2016 IEEE 55th Conference on Decision and Control (CDC)
ARIA Resort & Casino
December 12-14, 2016, Las Vegas, USA

On the new notion of Input-to-State Safety

Muhammad Zakiyullah Romdlony and Bayu Jayawardhana

Abstract— **In this paper, we study robustness analysis of systems' safety with respect to external input (or disturbance) signals. To this end, we introduce a new notion of input-to-state safety (ISSf) which allows us to quantify the systems' safety robustness, in the same way as the application of input-to-state stability (ISS) notion for analyzing robustness of systems' stability. In particular, ISSf prescribes the relationship between the evolution of state distance to the unsafe set with the initial conditions and the bounded external input signals. Finally, we discuss how to combine this notion with ISS for analyzing the robustness of both systems' stability and safety.**

I. Introduction

With the advent of complex cyber-physical systems (CPS) and industrial internet-of-thing, the safety of the integrated cyber-physical systems has become an important design feature that must be incorporated in all software levels [3]. In particular, this feature must also be present in the low-level control systems where both aspects of safety and stability are integrated in the control design.

For the past few years, a number of control design methods has been proposed in literature on the design of feedback controller that can guarantee both the safety and stability, simultaneously. To name a few, we refer interested readers to [1], [20], [14] and [15]. In [1] and [20], the authors proposed an optimization problem, in the form of a quadratic programming, where both control Lyapunov and control Barrier inequalities are formulated in the constraints. The proposed method generalizes the well-known pointwise min-norm control method for designing a control law using control Lyapunov functions via an optimization problem [12]. It has been successfully implemented in the cruise control of autonomous vehicle as reported in [9]. Another direct approach is pursued in [13], [15] which is based on the direct merging of control Lyapunov function and control Barrier function. The merging process results in a control Lyapunov-Barrier function which can be used to stabilize the system with guaranteed safety by using the Sontag's universal control law.

Despite the appealing idea in the aforementioned works for guaranteeing stability and safety, it remains unclear on how to analyze the robustness of the closed-loop system in the presence of external (disturbance) input signals. There are many tools available for analyzing the robustness of systems' stability, including, H_∞ and L_2-stability theories [17], [5], absolute stability theory [7], input-to-state stability (ISS) theory [19] and many others. However, analogous tools for systems' safety are still minimal in literature which makes it difficult to carry out robustness analysis to the aforementioned works that deal with the problem of stabilization with guaranteed safety.

The seminal work in [18], [19] on the characterization of input-to-state stability has been one of the most important tools in the stability analysis of nonlinear systems. It has allowed us to study stability of interconnected systems, to quantify systems' robustness with respect to external disturbances and to provide means for constructing a robustly stabilizing control law. The use of ISS Lyapunov function is crucial in all of these applications. In the following decade, the concept of ISS has been used and/or generalized in various direction with a commonality on the robustness analysis of systems' stability. Safety and constraint aspects have not been considered in this framework. By considering the complement of the set of unsafe state, one might consider to apply recent generalization of ISS to the stability of invariant sets as in [2]. But it may not give us an insightful detail on the influence of external disturbance signals to the state of safety of the system. In this case, the resulting ISS inequality will only provide us information on the effect of external input to the systems' trajectory with respect to the complement set of unsafe state, but not on how far it is from being unsafe.

In this paper, we present a preliminary work on the adaptation of ISS inequality to the systems' safety case. In particular, instead of the usual ISS inequality where the state trajectory $x(t)$ of the system can be bounded from above by a term that depends on initial condition and decay to zero and another term that depends on the L^∞-norm of the external input signal $u(t)$, we look at the following inequality

$$\sigma(|x(t)|_{\mathscr{D}}) \geq \alpha\left(|x(0)|_{\mathscr{D}}, t\right) - \phi\left(\|u\|_{L^\infty[0,t]}), t\right) \qquad (1)$$

where $\mathscr{D}$ is the set of unsafe state, $|x|_{\mathscr{D}}$ denotes the distance of x to $\mathscr{D}$, the function σ is a strictly increasing function, α and ϕ are strictly increasing function in both arguments with ϕ as the gain function that is dependent on input u, akin to the ISS case. As will be discussed later in Section III, the above inequality will be called input-to-state safety (ISSf) inequality.

Roughly speaking, this inequality can be interpreted as follows. When there is no external input signal u, then the state trajectory will never gets closer to $\mathscr{D}$. If there is an

The work of M.Z. Romdlony is supported by the Indonesian DIKTI scholarship program. This work is carried out within the national Dutch project on Region of Smart Factories (RoSF).

M.Z. Romdlony is with Faculty of Mathematics and Natural Science, University of Groningen and with Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia m.z.romdlony@rug.nl, zakiyullah@telkomuniversity.ac.id

B. Jayawardhana is with Engineering and Technology Institute Groningen, Faculty of Mathematics and Natural Science, University of Groningen b.jayawardhana@rug.nl

external input signal then it may jeopardize the systems' safety when the input signal u is taken sufficiently large. This interpretation serves very well with what we can expect in real systems where external disturbance input can potentially bring the system into the unsafe state. Xu *etal.* in [20] has presented also a preliminary study on the robustness aspect for systems' safety where they provide an indirect relationship between the external input norm to the admissible initial conditions such that the system remains safe. This relationship is also captured in (1) where if the bound on the input signal is known then the inequality (1) will make sense only if the initial conditions are bounded away from $\mathscr{D}$ by a constant that depends on the input norm.

Complement to the work of Xu *etal.* in [20], we adapt the ISS framework a'la Sontag to the systems' safety case through the use of ISSf barrier function which implies (1). For simplicity of presentation, we will consider the exponential convergence case and the extension of the work is presented in [16].

This paper is organized as follows. In Section II, we briefly recall the notion of stabilization with guaranteed safety, of ISS and of barrier certificate. In Section III, we introduce formally the notion of input-to-state safety and the characterization using ISSf barrier function. A small academic example is presented in this section. In Section IV, we combine both concepts of ISS and ISSf in order to provide a robustness analysis tool for stability with guaranteed safety. In Section V, we provide a numerical example of the aforementioned results for a simple mobile robot navigation system.

