Robustness analysis of systems' safety through a new notion of input-to-state safety

Romdlony, Muhammad Zakiyullah; Jayawardhana, Bayu

Published in:
International Journal of Robust and Nonlinear Control

DOI:
10.1002/rnc.4482

Publication date:
2019

Citation for published version (APA):
Romdlony, M. Z., & Jayawardhana, B. (2019). Robustness analysis of systems' safety through a new notion of input-to-state safety. *International Journal of Robust and Nonlinear Control*, *29*(7), 2125-2136. https://doi.org/10.1002/rnc.4482

Received: 10 April 2018 | Revised: 9 December 2018 | Accepted: 11 January 2019

DOI: 10.1002/rnc.4482

RESEARCH ARTICLE

WILEY

Robustness analysis of systems' safety through a new notion of input-to-state safety

Muhammad Zakiyullah Romdlony[1,2] | Bayu Jayawardhana[2]

[1]School of Electrical Engineering, Telkom University, Bandung, Indonesia

[2]Faculty of Science and Engineering, University of Groningen, Groningen, The Netherlands

Correspondence
Muhammad Zakiyullah Romdlony, School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia; or Faculty of Science and Engineering, University of Groningen, 9747 AG Groningen, The Netherlands.
Email: zakiyullah@telkomuniversity.ac.id

Present Address
Muhammad Zakiyullah Romdlony,
Jl. Telekomunikasi Terusan Buah Batu
Bandung 40257, Indonesia; or Nijenborgh
4 9747 AG Groningen, The Netherlands

Funding information
Indonesian government; Dutch SNN project on Region of Smart Factories; Ministry of Research, Technology and Higher Education of the Republic of Indonesia

Summary

In this paper, we propose a new robustness notion that is applicable for certifying systems' safety with respect to external disturbance signals. The proposed input-to-state safety notion allows us to certify systems' safety in the presence of the disturbances, which is analogous to the notion of input-to-state stability for analyzing systems' stability.

KEYWORDS

input-to-state safety, input-to-state stability, robust control, safety control

1 | INTRODUCTION

With the advent of complex cyber-physical systems (CPS) and industrial Internet-of-Things, the safety of integrated CPSs has become an important design feature that must be incorporated in all software levels.[1] 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 safety-critical systems, such as, biomedical devices, smart infrastructure systems, and smart energy systems.

For the past few years, a number of control design methods have 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 other works.[2-5] Ames et al[2] and Xu et al[4] 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.[6] It has been successfully implemented in the cruise control of autonomous vehicle as reported in the work of Mehra et al.[7] Another direct approach is pursued in the works of Romdlony and Jayawardhana,[5,8] which is based on the direct merging of control Lyapunov function and control barrier function. The merging process

Abbreviations: ISS, input-to-state stability; ISSf, input-to-state safety results in a control Lyapunov-barrier function, which can be used to stabilize the system with guaranteed safety by using Sontag's universal control law.

Some factual control problems in recent years, where safety certification/guarantee becomes important, are the cruise control problem in cars, control of collaborative robotic systems, and control of multiagent systems. As studied in the work of Ames et al,[2] the cruise controller in a (semi)autonomous car has to incorporate a collision avoidance control law. In this case, the presence of other cars in its surrounding can be embedded in sets of unsafe state. The uncertainties in the measured velocities and in the distance measurement can be regarded as external disturbance, and therefore, the safety needs to be certified against these disturbances. Similarly, for the collaborative robotic systems, the interaction between several robotic systems, as well as with human operators, has asked for safety guarantees from the deployed control systems. Such (distributed) control systems with guaranteed safety must also be made robust against all external disturbances that can affect all robotic systems, such as, vibrations and load variations. Lastly, for the control of multiagent systems, control issues related to obstacle and collision avoidance and area exploration and maneuvering in dynamically changing environment pose nontrivial challenges and are directly related to control with guaranteed safety.

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,[9,10] absolute stability theory,[11] input-to-state stability (ISS) theory,[12] and many others. However, analogous tools for systems' safety are still lacking which makes it difficult to carry out robustness analysis to the aforementioned results that deal with the problem of stabilization with guaranteed safety.

