme measures of $\mathcal{KP}_U$ will consist of those Dirac distributions δ_z, $z \in U$ for which we have:

$$g^S(y, z) \geq 1, \forall y \in U. \quad (19)$$

Therefore, an algorithm for the computation of (18) will start building up a "mesh" of U with the points $z \in U$ that correspond to the extreme Dirac distributions of $\mathcal{KP}_U$. Another view on the barrier function exploits the supermartingale property that can be derived from their excessivity. Upper bounds for the safety measure can be derived using supermartingale inequalities.

Proposition 4. (Wisniewski and Bujorianu (2017))

Let $A, U, S \in \mathcal{B}(\mathcal{Y})$ with S bounded, A closed and U open subsets of S and $\mathrm{cl}(A) \cap \mathrm{cl}(U) = \emptyset$. Consider a right process (X_t). Suppose that there is an excessive function $h : S \to \mathbb{R}_{\geq 0}$ (thought of as a barrier function). Then

$$P(A; U, S) \leq \frac{H_A}{H_U}, \quad (20)$$

where $H_A := \sup\{h(y) |\ y \in A\}$, $H_U := \inf\{h(y) |\ y \in U\}$.

Prop. 4 illustrates the fact that a barrier function is more 'optimal' as soon as the gap between its initial values (on the set A) and final values (on the target set U) is bigger.

3.2 p-Stability

In this paper, stability property of a set with respect to a stochastic process is defined as a sort of invariance. We will define p-stability based on the stability concepts presented in the Chapter II of Kushner (1967).

Let D be the closure of an open subset of S. Let $A \subset D$. We say that D is p-stable if for any $y \in A$, we have $(x_t) \in D$ for all $t < \infty$ with probability $1 - p$. Then we can write the following definition:

Definition 2. A process (X_t) is p-stable relative to the pair (A, D) if $\mathbf{P}^y[\zeta_D > 0] \leq p, \forall y \in A$, where ζ_D is the first exit time from D.

Different problems can be formulated based on the above definitions: (1) For given p and D is there a set A of initial states such that the process (X_t) is p-stable relative to the pair (A, D)? (2) For given p and D estimate the largest A such that problem (1) is satisfied. (3) For given D and A estimate the smallest p.

The method of solving the above problems involves finding functions of the (stochastic) Lyapunov type (excessive functions) (see Chapter 7 in Khasminskii (2012)).

Proposition 5. Let $A, D, S \in \mathcal{B}(\mathcal{Y})$ with S bounded, A and D closed subsets of S and $A \subset D$. Consider a right process (X_t). Suppose that there is an excessive function $h : S \to \mathbb{R}_{\geq 0}$ (thought of as a Lyapunov function), with

$$H_A := \sup\{h(y) |\ y \in A\},\ H_D := \sup\{h(y) |\ y \in D\}. \quad (21)$$

Then (X_t) is $\frac{H_A}{H_D}$-stable relative to the pair (A, D).

Proof. The proof is similar to that of Th.1 page 38 of the monograph Kushner (1967). Since h is an excessive function for the process (X_t), then it plays the role of a Lyapunov function in stability. From the definition of the excessive function, we obtain that $h(X_t)$ is a supermartingale, and then, by Doob's inequality we get:

$$\mathbb{P}^y[\sup_{t \leq \zeta_D} h(X_t) \geq \lambda] \leq \frac{h(y)}{\lambda}, \forall \lambda \leq H_D.$$

We define the stability function for (y, D) as: $\hat{P}(y; D, S) := \mathbf{P}^y[\zeta_D > 0]$, and for (A, D) as:

$$\hat{P}(A; D, S) := \sup_{y \in A} \mathbf{P}^y[\zeta_D > 0].$$

The following result is straightforward:

Proposition 6. The process (X_t) is p-stable relative to the pair (A, D) iff it is p-safe relative to the pair $(A, S \setminus D)$.

Remark 1. From the above characterization, it is easy to deduce that the Theorem 1 is true for the stability function w.r.t. the set of barrier functions $\mathcal{K}_V$, where $V := S \setminus D$.

4. MIXING SAFETY AND STABILITY

Let us consider: S a closed subset, U an open subset of $\mathcal{Y}$ with $U \subset S$, and a measurable set $D \subset S \setminus cl(U)$. Let $p_1, p_2 \in (0, 1)$ be error bounds for safety and stability.