II. Preliminaries

Notation. Throughout this paper, we consider an affine non-linear system described by

$$\dot{x} = f(x) + g(x)u, \qquad x(0) = x_0, \tag{2}$$

where $x(t) \in \mathbb{R}^n$ denotes a state vector, $u(t) \in \mathbb{R}^m$ denote an (external) input or disturbance to the system. The functions $f(x)$ and $g(x)$ are $\mathscr{C}^1$ where the space $\mathscr{C}^1(\mathbb{R}^l, \mathbb{R}^m)$ consists of all continuously differentiable functions $F : \mathbb{R}^l \to \mathbb{R}^m$.

For a given signal $x : \mathbb{R}_+ \to \mathbb{R}^n$, its L^p norm on the interval $\mathscr{I} \subset \mathbb{R}_+$ is given by $\|x\|_{L^p(\mathscr{I})} := (\int_{\mathscr{I}} \|x(t)\|^p \mathrm{d}t)^{1/p}$ for $p = [1, \infty)$ and similarly, its L^∞ norm is defined by $\|x\|_{L^\infty(\mathscr{I})} := (\text{ess})\ \sup_{t \in \mathscr{I}}(\|x(t)\|)$. For the sake of conciseness, for $\mathscr{I} = [0,t)$, we denote the L^∞ norm of x simply by $\|x\|_{L^\infty}$. For a given bounded set $\mathscr{M} \subset \mathscr{X} \subset \mathbb{R}^n$, we define the distance of a point $\xi \in \mathbb{R}^n$ with respect to $\mathscr{M}$ by $|\xi|_{\mathscr{M}} := \min_{a \in \mathscr{M}} \|\xi - a\|$ where $\|\cdot\|$ is a metric norm. We define an open ball centered at a point $a \in \mathbb{R}^n$ with radius $r > 0$ by $\mathbb{B}_r(a) := \{\xi \in \mathbb{R}^n | \|\xi - a\| < r\}$ and its closure is denoted by $\overline{\mathbb{B}}_r(a)$.

We define the class of continuous strictly increasing functions $\alpha : \mathbb{R}_+ \to \mathbb{R}_+$ by $\mathscr{P}$ and denote by $\mathscr{K}$ all functions $\alpha \in \mathscr{P}$ which satisfy $\alpha(0) = 0$. Moreover $\mathscr{K}_\infty$ denotes all functions $\alpha \in \mathscr{K}$ which satisfy $\alpha(r) \to \infty$ as $r \to \infty$. By $\mathscr{KL}$ we denote all functions $\beta : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $\beta(\cdot, t) \in \mathscr{K}$ for a fixed $t \geq 0$ and and $\beta(s, \cdot)$ is strictly decreasing and converging to zero for a fixed $s \geq 0$. Correspondingly, we also denote by $\mathscr{KK}$ all functions $\gamma : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $\gamma(\cdot, t) \in \mathscr{K}$ for a fixed $t \geq 0$ and similarly, $\gamma(s, \cdot) \in \mathscr{K}$ for a fixed $s \geq 0$.

Let $\mathscr{X}_0 \subset \mathbb{R}^n$ be the set of initial conditions and let an open and bounded set $\mathscr{D} \subset \mathbb{R}^n$ be the set of unsafe states, where we assume that $\mathscr{D} \cap \mathscr{X}_0 = \emptyset$. Since we consider also a stabilization problem of the origin, we assume that $0 \in \mathscr{X}_0$. For a given set $\mathscr{D} \subset \mathbb{R}^n$, we denote the boundary of $\mathscr{D}$ by $\partial\mathscr{D}$ and the closure of $\mathscr{D}$ by $\overline{\mathscr{D}}$.

Following definition in [15], the (autonomous) system (2) with $u = 0$ is called *safe* if for all $x_0 \in \mathscr{X}_0$ and for all $t \in \overline{\mathbb{R}}_+$, $x(t) \notin \overline{\mathscr{D}}$. Additionally, (2) with $u = 0$ is called (asymptotically) stable with guaranteed safety if it is both (asymptotically) stable and safe. Based on these notions, the problem of stabilization with guaranteed safety has been investigated in [15] where the control problem is to design a feedback law $u = k(x)$ such that the closed loop system is safe and asymptotically stable, i.e. for all $x_0 \in \mathscr{X}_0$, we have that $x(t) \notin \mathscr{D}$ for all t and $\lim_{t \to \infty} \|x(t)\| = 0$. Moreover, when $\mathscr{X}_0 = \mathbb{R}^n \setminus \mathscr{D}$ the problem is called *the global stabilization with guaranteed safety*.

As discussed briefly in the Introduction, analyzing the robustness of systems stability in the presence of an (external) input signal can be done using the input-to-state stability (ISS) framework [18], [19]. Let us briefly recall the ISS concept from [19].

The system (2) is called *input-to-state stable* if there exist a $\beta \in \mathscr{KL}$ and $\gamma \in \mathscr{K}$ such that for any $u \in L^\infty$ and $x_0 \in \mathscr{X}_0$, the following inequality holds for all t:

$$\|x(t)\| \leq \beta(\|x_0\|, t) + \gamma(\|u\|_{L^\infty}). \tag{3}$$

In this notion, the functions β and γ in (3) describe the decaying effect from a non-zero initial condition x_0 and the influence of a bounded input signal u to the state trajectory x, respectively. The Lyapunov characterization of ISS systems is provided in the following well-known theorem from [18], [19].

Theorem 1: The system (2) is ISS if and only if there exists a smooth $V : \mathbb{R}^n \to \mathbb{R}_+$, functions $\alpha_1, \alpha_2, \alpha_3 \in \mathscr{K}_\infty$ and a function $\gamma \in \mathscr{K}$ such that

$$\alpha_1(\|\xi\|) \leq V(\xi) \leq \alpha_2(\|\xi\|) \tag{4}$$

and

$$\frac{\partial V(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leq -\alpha_3(\|\xi\|) + \gamma(\|v\|) \tag{5}$$

hold for all $\xi \in \mathbb{R}^n$ and for all $v \in \mathbb{R}^m$.