The seminal work of Sontag and Wang[12,13] on the characterization of ISS 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 directions with a commonality on the robustness analysis of systems' stability. However, safety and constraint aspects have not been considered in this framework. By considering the complement of the set of unsafe states, one might consider to apply recent generalization of ISS to the stability of invariant sets as in the work of Angeli and Efimov.[14] However, 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 propose a new notion of input-to-state safety (ISSf), which is an 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 decays to zero and another term that depends on the L^∞-norm of the external input signal $u(t)$, we look at the following inequality for almost all t:

$$\sigma(|x(t)|_{\mathcal{D}}) \geq \min\{\mu(|x(0)|_{\mathcal{D}}, t), \delta\} - \phi(\|u(t)\|), \tag{1}$$

where $\mathcal{D}$ is the set of unsafe states, $|x|_{\mathcal{D}}$ denotes the distance of x to $\mathcal{D}$, the function σ is strictly increasing function, μ is strictly increasing function in both arguments, $\delta > 0$ and ϕ as the gain function that is dependent on input u, akin to the ISS case. As will be discussed later in Section 3, inequality (1) will be called 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 get closer to $\mathcal{D}$. On the other hand, if there is an external input signal, then it may jeopardize the systems' safety when the input signal u is taken sufficiently large. The constant δ refers to the situation when the system is no longer attracted to the set of unsafe states (eg, the state trajectory is already sufficiently far from this set).

The above 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 et al[4] have 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 inequality (1) will make sense only if the initial conditions are bounded away from $\mathcal{D}$ by a constant that depends on the input norm.

Complementary to the work of Xu et al,[4] we adapt the ISS framework a'la Sontag to the systems' safety case through the use of ISSf barrier function which implies (1). Preliminary work on this concept has been presented in the work of Romdlony and Jayawardhana,[15] which is restricted to the case of exponential ISSf. In this paper, we extend it to general nonlinear case, as well as to the analysis of feedback interconnection.

This paper is organized as follows. In Section 2, we briefly recall the notion of stabilization with guaranteed safety of ISS and of barrier certificate. In Section 3, we introduce formally the notion of ISSf and its characterization using ISSf barrier function. In Section 4, we provide a numerical example of the aforementioned results for a simple mobile robot navigation system.

2 | PRELIMINARIES

Notation. Throughout this paper, we consider an affine nonlinear 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, $u(t) \in \mathcal{U} \subseteq \mathbb{R}^m$ denotes an (external) input or disturbance to the system. The functions $f(x)$ and $g(x)$ are $\mathcal{C}^1$, where $\mathcal{C}^1(\mathbb{R}^l, \mathbb{R}^m)$ is the space of all continuously differentiable functions $F : \mathbb{R}^l \to \mathbb{R}^m$. Without loss of generality and for simplicity of presentation, we will assume throughout that the solution to (2) is complete (ie, it exists for all $t \geq 0$) for any bounded signal u. This assumption holds when the system has the ISS property, which we will recall shortly.

For a given signal $x : \mathbb{R}_+ \to \mathbb{R}^n$, its L^p norm is given by $\|x\|_{L^p} := (\int_0^\infty \|x(t)\|^p dt)^{1/p}$ for $p = [1, \infty)$ and its L^∞ norm is defined by $\|x\|_{L^\infty} := x(\text{ess})\sup_t(\|x(t)\|)$. For a given bounded set $\mathcal{M} \subset \mathcal{X} \subset \mathbb{R}^n$, we define the distance of a point $\xi \in \mathbb{R}^n$ with respect to $\mathcal{M}$ by $|\xi|_\mathcal{M} := \min_{a \in \mathcal{M}} \|\xi - a\|$ 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 $\mathcal{P}$ and denote by $\mathcal{K}$ all functions $\alpha \in \mathcal{P}$ which satisfy $\alpha(0) = 0$. Moreover, $\mathcal{K}_\infty$ denotes all functions $\alpha \in \mathcal{K}$ which satisfy $\alpha(r) \to \infty$ as $r \to \infty$. By $\mathcal{KL}$, we denote all functions $\beta : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $\beta(\cdot, t) \in \mathcal{K}$ for a fixed $t \geq 0$ and $\beta(s, \cdot)$ is decreasing and converging to zero for a fixed $s \geq 0$. Correspondingly, we also denote by $\mathcal{KK}$ all functions $\mu : \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$ such that $\mu(0, 0) = 0$ and $\mu(s, t)$ is strictly increasing in both arguments.