Definition 3. The process (X_t) is (p_1, p_2)-stable-safe (S-safe) w.r.t. the tuple (A, D, U, S) if for all $y \in A$:

$$\mathbf{P}^y[\zeta_D > 0] \leq p_1,\ \mathbf{P}^y[\tau_U < \zeta_S] \leq p_2. \quad (22)$$

Obviously, we need to have $p_2 \leq p_1$.

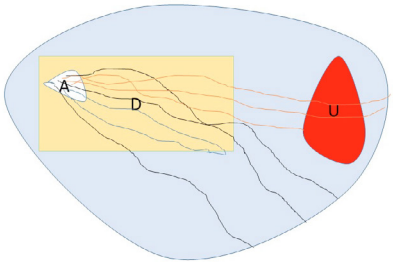

Fig. 1. S-Safety

In the Fig.1, S-safety means that the set of trajectories that escape from D (black and red colored) has the probability at most p_1, and the set of trajectories that reach U has the probability p_2. It is clear that the most unsafe trajectories are the ones in red.

In the following subsections, we will characterize the red trajectories using the properties of barrier functions and barrier measures.

4.1 S-Safety characterization

Prop. 4 can be generalized now to capture both stability and safety.

Proposition 7. Let $A, D, U, S \in \mathcal{B}(\mathcal{Y})$ with S bounded, A and D closed subsets of S, $A \subset D$, and U open subset of S such that $D \subset (S \setminus U)$. Consider a right process (X_t). Suppose that there is an excessive function $h : S \to \mathbb{R}_{\geq 0}$ (thought of as a Lyapunov function), with H_A and H_D given by (21), and $H_U := \inf\{h(y)|\ y \in U\}$.

Then (X_t) is $(\frac{H_A}{H_D}, \frac{H_A}{H_U})$-S-safe.

Prop. 7 provides some insights on the S-Safety problem, but these are not enough to glue together both concepts of safety and stability. Some other facets of these problems will be studied in the next subsections, which will set up the formal integration of these concepts.

4.2 Statistical constraints on S-safety

The definition of S-safety relative to the tuple (A, D, U, S) and the characterizations from the previous subsection prove that the study of S-safety can be reduced to the study of two safety problems (one with respect to U and another one with respect to $V = S \setminus D$). Then a barrier function for V is also barrier function for U, but the two problems can be investigated independently. To make the S-safety more pertinent, we need to add extra constraints. These constraints envisage the probability distribution of the process trajectories that escape from D and reach U.

When we consider that U is a dangerous region of the state space, the reach of this set could be thought of as an extreme event that has to be avoided as much as possible. Therefore, the process occupation measure of $V \setminus U$ has to be minimized. One way to characterize the occupation degree of $V \setminus U$ by the process trajectories that have the source in D and target U is to use a statistical tool called *probability current*.

In Bujorianu and Wisniewski (2019), we have shown that the safety function can be seen as an *equilibrium potential* for the "condenser" (U, S). In the case of S-Safety, we deal with two condensers (V, S) and (U, S). We will mainly use the properties of the condenser (V, S) and aim to find conditions that ensure a very small probability for reaching U. The equilibrium potential of (V, S) can be expressed using the integral of the Green function w.r.t. the *equilibrium measure* of V. In the following, we explain the technicalities behind these characterizations. In this work, we suppose that the trajectories of the underlying Markov process are right continuous with left limits. Then for the set V, we define a version of the *last exit time* as:

$$\gamma_V := \sup\{t > 0 | X_{t-} \in V\}. \tag{23}$$

Note that the last exit time is NOT a stopping time because it might depend on the process future. However, it has been proved that the distribution of last exit time can be used to characterize the equilibrium potential of V, which is, in fact, the safety function corresponding to this set. For any measurable set B, we consider the distribution of the last exit position X_{γ_V} given by:

$$\Gamma_V(y, B) := \mathbf{P}^y\{\gamma_V > 0, X_{\gamma_V} \in B\}. \tag{24}$$

The safety function associated to (V, S) (or equilibrium potential of V for the process restricted to S) can be uniquely written as:

$$P(y; V, S) = \int_V g^S(y, z)\sigma_V(dz), \forall y \in S, \tag{25}$$

where σ_V is the equilibrium measure of V. Here, $g^S(\cdot, \cdot)$ is the Green function of the process (X_t) restricted to S. For the physical interpretation of the equilibrium measure of a capacitor the interested reader can consult Bass (1995), pg. 139. Different versions of the following result have been proved in the literature (see, e.g., Chung and Getoor (1977), and the references therein). We adapt this result for the restriction of (X_t) to S.