The notion of ISS and its Lyapunov characterization as above has been seminal in the study of nonlinear systems robustness with respect to the uncertainties in the initial conditions and to the external disturbance signals. For instance, a well-known nonlinear small-gain theorem in [8] is based on the use of β and γ. The study of convergence input convergence state property as in [6] is based on the use of ISS Lyapunov function. However, as mentioned in the Introduction, existing results on robustness have focused on the systems' stability and there is not many attention on the robustness analysis on systems' safety.

Let us recall few main results in literature on safety analysis. In order to verify the safety of system (2) with respect to a given unsafe set $\mathscr{D}$, a Lyapunov-like function which is called barrier certificate has been introduced in [11] where the safety of the system can be verified through the satisfaction of a Lyapunov-like inequality without having to explicitly evaluate all possible systems' trajectories. It is summarized in following theorem.

Theorem 2: Consider the (autonomous) system (2) with $u = 0$, i.e., $\dot{x} = f(x)$, with a given unsafe set $\mathscr{D}$ and set of initial conditions $\mathscr{X}_0$. Assume that there exists a barrier certificate $B : \mathscr{X} \to \mathbb{R}$ where $\mathscr{X} \subset \mathbb{R}^n$ satisfying

$$B(\xi) > 0 \quad \forall \xi \in \mathscr{D} \tag{6}$$

$$B(\xi) \leq 0 \quad \forall \xi \in \mathscr{X}_0 \tag{7}$$

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq 0 \quad \forall \xi \in \mathscr{X} \quad \text{such that} \quad B(\xi) = 0. \tag{8}$$

Then the system is safe.

The proof of this theorem is based on the fact that the evolution of B starts from a non-positive value (c.f. (7)) and together with (8), B will never cross the zero level set, i.e., the state trajectory will always be safe according to (6).

Although the safety result as in Theorem 2 is formulated only for autonomous systems, an extension to the non-autonomous case has also been presented in [11]. For the case where an external input u is considered, e.g., the complete system as in (2), the safety condition (8) becomes

$$\frac{\partial B(\xi)}{\partial \xi} (f(\xi) + g(\xi)v) \leq 0 \quad \forall (\xi, v) \in \mathscr{X} \times \mathscr{U} \tag{9}$$

where $\mathscr{U} \subset \mathbb{R}^m$ denotes the admissible set of input. However, the condition (9) is a very restrictive assumption since it must hold for all $u(t) \in \mathscr{U}$ including the case when the initial condition $x(0)$ is very close to $\mathscr{D}$. It means that when we start very close to the unsafe state, the system will always remain safe for whatever type of input signals u as long as it has values in $\mathscr{U}$. In this case, we can say that such system is very robust with respect to bounded external input signals. In practice, we should expect a certain degree of fragility in the system, in the sense that, if we start very close to the unsafe state, a small external input signal can already jeopardize the systems' safety; a feature that is not captured in (9).

Instead of considering the inequality (9), we will consider a less restrictive condition on B for our main results later, where the non-increasing assumption of B as in (8) is replaced by a strict inequality as follows

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq -\alpha(|x|_{\mathscr{D}}) \tag{10}$$

where α is a $\mathscr{K}$ function.

In [15], [21], the use of such barrier function B for control design that guarantees safety has been presented. It is shown in these works that the standard Lyapunov-based control design can directly be extended to solving the safety problem by replacing the Lyapunov function with the barrier one. Interested readers are referred to [15] for control design methods that solve the stabilization with guaranteed safety by merging the control Lyapunov function with the control barrier function.

III. Input-to-state safety

In this section, we will explore a new notion of input-to-state safety as a tool to analyze the robustness of systems' safety. In particular, we focus our study on extending existing results on barrier certificate to the input-to-state safety framework; akin to the role of Lyapunov function in the input-to-state stability results.

Definition 1: The system (2) is called *practically input-to-state safe* (pISSf) with respect to the set of unsafe state $\mathscr{D}$ if there exist $\alpha, \phi \in \mathscr{K}\mathscr{K}$ and $\gamma \in \mathscr{P}$ such that

$$\sigma(|x(t)|_{\mathscr{D}}) \geq \alpha(|x_0|_{\mathscr{D}}, t) - \phi(\|u\|_{L^\infty}, t) - \gamma(t) \tag{11}$$

holds for all t. Furthermore, if $\gamma = 0$ then it is called input-to-state safe (ISSf).

There are implicit assumptions on α, ϕ and γ which will be evident later in this section.

Note that in this definition, we implicitly assume that the system (2) can be brought to unsafe state if the L^∞-norm of u is sufficiently large such that the RHS of (11) is negative. Hence one can quantify the robustness of the system's safety with respect to an external input signal using this notion of input-to-state safety.

For instance, if the initial condition x_0 is in the neighborhood of the boundary of unsafe state $\mathscr{D}$ then (11) shows that a small external input signal u can steer the state trajectory to enter $\mathscr{D}$; even when the autonomous case is safe. Since the first element on the RHS of (11) is a $\mathscr{K}\mathscr{K}$ function, it implies that the distance between $x(t)$ and $\mathscr{D}$ grows. As the distance increases with time, (11) means that the system can withstand larger input signal.

Another possible application of the input-to-state safety inequality (11) is as follows. If u is considered to be a disturbance signal with known magnitude, e.g., $\|u\|_{L^\infty} \leq \kappa$ with $\kappa > 0$, then (11) provides us with information on the admissible x_0 such that the RHS of (11) remains positive so that the system under such external disturbance will remain safe.

In view of this remark, we implicitly assume following conditions on α, ϕ and γ for the pISSf inequality (11) is well-posed

(I) For every $\varepsilon > 0$ there exists $\delta > 0$ such that $\alpha(\delta, t) - \phi(\varepsilon, t) - \gamma(t) \geq 0$ for all t.

Assumption **(I)** ensures that for any given bounded input signal u there always exists an admissible initial condition in the pISSf inequality (11). This can have another interpretation as follows. For any given initial $x(0)$ there is an upper bound on the allowable bounded input u to guarantee the systems' safety.