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

Following safety definition in the work of Romdlony and Jayawardhana,[5] the (autonomous) system (2) with $u = 0$ is called *safe* if for all $x_0 \in \mathcal{X}_0$ and for all $t \in \overline{\mathbb{R}}_+$, $x(t) \notin \overline{\mathcal{D}}$. 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 the aforementioned work,[5] where the control problem is to design a feedback law $u = k(x)$ such that the closed-loop system is safe and asymptotically stable, ie, for all $x_0 \in \mathcal{X}_0$, we have that $x(t) \notin \mathcal{D}$ for all t and $\lim_{t\to\infty} \|x(t)\| = 0$. Moreover, when $\mathcal{X}_0 = \mathbb{R}^n \backslash \mathcal{D}$, 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 ISS framework.[12,13] Let us briefly recall the ISS concept from the work of Sontag and Wang.[12]

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

$$\|x(t)\| \leq \beta(\|x_0\|, t) + \gamma\left(\|u\|_{L^\infty([0,t))}\right). \tag{3}$$

In this notion, the functions β and γ in (3) describe the decaying effect from a nonzero 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 the works of Sontag and Wang.[12,13]

Lemma 1. *System (2) is ISS if and only if there exists a smooth $V : \mathbb{R}^n \to \mathbb{R}_+$, functions $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{K}_\infty$, and a function $\gamma \in \mathcal{K}$ 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 have 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 the work of Jiang et al[16] is based on the use of β and γ. The study of convergence input convergence state property as in the work of Jayawardhana et al[17] 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.

One may incorrectly think that the ISS inequality (3) can directly be adapted for safety analysis. First of all, we may try to infer from (3) the lower bound of $|x(t)|_{\mathcal{D}}$. In this case, we can use the triangular inequality $|0|_{\mathcal{D}} \leq |x(t)|_{\mathcal{D}}+\|x(t)\|+\text{diam}(\mathcal{D})$, where diam($\mathcal{D}$) denotes the diameter of a set $\mathcal{D}$. Using (3) and this triangular inequality relation, we get

$$\begin{aligned} |x(t)|_{\mathcal{D}} &\geq |0|_{\mathcal{D}} - \text{diam}(\mathcal{D}) - \|x(t)\| \\ &\geq (|0|_{\mathcal{D}} - \text{diam}(\mathcal{D})) - \beta(\|x_0\|, t) - \gamma\left(\|u\|_{L^\infty([0,t))}\right). \end{aligned} \tag{6}$$

This inequality gives us a very conservative estimate of the lower bound of $|x(t)|_{\mathcal{D}}$, and it is not equivalent to (1). In (1), the function μ is assumed to be of $\mathcal{KK}$ function while, in the above inequality, the function $-\beta(\cdot,\cdot)$ is neither a $\mathcal{KL}$ nor $\mathcal{KK}$ function. Qualitatively, for a given initial condition x_0 in the neighborhood of the origin and with zero input, the above inequality resembles (1). In this case, as t increases, the lower bound in (6) increases as well, similar to the qualitative behavior observed in (1). However, when we initialize it close to $\mathcal{D}$, the lower bound in (6) can become negative, and thus, the safety can no longer be guaranteed.

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 $\mathcal{D}$, a Lyapunov-like function, which is called barrier certificate has been introduced in the work of Prajna and Jadbabaie,[18] 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. Such barrier certificate is a reminiscent of Chetaev function for analyzing instability of nonlinear systems. While the Chetaev instability theorem[19,(theorem 4.3)] can be used to show that the trajectory of an autonomous system escapes a given compact set, the barrier certificate is mainly applied to show that a trajectory does not enter a given compact set. The barrier certificate theorem is summarized in following theorem.

Theorem 1. *Consider the (autonomous) system (2) with $u = 0$, ie, $\dot{x} = f(x)$ where $x(t) \in \mathcal{X} \subset \mathbb{R}^n$, with a given unsafe set $\mathcal{D} \subset \mathcal{X}$ and set of initial conditions $\mathcal{X}_0 \subset \mathcal{X}$. Assume that there exists a barrier certificate $B : \mathcal{X} \to \mathbb{R}$ satisfying*

$$B(\xi) > 0 \quad \forall \xi \in \mathcal{D} \tag{7}$$

$$B(\xi) < 0 \quad \forall \xi \in \mathcal{X}_0 \tag{8}$$

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq 0 \quad \forall \xi \in \mathcal{X} \quad \text{such that} \quad B(\xi) = 0. \tag{9}$$

Then, the system is safe.