Proposition 8. The last exit distribution kernel Γ_V is 'absolutely continuous' w.r.t. the equilibrium measure σ_V, i.e.,

$$\Gamma_V(y, B) = \int_B g^S(y, z)\sigma_V(dz), \forall y \in S. \tag{26}$$

Remark 2. Clearly, from the Prop. 8, we get that

$$P(y; V, S) = \Gamma_V(y, V)$$

and, moreover, the last exit kernel provide information about the visits of the process to all the subsets of V, including our unsafe set U, i.e.,

$$\Gamma_V(y, U) = \int_U g^S(y, z)\sigma_V(dz), \forall y \in S.$$

Based, on the Remark 2, the last exit distribution from V becomes the essential tool in analysing the unsafe set of trajectories that end in U. Ideally, to make our process safe, we need that the support of the equilibrium measure σ_V to have 'little' (negligible) intersection with U.

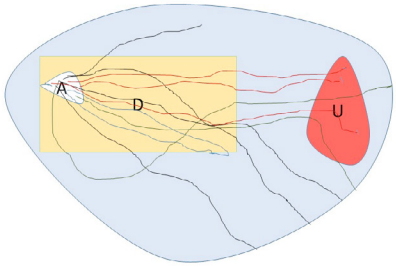

Fig. 2. Last exit - unsafe

In the Fig.2, we draw a weaker version of S-safety. The trajectories that escape from D (black, green and red colored) have different safety weights. The black ones are safe, they do not reach U. The green trajectories are 'fixable' because even they reach U, they do not die there, they return to V. The red trajectories have the last exit time from V situated in U. Then, they terminate in U. It is clear that the most unsafe trajectories are the ones in red. Then we are interested to compute the following weak S-safety function:

$$\bar{P}(y, D, V, U, S) := \mathbf{P}^y\{\zeta_D > 0, X_{\gamma_V} \in U\} = \Gamma_V(y, U).$$

For the set A of initial states, the aim of S-safety analysis will be to compute:

$$\bar{P}(A) := \sup_{y \in A} \bar{P}(y). \tag{27}$$

4.3 Last exit distribution approach

In the previous subsection, we have seen that the weak S-safety function can be calculated using the distribution

of the last exit kernel Γ_V. It is important to observe that Γ_V is a Markovian kernel, and it can be used to build up a discrete time Markov chain $(Y_k)_{k\in\mathbb{N}}$. This Markov chain records the terminal position of the process (X_t) in the set V. The chain $(Y_k)_{k\in\mathbb{N}}$ represents the *artificial dynamics* associated to (X_t).

Intuitively, the transition probabilities of the chain (Y_k) are used to define the weak S-safety function. Moreover, $\bar{P}(A)$ defined by (27) can be thought of as a reachability measure for (Y_k), when the initial state belongs to A.

The last exit time γ_V is not usually a stopping time for the given process. In fact, γ_V is the first hitting time of the reverse process coming from infinite. Then, we cannot use it in connection with the martingale problem associated to the process generator. The time γ_V might be related with the infinitesimal generator of the dual process. Moreover, the stochastic kernel Γ_V is mapping all the states from S to the support of the equilibrium measure σ_V. Therefore, the chain (Y_k) does not simulate the behaviour of (X_t), it plays the role of a sweeping process. To study the safety of the process with respect to the set U and the set of initial states A, we consider the following S-safety measure:

$$\langle \lambda, \bar{P}\rangle(A, D, V, U, S) := \int_A \Gamma_V(y, U)\lambda(dy),$$

defined for all initial distributions λ on A. This can be related with the entrance probability law of the chain (Y_k).

Furthermore, we need the *measure energy* with respect to the Green function given by (5). The following result is a direct consequence of the Cor. 2 and Prop. 8:

Proposition 9. Let (X_t) be a right process. Suppose $A,\ D,\ U,\ S \in \mathcal{B}(\mathcal{Y})$, with S bounded, A and D closed subsets of S, $A \subset D$, and U open subset of S such that $D \subset (S \setminus U)$. Suppose that the hypothesis (1) holds. Then

$$\bar{P}(A) = \inf_{\mu\in\mathcal{KP}_V} \sup_{y\in A} \Lambda(y, I_U\mu), \tag{28}$$

where I_U is the indicator function of U and $\mathcal{KP}_V$ is the set of barrier measures for $V = S \setminus D$.