In the rest of this paper, we will consider a particular case of exponential rate for α, ϕ and γ where in this case (11) becomes

$$|x(t)|^p_{\mathscr{D}} \geq k_1 e^{\lambda_1 t} |x_0|^p_{\mathscr{D}} - k_2 e^{\lambda_2 t} \|u\|^q_{L^\infty} - k_3 e^{\lambda_3 t} \tag{12}$$

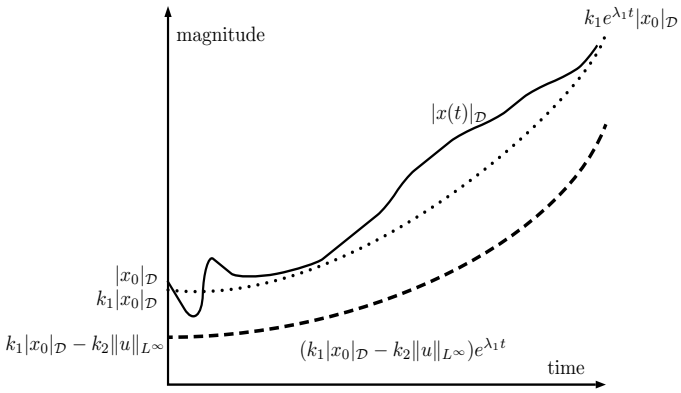

Fig. 1. An illustration of the ISSf-inequality (11) for the exponential rate case as presented in Proposition (1) with $\kappa = 0$. The dotted-line describes the lower-bound of distance to unsafe set that is due to the initial conditions (e.g., the first term on RHS of (11)) while the dashed-line shows the influence of the bounded external input in decreasing this lower-bound. The solid-line shows a possible time evolution of the distance to the unsafe set following (11). If the dashed-line crosses the zero line then the system may enter the unsafe set.

where $k_1, k_2, k_3, \lambda_1, \lambda_2, \lambda_3 > 0$. In order to satisfy **(I)**, it is implicitly assumed that $\lambda_1 \geq \max\{\lambda_2, \lambda_3\}$.

Figure 1 shows an illustration of the ISSf-inequality with an exponential rate as in (12) and $k_3 = 0$, i.e., the case of input-to-state safe. In this figure, the evolution of state distance to the unsafe set is always lower-bounded by $k_1 e^{\lambda_1 t}|x_0|_{\mathscr{D}} - k_2 e^{\lambda_2 t}\|u\|_{L^\infty}$, with $\lambda_1 = \lambda_2$. When the lower bound crosses the zero line (for instance, if the input is sufficiently large or the initial distance to the unsafe set is very small) then safety of the system is no longer guaranteed for such input and initial state setting.

In the following proposition, we show a barrier function characterization that gives rise to the input-to-state safety inequality (12).

Proposition 1: Consider the nonlinear system in (2) that is forward complete and let the set of unsafe state be given by a compact set $\mathscr{D} \subset \mathbb{R}^n$. Suppose that there exists an ISSf barrier function $B : \mathbb{R}^n \to \mathbb{R}$ satisfying

$$-c_1|\xi|^p_{\mathscr{D}} - \kappa \leq B(\xi) \leq -c_2|\xi|^p_{\mathscr{D}} \tag{13}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leq -c_3|\xi|^p_{\mathscr{D}} + c_4\|v\|^q \tag{14}$$

where $c_i > 0$, $i = 1,2,3,4$ and $\kappa \geq 0$. Then the system is practically input-to-state safe w.r.t. $\mathscr{D}$ where $\alpha(s,t) = \frac{c_2}{c_1}e^{\frac{c_3}{c_1}t}s^p$, $\phi(s,t) = \frac{c_4}{c_3}e^{\frac{c_3}{c_1}t}s^q$ and $\gamma(t) = \frac{\kappa}{c_1}e^{\frac{c_3}{c_1}t}$.

Proof : Let $x(t)$ be the solution of (2). Evaluating the time derivative of $B(x(t))$ along the trajectory of x, it follows from (13) and (14) that

$$\dot{B}(x) \leq \frac{c_3}{c_1}B(x) + \frac{\kappa c_3}{c_1} + c_4\|u\|^q.$$

By the standard application of comparison lemma, the above differential inequality implies immediately that

$$B(x(t)) \leq e^{\frac{c_3}{c_1}t}B(x(0)) + \int_0^t e^{\frac{c_3}{c_1}(t-\tau)}\left(\frac{\kappa c_3}{c_1} + c_4\|u(\tau)\|^q\right)\mathrm{d}\tau.$$

Following a routine computation on the RHS of this inequality, we get

$$\begin{aligned} B(x(t)) &\leq e^{\frac{c_3}{c_1}t}B(x(0)) + \left(\frac{\kappa c_3}{c_1} + c_4\|u\|^q_{L^\infty}\right)\int_0^t e^{\frac{c_3}{c_1}(t-\tau)}\mathrm{d}\tau \\ &= e^{\frac{c_3}{c_1}t}B(x(0)) + \left(\kappa + \frac{c_4c_1}{c_3}\|u\|^q_{L^\infty}\right)\left(e^{\frac{c_3}{c_1}t} - 1\right) \end{aligned}$$