The proof of this theorem is based on the fact that the evolution of B starting from a nonpositive value (cf (8)) will never cross the zero level set due to (9), ie, the state trajectory will always be safe according to (7).

Although the safety result as in Theorem 1 is formulated only for autonomous systems, an extension to the nonautonomous case has also been presented in the work of Prajna and Jadbabaie.[18] For the case where an external input u is considered,eg, the complete system as in (2), the safety condition (9) becomes

$$\frac{\partial B(\xi)}{\partial \xi} (f(\xi) + g(\xi)v) \leq 0 \quad \forall (\xi, v) \in \mathcal{X} \times \mathcal{U}, \tag{10}$$

where $\mathcal{U} \subset \mathbb{R}^m$ denotes the admissible set of input. However, condition (10) is a very restrictive assumption since it must hold for all $u(t) \in \mathcal{U}$ including the case when the initial condition $x(0)$ is very close to $\mathcal{D}$. It means that when we start very close to the unsafe state, the system must always remain safe for whatever type of input signals u as long as it has values in $\mathcal{U}$. 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 (10). For instance, when $\|u(\cdot)\|$ is of $\mathcal{K}$ function, the safety condition in (10) must hold for the worst-case scenario $\|u\|_{L^\infty}$ while the ISSf inequality in (1) allows for the gradual increase of $\|u(\cdot)\|$ even when it is initialized closed to the boundary of $\mathcal{D}$.

Instead of considering inequality (10), we will consider a more restrictive condition on B for our main results later, where the nonincreasing assumption of B as in (9) is replaced by a strict inequality as follows:

$$\frac{\partial B(\xi)}{\partial \xi} f(\xi) \leq -\alpha(|x|_{\mathcal{D}}), \tag{11}$$

where α is a $\mathcal{K}$ function.

In the works of Romdlony and Jayawardhana[5] and Wieland and Allöwer,[20] 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 the work of Romdlony and Jayawardhana[5] for control design methods that solve the stabilization with guaranteed safety by merging the control Lyapunov function with the control barrier function.

3 | INPUT-TO-STATE SAFETY

In this section, we will explore a new notion of ISSf 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 ISSf framework; akin to the role of Lyapunov stability theory in the ISS results.

Definition 1. System (2) is called input-to-state safe (ISSf) locally in $\mathcal{X} \subset \mathbb{R}^n$ and with respect to the set of unsafe states $\mathcal{D} \subset \mathcal{X}$ if for all $x_0 \in \mathbb{R}^n \backslash \mathcal{D}$, there exist $\sigma, \phi \in \mathcal{K}$, $\mu \in \mathcal{KK}$ and $\delta > 0$ such that

$$\sigma(|x(t)|_{\mathcal{D}}) \geq \min\{\mu(|x_0|_{\mathcal{D}}, t), \delta\} - \phi(\|u(t)\|) \tag{12}$$

holds for almost all $t \in [0, \infty)$ and for all admissible* (x_0, u), where the constant $\delta > 0$ can be dependent on boundary of $\mathcal{X}$.

If a system is ISSf, we can infer from (12) that system (2) may be brought to the unsafe state if the L^∞-norm of u is sufficiently large such that the RHS of (12) is negative. Hence, one can quantify the robustness of the system's safety with respect to an external input signal using this notion. For instance, if the initial condition x_0 is in the neighborhood of the boundary of unsafe state $\mathcal{D}$, then (12) shows that a small external input signal u may steer the state trajectory to enter $\mathcal{D}$, even when the autonomous case is safe. Since the first element on the RHS of (12) is a $\mathcal{KK}$ function, it implies that the distance between $x(t)$ and $\mathcal{D}$ is lower bounded by a strictly increasing function until $x(t)$ leaves $\mathcal{X}$. As this lower bound of the distance is nondecreasing with time, (12) means that the system can eventually withstand larger input signal.

We can also take a different view to the ISSf inequality above. If u is considered to be a disturbance signal with known magnitude, eg, $\|u\|_{L^\infty} \leq k$ with $k > 0$, then (12) provides us with information on the admissible x_0 such that the RHS of (12) remains positive so that the system under such external disturbance will remain safe.

Let us now investigate the ISS Lyapunov-like condition for ISSf of system (2).