The weak S-safety function of interest is expressed using the last exit kernel, or the Green potential with respect to the equilibrium measure of V. Analytical expressions for this measure exist only for some special stochastic processes. The computation the equilibrium measure will be based on the characterization of the extreme measures of $\mathcal{KP}_V$. The estimation of the weak S-safety function is closely related with the estimation of the Green kernel.

For convenience, we assume that the following hypothesis with respect to the Green function is satisfied.

Hypothesis 2. We suppose that the process lives in the Euclidean space $\mathbb{R}^d$ with $d \geq 3$ and there exists $\alpha \in (0, d)$ such that for any compact set K given there exists $\delta > 0$ and two constants $C_1, C_2 > 0$ such that:

$$C_2||y - z||^{-\alpha} \leq g^S(y, z) \leq C_1||y - z||^{-\alpha}, \tag{29}$$

for all $y, z \in K$ with $||y - z|| < \delta$.

The hypothesis (2) is not very restrictive, it shows the fact that most of stochastic processes are derived from the Brownian motion. In practice, the Green functions associated to the majority of standard Markov processes satisfy this kind of condition (see Kanda (1967)).

Proposition 10. Let (X_t) be a right process. Suppose $A,\ D,\ U,\ S \in \mathcal{B}(\mathcal{Y})$, with S compact, A and D closed subsets of S, $A \subset D$, and U open subset of S such that $D \subset (S \setminus U)$. Suppose that the hypotheses (1) and (2) hold. Then:

$$\bar{P}(A) \leq C_1(\rho(A, U))^{-\alpha}\sigma_V(U), \tag{30}$$

where $\rho(A, U)$ is the distance between the sets A and U.

5. CONCLUSIONS

In this paper, we have developed a stochastic framework to combine safety and stability. Safety is formulated as a state-constrained reachability problem and is studied using stochastic barrier functions generated via Green functions and potentials. Stability is defined in terms of an invariance/viability problem. We have defined a merging approach that is able to encapsulate both safety and stability. The approach is based on the concept of last exit distribution and makes use of the Krein-Milman theorem.

REFERENCES

Bass, R.F. (1995). *Probabilistic Techniques in Analysis*. Springer Verlag.

Blumenthal, R.M. and Getoor, R.K. (1968). *Markov processes and potential theory*. Pure and Applied Mathematics, Vol. 29. Academic Press, New York-London.

Bujorianu, L. (2012). *Stochastic Reachability Analysis of Hybrid Systems*. Communications and Control Engineering. Springer London, London. doi:10.1007/978-1-4471-2795-6.

Bujorianu, L. and Wisniewski, R. (2019). New insights on p-safety of stochastic systems. 2390–2395. IEEE.

Chung, K.L. and Getoor, R.K. (1977). The condenser problem. *Ann. Probab.*, 5(1), 82–86.

Chung, K. (1973). Probabilistic approach in potential theoryto the equilibrium problem. *Annales de lInstitut Fourier*, 23(3), 313–322.

Davis, M.H.A. (1993). *Markov models and optimization*. Chapman & Hall.

Doob, J.L. (2001). *Classical Potential Theory and Its Probabilistic Counterpart*. Springer Verlag.

Fuglede, B. (1965). Le theoreme du minimax et la theorie fine du potentiel. *Ann. Inst. Fourier*, 15(1), 65–87.

Hmissi, M. (1989). Methods of preparing thin-section slides. *Sminaire de Thorie du Potentiel Paris*, 5, 135–144.

Kallenberg, O. (2006). *Foundations of Modern Probability*. Springer Verlag.

Kanda, M. (1967). Regular points and green functions in markov processes. *J. Math. Soc. Japan*, 19(1), 46–69.

Khasminskii, R. (2012). *Stochastic Stability of Differential Equations*. Springer-Verlag, Berlin Heidelberg.

Kushner, H. (1967). *Stochastic Stability and Control*. Academic Press Inc, London.

Morters, P. and Peres, Y. (2010). *Brownian Motion*. Cambridge Series in Statistical and Probabilistic Mathematics.

Wisniewski, R. and Bujorianu, L. (2017). Stochastic safety analysis of stochastic hybrid systems. 2390–2395. IEEE.