By using the lower bound of $B(x(t))$ in (13) into the above inequality, it is easy to see that

$$\begin{aligned} -c_1|x(t)|^p_{\mathscr{D}} - \kappa &\leq e^{\frac{c_3}{c_1}t}B(x(0)) + \left(\kappa + \frac{c_4c_1}{c_3}\|u\|^q_{L^\infty}\right)\left(e^{\frac{c_3}{c_1}t} - 1\right) \\ \Rightarrow -c_1|x(t)|^p_{\mathscr{D}} &\leq -c_2e^{\frac{c_3}{c_1}t}|x(0)|^p_{\mathscr{D}} + \frac{c_4c_1}{c_3}\|u\|^q_{L^\infty}\left(e^{\frac{c_3}{c_1}t} - 1\right) + \kappa e^{\frac{c_3}{c_1}t} \\ \Rightarrow |x(t)|^p_{\mathscr{D}} &\geq \frac{c_2}{c_1}e^{\frac{c_3}{c_1}t}|x(0)|^p_{\mathscr{D}} - \frac{c_4}{c_3}\|u\|^q_{L^\infty}(e^{\frac{c_3}{c_1}t} - 1) - \frac{\kappa}{c_1}e^{\frac{c_3}{c_1}t} \\ &\geq \frac{c_2}{c_1}e^{\frac{c_3}{c_1}t}|x(0)|^p_{\mathscr{D}} - \frac{c_4}{c_3}\|u\|^q_{L^\infty}e^{\frac{c_3}{c_1}t} - \frac{\kappa}{c_1}e^{\frac{c_3}{c_1}t}. \end{aligned}$$

□

As shown in Proposition (1), a practical input-to-state safety can be shown if there exists B such that the inequalities (13) and (14) holds. When $\kappa = 0$ then (13) & (14) $\Rightarrow$ the system (2) is input-to-state safe. In the following, we define the function B satisfying (13) and (14) as pISSf barrier function. Moreover, if $\kappa = 0$ then it is called ISSf barrier function.

The constant κ is introduced in (13) to accomodate a polynomial function B of x as typically considered in the construction of a barrier certificate via sum-of-squares programming (for the safety analysis of an autonomous system). The gradient of such function B on the boundary of $\mathscr{D}$ may be non-zero. For example, in Figure 2, the red-line depicts a quadratic function B that has values larger than zero in the unsafe set $\mathscr{D}$ and is less than zero otherwise. Since the gradient of B on $\partial\mathscr{D}$ is non-zero, it cannot be lower bounded only by using $-c_1|x|_{\mathscr{D}}$ whose gradient on $\partial\mathscr{D}$ is equal to zero. In this case, by taking an arbitrary small $\kappa > 0$, we can find a sufficiently large $c_1 > 0$ such that the lower bound in (13) holds. Note that an arbitrary large c_1 will give us a conservative estimate in the growth of the bound in the ISSf inequality.

An example of an ISSf barrier function that satisfies (13) with $\kappa = 0$ is shown in Figure (3). In this figure, the ISSf

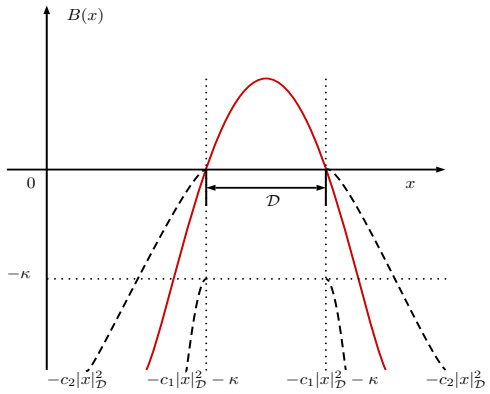

Fig. 2. An illustration of a practical ISSf barrier function which takes the form of a quadratic function, e.g., $B(x) = -(x-x^*)^T P(x-x^*)+c$ where P is a positive definite matrix, x^* is the centroid of the unsafe set $\mathscr{D}$ and c is a constant that is chosen such that the zero level of B is equal to the boundary of $\mathscr{D}$. The solid red-line is the plot of B and the dashed-line shows the possible lower and upper bound of B using the set distance function $|x|_{\mathscr{D}}$ and a bias constant $\kappa > 0$ as used in Proposition (1), c.f., (13).

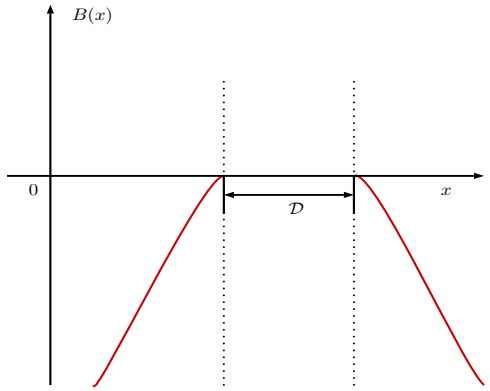

Fig. 3. The plot of an ISSf barrier function $B(x) = -c|x|^2_{\mathscr{D}}$ with $c > 0$.

barrier function is constructed directly using the set distance function $|x|_{\mathscr{D}}$.

One can observe that in the standard barrier certificate result as given in Theorem 2, the condition (8) is imposed so that the barrier certificate B is non-increasing along the trajectory of $x(t)$ which is similar to the Lyapunov stability analysis. However, we cannot use such B as an ISSf barrier function for the non-autonomous system (2). If we consider a barrier certificate B which satisfies (10) instead, then we may be able to use it as a candidate for an ISSf barrier function.

Corollary 1: Consider a forward complete system (2) with bounded g and let the set of unsafe state be given by a compact set $\mathscr{D} \subset \mathbb{R}^n$. Suppose that there exists a barrier certificate $B : \mathbb{R}^n \to \mathbb{R}$ such that

$$-c_1|\xi|^p_{\mathscr{D}} - \kappa \leq B(\xi) \leq -c_2|\xi|^p_{\mathscr{D}} \tag{15}$$

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq -c_3|\xi|^p_{\mathscr{D}} \tag{16}$$

$$\left\| \frac{\partial B(\xi)}{\partial \xi} \right\| \leq c_4 \|\xi\|^q \tag{17}$$

where $c_i > 0$, $i = 1,2,3,4$ and $\kappa \geq 0$. Then the system is practically input-to-state safe w.r.t. $\mathscr{D}$ with an exponential rate.

The proof of this corollary is straightforward and is therefore omitted.

Similar to this corollary, one can also easily show that if the system admits a control barrier function B with the strict version of the Artstein's like condition, e.g.,

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq -c|\xi|^p_{\mathscr{D}} \qquad \forall \xi \text{ s.t. } \frac{\partial B(\xi)}{\partial \xi} g(\xi) = 0,$$

then we may use B to design a control law (for instance, via the Sontag's universal control law) such that the closed-loop system is pISSf or ISSf which depends on (13).