Proposition 1. *Consider system (2) with a given unsafe set $\mathcal{D} \subset \mathcal{X} \subset \mathbb{R}^n$. Suppose that there exists an ISSf barrier function $B \in C^1(\mathbb{R}^n, \mathbb{R})$ satisfying*

$$-\alpha_1(|\xi|_{\mathcal{D}}) \leq B(\xi) \leq -\alpha_2(|\xi|_{\mathcal{D}}) \ \forall \xi \in \mathcal{X} \backslash \mathcal{D} \tag{13}$$

$$\frac{\partial B(\xi)}{\partial \xi}(f(\xi) + g(\xi)v) \leq -\alpha_3(|\xi|_{\mathcal{D}}) + \alpha_4(\|v\|)$$

$$\forall \xi \in \mathcal{X} \backslash \mathcal{D}, \forall v \in \mathcal{U}, \tag{14}$$

where $\alpha_i \in \mathcal{K}_\infty$, $i = 1, \dots, 4$. Assume further that the system is ISS.

Then, the system is input-to-state safe locally in $\mathcal{X}$ and w.r.t. $\mathcal{D}$. In particular, for any $\theta, \epsilon \in (0, 1)$ and for all $x_0 \in \mathcal{X} \backslash \overline{\mathcal{D}}$, the ISSf inequality (12) holds for all $t \geq 0$ and for all admissible (x_0, u) where $\sigma(s) = s$, $\delta = \min_{\xi \in \partial \mathcal{X}} \epsilon |\xi|_{\mathcal{D}}$,

$$\mu(s, t) = \epsilon \alpha_1^{-1}(\tilde{\alpha}(\alpha_2(s), t)) \qquad \forall s, t \geq 0$$

and

$$\phi(s) = \alpha_2^{-1} \circ \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(s)}{\theta} \qquad \forall s \geq 0,$$

*By admissible (x_0, u), we mean that the tuple is such that the RHS of (12) is strictly positive for almost all $t \geq 0$.

with $\tilde{\alpha} \in \mathcal{KK}$ being the solution of the following initial value problem:

$$\dot{y} = (1-\theta)\alpha_3 \circ \alpha_1^{-1}(y), \quad y(0) = s \in \mathbb{R}_+,$$

so that $\tilde{\alpha}(s,t) := y(t)$ for all $s \geq 0$.

Prior to proving this proposition, a few remarks can be made on the relation between the ISSf barrier function satisfying (13)-(14) and the barrier certificate satisfying (7)-(9). First, it is easy to see that condition (13) implies (8) where $\mathcal{X}_0$ in (8) is $\mathcal{X}\backslash\overline{\mathcal{D}}$. Second, when we consider the autonomous case (ie, $u = 0$), then (14) implies the strict version of (9) (cf (11)). In this proposition, $\mathcal{X}$ defines the domain where the ISSf barrier function B is active. Particularly, when $\mathcal{X}$ is bounded, then the ISSf estimate (12) holds only until x escapes $\mathcal{X}$. Trivially, the case $\mathcal{X} = \emptyset$ represents the situation where all state are safe and the case $\mathcal{X} = \mathbb{R}^n$ represents the case where all state trajectories grow unbounded. If $\mathcal{X} = \mathcal{D}$, then we do not have an input-to-safe certificate B. The latter implies also that we do not have a safety certificate for the autonomous system (eg, (2) with $u = 0$).

Proof. Let us first evaluate the solution $x(t)$ of (2) with $x_0 \in \mathcal{X}\backslash\overline{\mathcal{D}}$. From (13), it follows that $|x(t)|_{\mathcal{D}} \geq \alpha_1^{-1}(-B(x(t)))$, thus evaluating the time derivative of $B(x(t))$ gives us

$$\begin{aligned}\dot{B}(x(t)) &\leq -\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) + \alpha_4(\|u(t)\|)\\ &= -(1-\theta)\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) - \theta\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) + \alpha_4(\|u(t)\|),\end{aligned} \tag{15}$$

with $\theta \in (0,1)$ which holds whenever $x(t) \in \mathcal{X}\backslash\overline{\mathcal{D}}$.