IV. Input-to-State Stability with Guaranteed Safety

Equip with the result on input-to-state safety from the previous section, we can now combine the notion of input-to-state stability and that of input-to-state safety that allows us to study the robustness of a stable and safe system with respect to external input u.

Definition 2: System (2) is called ISS with guaranteed safety (ISS-GS) with respect to $\mathscr{D}$ if it is both input-to-state stable and input-to-state safe with respect to $\mathscr{D}$.

Since ISS is a global property, combining both notions of ISS and ISSf can be counteractive. For instance, consider again the exponential rate case for both ISS and ISSf. The ISS notion implies that the state trajectories will converge to a ball close to the origin where the ball size is determined by the input. Since the distance between the origin and $\mathscr{D}$ is finite, it follows then that the evolution of distance to $\mathscr{D}$ will also converge to a finite value which contradicts the ISSf inequality in (12). Thus, one needs to either impose ISSf only locally or to allow the $\mathscr{KK}$ functions α, ϕ and γ in (11) to have a bounded range or saturation.

It is trivial to show that if there exist both a quadratic ISS Lyapunov function V satisfying (4)–(5) and an ISSf barrier function B satisfying (13)–(14) locally on $\Xi \subset \mathbb{R}^n$ with $\kappa = 0$ and $\mathscr{D} \subset \Xi$ then the system is input-to-state stable with guaranteed safety. Instead of considering two separate functions V and B as suggested before, we can also consider combining the ISS Lyapunov inequality (5) and ISSf barrier inequality (14) as given in the following proposition.

Proposition 2: Suppose that there exists $W : \mathbb{R}^n \to \mathbb{R}$ and $\mathscr{D} \subset \Xi \subset \mathbb{R}^n$ such that

$$c_1\|\xi\|^p \leq W(\xi) \leq c_2\|\xi\|^p \quad \forall \xi \in \mathbb{R}^n \tag{18}$$

$$-c_3|\xi|^p_{\mathscr{D}} - \kappa \leq W(\xi) \leq -c_4|\xi|^p_{\mathscr{D}} \quad \forall \xi \in \Xi \tag{19}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi)+g(\xi)v) \leq -c_5\|\xi\|^p - c_6\chi_\Xi(\xi)|\xi|^p_{\mathscr{D}} + c_7\|v\|^q \tag{20}$$

where χ_Ξ is an indicator function for Ξ, the constants $c_i > 0$, $i = 1,2,..$ and $\kappa > 0$. Then it is ISS with guaranteed safety with respect to $\mathscr{D}$.

Proof : It is trivial to check that $W(x)$ qualifies as an ISS Lyapunov function satisfying (4)–(5) and as an ISSf barrier function satisfying (13)–(14) locally in Ξ. Indeed, from (20), we have that

$$\dot{W}(x(t)) \leq -c_5\|x(t)\|^p + c_7\|u(t)\|^q.$$

Using a standard result from ISS and using (18), it follows immediately that

$$\|x(t)\|^p \leq \frac{c_2}{c_1}e^{-\frac{c_5}{c_1}t}\|x_0\|^p + \frac{c_7}{c_5}\|u\|^q_{L^\infty}$$

which shows the robustness of systems' stability. On the other hand, from (20), it follows that in Ξ

$$\dot{W}(x(t)) \leq -c_6\|x(t)\|^p_{\mathscr{D}} + c_7\|u(t)\|^q.$$

Hence, as shown before, together with (19) it implies that

$$|x(t)|^p_{\mathscr{D}} \geq \frac{c_4}{c_3}e^{\frac{c_6}{c_3}t}|x(0)|^p_{\mathscr{D}} - \frac{c_7}{c_6}\|u\|^q_{L^\infty}e^{\frac{c_6}{c_3}t} - \frac{\kappa}{c_3}e^{\frac{c_6}{c_3}t}$$

holds for all $x(t) \in \Xi$, i.e., it is safe. □

V. Simulation result on mobile robot navigation

In this section, we consider an example of a simple mobile robot navigation described by the following equations

$$\begin{aligned}\dot{x}_1 &= v_1 + u_1\\ \dot{x}_2 &= v_2 + u_2\end{aligned} \tag{21}$$

where $x = [x_1, x_2]^T$ is the position in a 2D plane, $v = [v_1, v_2]^T$ is its velocity which is used as a feedback control input, and $u = [u_1, u_2]^T \in L^\infty$ is external disturbance signal.

Example 1: (*Input-to-state safety*). Consider system (21) with a given unsafe set $\mathscr{D} := \{x \in \mathbb{R}^2 | (x_1-4)^2 + (x_2-6)^2 < 4\}$. We can construct an ISSf barrier function $B(x) = -(x_1-4)^2 - (x_2-6)^2 + 4$. Consider a gradient-based control law for (21) using $B(x)$, i.e., $\left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right] = -\nabla_x B(x) = -\frac{\partial^T B}{\partial x}$.

It can be checked that this ISSf barrier function B fulfills all hypotheses in Proposition 1. In this example, the function $B(x)$ can be lower-bounded by $-c_1|x|^2_{\mathscr{D}} - \kappa$, with $c_1 = 1.2, \kappa = 0.1$ and can be upper-bounded by $-c_2|x|^2_{\mathscr{D}}$, with $c_2 = 0.8$. Thus it satisfies (13). It remains for us to check whether (14) holds. A routine computation shows that

$$\dot{B} = \frac{\partial B}{\partial x}(-\frac{\partial^T B}{\partial x} + u) \tag{22}$$

$$\leq -\left\|\frac{\partial B}{\partial x}\right\|^2 + \left\|\frac{\partial B}{\partial x}\right\|\|u\| \tag{23}$$

$$\leq -c_3|x|^2_{\mathscr{D}} + c_4\|u\|^2. \tag{24}$$

with $c_3 = 2$, and $c_4 = 0.5$ which satisfies (14).

Figure 4 shows the time plots of $\|x(t)\|$ and $|x(t)|^2_{\mathscr{D}}$ started from an initial condition $x_0 = (2,2)$. The infinity norm of disturbance $u(t)$ is given by $\|u\|_{L^\infty} = 2.5112$. The dashed curve shows $\frac{c_2}{c_1}e^{\frac{c_3}{c_1}t}|x_0|^2_{\mathscr{D}} - \frac{c_4}{c_3}\|u\|^2_{L^\infty}e^{\frac{c_3}{c_1}t} - \frac{\kappa}{c_1}e^{\frac{c_3}{c_1}t}$, which is the lower-bound of $|x(t)|^2_{\mathscr{D}}$ such that the safety of (21) still preserved in the presence of disturbance.

Example 2: (*Input-to-state stability with guaranteed safety*)

Let us consider the same system (21) and the same unsafe set as in Example 1. We consider a disturbance signal u whose norm is given by $\|u\|_{L^\infty} = 2.6638$. In addition to ensuring the safety of the system, we also consider now the stabilization problem of the origin. The system (21) admits a ISS Lyapunov function $V(x) = x_1^2 + x_1x_2 + x_2^2$ that can be lower-bounded and upper-bounded by $0.5\|x\|^2$ and $2\|x\|^2$ respectively, so that (19) holds. As discussed in Proposition 2, we need to define ISSf barrier function locally in $\mathbb{B}(0)_{0.5}$ neighborhood of unsafe state $\mathscr{D}$, i.e., $\mathscr{X} := \mathscr{D} + \mathbb{B}(0)_{0.5} = \{x \in \mathbb{R}^2 | (x_1-4)^2 + (x_2-6)^2 < 9\}$. Since the ISSf barrier function $B(x)$ discussed in Example 1 is not lower-bounded so we can not define it locally, we can construct a lower-bounded one $\widetilde{B}(x)$ by following construction procedure in [15] instead. The lower-bounded ISSf barrier function is given as follows

$$\widetilde{B}(x) = B(\omega) + \oint_\Gamma 0.5\left(\cos\left(\frac{\pi}{\delta}B(\sigma)\right) + 1\right)\frac{\partial B(\sigma)}{\partial x}d\sigma \qquad \forall x \in \mathscr{X}$$

where $\omega \in \partial\mathscr{D}$ is any point in the boundary of $\mathscr{D}$, Γ is any path from point ω to any point $\phi \in \mathscr{X}$, and $\delta = -B(\partial\mathscr{X}) = 5$. For $x \in \mathbb{R}^2 \setminus \mathscr{X}$, $\widetilde{B}(x)$ is defined as negative constant, i.e. $-\delta = -5$.

Following the same procedure discussed in [15] for achieving the stability and the safety of a system simultaneously, we then merge the ISS Lyapunov function and the ISSf barrier function into $V(x) + k_1\widetilde{B}(x) + k_2$, with $k_1 = 100$, $k_2 = -10$ such that the equations (18)-(20) are satisfied.

In this example, we use also the gradient of $W(x)$ as a control law for (21), i.e., $v = -\nabla_x W(x) = -\frac{\partial^T W}{\partial x}$. An explicit form of this gradient-based control law is given by

$$v = \begin{cases} -\nabla_x V(x) - k_1\nabla_x\widetilde{B}(x) & \forall x \in \mathscr{X} \\ -\nabla_x V(x) & \forall x \in \mathbb{R}^2 \setminus \mathscr{X}. \end{cases} \tag{25}$$

Figure 5 shows the evolution of state x_1 and x_2 starting from four different initial conditions. Under the influence of bounded disturbance, the state trajectories converge to origin and avoid the unsafe state. Thus the system is input-to-state stable with guaranteed safety.

Figure 6 shows the time plots of $\|x(t)\|$ and $|x(t)|_{\mathscr{D}}$ started from $x_0 = (5,8)$. From the figure we can conclude that the system is robustly stable and safe with respect to the disturbance $u(t)$.

VI. Conclusion

In this paper, we have presented a novel notion of input-to-state safety which can be a complementary to the well-known input-to-state stability notion. The new notion has allowed us to characterize the evolution of the state distance to the set of unsafe state whose lower bound depends on the initial condition and the external input signal. It can be used for the robustness analysis of systems' safety. The use of an ISSf barrier function is also presented, which is analogous to

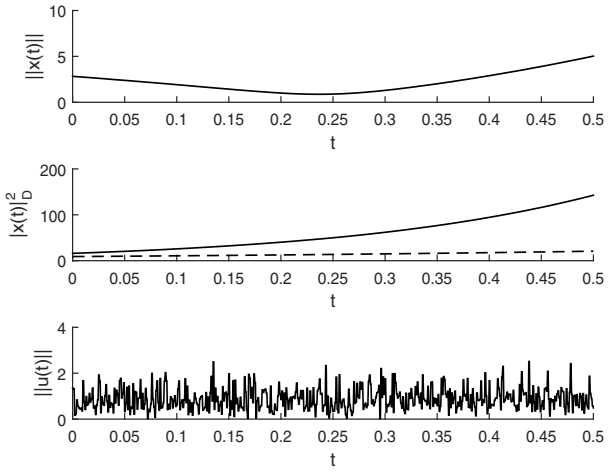

Fig. 4. The time plots of $\|x(t)\|$, $|x(t)|^2_{\mathscr{D}}$, and $\|u(t)\|$ with initial state $x_0 = (2,2)$. The dashed curve in the middle plot shows the lower-bound of $|x(t)|^2_{\mathscr{D}}$ such that the safety of (21) is still preserved in the presence of disturbance u.

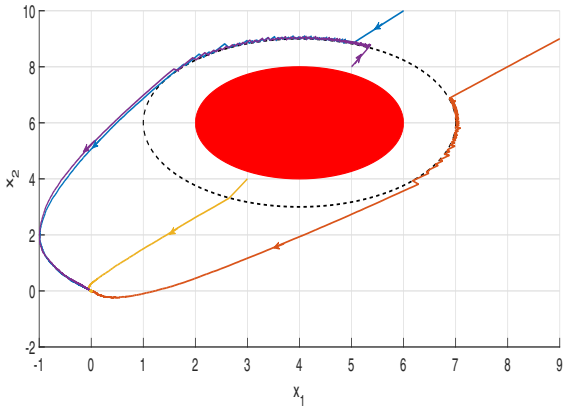

Fig. 5. State trajectories $x(t)$ discussed in Example 2, starting from four different initial conditions. The set of unsafe state $\mathscr{D}$ is shown in red area, and the boundary of $\mathscr{X}$ is shown by dashed line.

the use of ISS Lyapunov function for ISS. The applicability of the new notion has been shown as well through numerical simulation.