Thus, for almost all t such that $\|u(t)\| \leq \alpha_4^{-1} \circ \theta\alpha_3 \circ \alpha_1^{-1}(-B(x(t))) =: \rho(x(t))$, inequality (15) implies that

$$\dot{B}(x(t)) \leq -(1-\theta)\alpha_3 \circ \alpha_1^{-1}(-B(x(t)))$$

holds whenever $x(t) \in \mathcal{X}\backslash\overline{\mathcal{D}}$. By letting $\tilde{B}(x(t)) = -B(x(t))$, the last inequality becomes

$$\dot{\tilde{B}}(x(t)) \geq (1-\theta)\alpha_3 \circ \alpha_1^{-1}(\tilde{B}(x(t))). \tag{16}$$

Note that function $(1-\theta)\alpha_3 \circ \alpha_1^{-1}(r)$ belongs to $\mathcal{K}$ function and the function $\tilde{B}$ is positive definite. Hence, the RHS of (16) is always positive. Now, by the comparison lemma as given in Lemma 2 in the Appendix,

$$\tilde{B}(x(t)) \geq \tilde{\alpha}(\tilde{B}(x_0), t), \tag{17}$$

where $\tilde{\alpha} \in \mathcal{KK}$ is the solution $y(t)$ of

$$\dot{y} = (1-\theta)\alpha_3 \circ \alpha_1^{-1}(y), \quad y(0) = \tilde{B}(x_0) \in \mathbb{R}_+.$$

By substituting (17) into the lower bound and upper bound of $B(x)$ in (13), it follows that

$$\begin{aligned}&\alpha_1(|x(t)|_{\mathcal{D}})v \geq \tilde{\alpha}(\tilde{B}(x_0), t) \geq \tilde{\alpha}(\alpha_2(|x_0|_{\mathcal{D}}), t)\\ &\Rightarrow \ |x(t)|_{\mathcal{D}} \geq \alpha_1^{-1}\tilde{\alpha}(\alpha_2(|x_0|_{\mathcal{D}}), t) =: \widetilde{\mu}(|x_0|_{\mathcal{D}}, t),\end{aligned} \tag{18}$$

which holds for almost all t s.t. $\|u(t)\| \leq \rho(x(t))$ and whenever $x(t) \in \mathcal{X}\backslash\overline{\mathcal{D}}$.

Now, let us consider the other case where $\|u(t)\| > \rho(x(t))$. In this case, it follows immediately that

$$\begin{aligned}&-B(x(t)) \leq \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta}\\ \Rightarrow\ &\alpha_2(|x(t)|_{\mathcal{D}}) \leq \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta}\\ \Rightarrow\ &|x(t)|_{\mathcal{D}} \leq \alpha_2^{-1} \circ \alpha_1 \circ \alpha_3^{-1} \circ \frac{\alpha_4(\|u(t)\|)}{\theta} =: \widetilde{\phi}(\|u(t)\|).\end{aligned} \tag{19}$$

We will now combine these two cases as follows. Firstly, from (18), it follows that

$$-\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) + |x(t)|_{\mathcal{D}} \geq (1-\epsilon)\widetilde{\mu}(|x_0|_{\mathcal{D}}, t) - \eta\widetilde{\phi}(\|u(t)\|), \tag{20}$$

where $\epsilon, \eta \in (0,1)$. This inequality is obtained by adding both sides of (18) by $-\epsilon\widetilde{\mu}(|x_0|_{\mathcal{D}}, t)$ and subtracting the right-hand side of (18) by $-\eta\widetilde{\phi}(\|u(t)\|)$ which is nonpositive for all $u(t)$. On the other hand, by multiplying both sides of (19) by $-\eta$ and then by adding both sides by $(1-\epsilon)\widetilde{\mu}(|x_0|_D, t)$, we get

$$(1-\epsilon)\widetilde{\mu}(|x_0|_D, t) - \eta|x(t)|_D \geq (1-\epsilon)\widetilde{\mu}(|x_0|_D, t) - \eta\widetilde{\phi}(\|u(t)\|). \tag{21}$$

Thus, (20) (which holds for $\|u(t)\| \leq \rho(x(t))$) and (21) (which is true for $\|u(t)\| > \rho(x(t))$) imply that

$$\max\left\{-\epsilon\widetilde{\mu}(|x_0|_D, t) + |x(t)|_D,\ (1-\epsilon)\widetilde{\mu}(|x_0|_D, t) - \eta|x(t)|_D\right\} \geq (1-\epsilon)\widetilde{\mu}(|x_0|_D, t) - \eta\widetilde{\phi}(\|u(t)\|) \tag{22}$$

holds for all $t \geq 0$ s.t. $x(t) \in \mathcal{X}\backslash\overline{D}$.