REFERENCES

[1] A. D. Ames, J. W. Grizzle, P. Tabuada,"Control Barrier Function based Quadratic Programs with Application to Adaptive Cruise Control" Proc. IEEE Conf. Dec. Contr., Los Angeles, 2014.

[2] D. Angeli & D. Efimov, "Characterizations of Input-to-State stability for systems with multiple invariant sets," IEEE Trans. Aut. Contr., vol. 60, no. 12, pp. 3242-3256, 2015.

[3] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, "Ensuring Safety, Security, and sustainability of Mission-Critical Cyber-Physical Systems," Proc. IEEE, vol. 100, no. 1, pp. 283-299, 2011.

[4] E. Garone & M.M. Nicotra,"Explicit Reference Governor for Constrained Nonlinear Systems,"*IEEE Transactions on Automatic Control*, doi: 10.1109/TAC.2015.2476195, in-press, 2016.

[5] B. Jayawardhana & G. Weiss, "State Convergence of Passive Nonlinear Systems With an L^2 Input," IEEE Trans. Aut. Contr., vol. 54, no. 7, pp. 1723-1727, 2009.

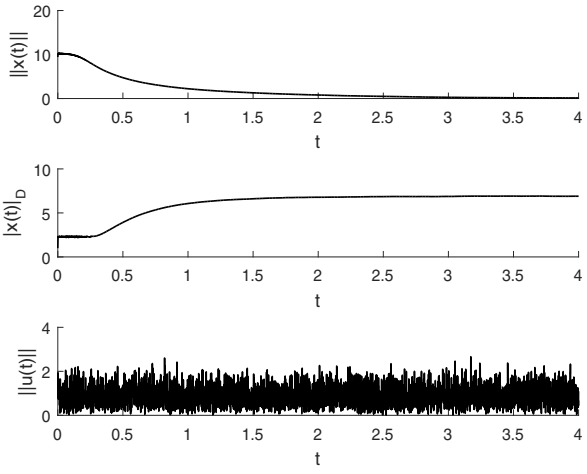

Fig. 6. The time plots of $\|x(t)\|$ and $|x(t)|_{\mathscr{D}}$ started from $x_0 = (5,8)$, and disturbance signal $u(t)$ as discussed in Example 2.

[6] B. Jayawardhana, E.P. Ryan & A.R. Teel"Bounded-Energy-Input Convergent-State Property of Dissipative Nonlinear Systems: An iISS Approach," IEEE Trans. Aut. Contr., vol. 55, no. 1, pp. 159-164, 2010.

[7] B. Jayawardhana, H. Logemann, E.P. Ryan, "The circle criterion and input-to-state stability," IEEE Contr. Syst. Mag., vol. 31, no. 4, pp. 32-67, 2011.

[8] Z.P. Jiang et.al."Small-Gain Theorem for ISS Systems and Applications", *Math. Control Signals Systems*, vol.7, pp. 95-120.

[9] A. Mehra, W-L. Ma, F. Berg, P. Tabuada, J. W. Grizzle, & A.D. Ames, "Adaptive Cruise Control: Experimental Validation of Advanced Controllers on Scale-Model Cars", Proc. Amer. Contr. Conf., pp. 1411-1418, Chicago, 2015.

[10] D. Panagou, "Distributed Coordination Control for Multi-Robot Networks Using Lyapunov-Like Barrier Functions", *IEEE Transactions on Automatic Control*, vol.PP. Issue 99.

[11] S. Prajna, A. Jadbabaie, "Safety verification of hybrid systems using Barrier certificates," Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, pp. 477-492, Springer-Verlag, 2004.

[12] J.A. Primbs, V. Nevistić, & J.C. Doyle, "Nonlinear Optimal Control: A control Lyapunov function and receding horizon perspective," Asian Journal of Control, vol. 1, no. 1, pp. 14-24, 1999.

[13] M. Z. Romdlony & B. Jayawardhana, "Uniting Control Lyapunov and Barrier Function," *IEEE Conference on Decision and Control*, Los Angeles, pp. 2293-2298, 2014.

[14] M. Z. Romdlony & B. Jayawardhana, "Passivity-Based Control with Guaranteed Safety via Interconnection and Damping Assignment," Proc. 5th IFAC Conf. Analys. Des. Hybr. Syst., p. 74-79, Georgia, 2015.

[15] M. Z. Romdlony & B. Jayawardhana, "Stabilization with Guaranteed Safety Using Control Lyapunov-Barrier Function," *Automatica*, vol. 66, pp. 39-47, 2016.

[16] M. Z. Romdlony & B. Jayawardhana, "Robustness Analysis of Systems' Safety through a New Notion of Input-to-State Safety," under review, 2016.

[17] A. J. van der Schaft, *Gain and Passivity Techniques in Nonlinear Control*, London, U.K.: Springer-Verlag, 2000.

[18] E.D. Sontag, "Smooth Stabilization Implies Coprime Factorization" *IEEE Transaction on Automatic Control*, vol. 34, no.4, 1989.

[19] E.D. Sontag, Y. Wang, "New characterization of Input-to-State stability," IEEE Trans. Aut. Contr., vol. 41, no. 9, pp. 1283-1294, 1996.

[20] X. Xu et.al., "Robustness of Control Barrier Functions for Safety Critical Control"*IFAC Conference on Analysis and Design of Hybrid Systems*, Atlanta, pp. 54-61, 2015.

[21] P. Wieland, F. Allgöwer, "Constructive safety using control barrier functions," Proc. IFAC Symp. Nonl. Contr. Syst., pp. 473-478, Pretoria, 2007.