Since the state trajectory starts from the safe region, then for a given initial condition x_0 and bounded input u, there exists sufficiently small η, ϵ and $T_1 > 0$ such that the right-hand side of (22) and each term on the left-hand side are positive for all $t \in [0, T_1)$. Thus, since $\max\{a, b\} \leq a + b$ for $a, b \geq 0$, (22) implies that

$$\begin{aligned}
&(1-2\epsilon)\widetilde{\mu}(|x_0|_D, t) + (1-\eta)|x(t)|_D \\
&\qquad \geq (1-\epsilon)\widetilde{\mu}(|x_0|_D, t) - \eta\widetilde{\phi}(\|u(t)\|) \\
&\Leftrightarrow (1-\eta)|x(t)|_D \geq \epsilon\widetilde{\mu}(|x_0|_D, t) - \eta\widetilde{\phi}(\|u(t)\|) \\
&\Leftrightarrow |x(t)|_D \geq \frac{\epsilon}{1-\eta}\widetilde{\mu}(|x_0|_D, t) - \frac{\eta}{1-\eta}\widetilde{\phi}(\|u(t)\|)
\end{aligned} \tag{23}$$

holds for almost all $t \in [0, T_1)$.

We will prove now that we can extend the time interval, where (23) is valid, to $[0, T_{1,\max})$ with finite $T_{1,\max} < \infty$ if x leaves the set $\mathcal{X}$ at time $T_{1,\max}$, or $T_{1,\max} = \infty$ when x stays in $\mathcal{X}\backslash\overline{D}$ at all time. In particular, we show that we can choose η and ϵ such that both terms on the LHS of (22) are positive for almost all $t \in [0, T_{1,\max})$, so that (23) holds accordingly.

Firstly, let us show that for any $\epsilon \in (0, 1)$, there exists $\eta \in (0, 1)$ such that

$$|x(t)|_D \leq \frac{1-\epsilon}{\eta}\widetilde{\mu}(|x_0|_D, t) \qquad \forall t \in [0, \infty). \tag{24}$$

Since the system is ISS, there exists $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}_\infty$ such that

$$\begin{aligned}
|x(t)| &\leq \beta(|x_0|, t) + \gamma(\|u\|_{L^\infty}) \\
&\leq \beta(|x_0|, 0) + \gamma(\|u\|_{L^\infty}) =: D_1.
\end{aligned}$$

By triangular inequality and by denoting $D_2 = \max_{\xi\in D}|\xi|$, it follows that

$$\begin{aligned}
|x(t)|_D &\leq D_2 + |x(t)| \leq D_1 + D_2 \\
&\leq \frac{D_1 + D_2}{\widetilde{\mu}(|x_0|_D, 0)}\widetilde{\mu}(|x_0|_D, t),
\end{aligned} \tag{25}$$

where the last inequality is due to the fact that $\widetilde{\mu}(|x_0|_D, t) \geq \widetilde{\mu}(|x_0|_D, 0)$ for all $t \geq 0$. Thus, by taking

$$\eta = \min\left\{0.5, \frac{(1-\epsilon)\widetilde{\mu}(|x_0|_D, 0)}{D_1 + D_2}\right\} \in (0, 0.5], \tag{26}$$

inequality (25) implies that (24) holds for all $t \geq 0$. Hence, the second term on the LHS of (22) is always positive for all t.

It remains now to check whether

$$|x(t)|_D > \epsilon\widetilde{\mu}(|x_0|_D, t)$$

for all $t \in [0, T_{1,\max})$. We will show this by contradiction. Suppose that there is a finite $\tau < T_{1,\max}$ that defines the time when $|x(\tau)|_D = \epsilon\widetilde{\mu}(|x_0|_D, \tau)$. In this case, (23) still holds and we have that

$$\begin{aligned}
|x(\tau)|_D &\geq \frac{\epsilon}{1-\eta}\widetilde{\mu}(|x_0|_D, \tau) - \frac{\eta}{1-\eta}\widetilde{\phi}(\|u(\tau)\|) \\
&= \epsilon\widetilde{\mu}(|x_0|_D, \tau) + \frac{\eta}{1-\eta}\left(\epsilon\widetilde{\mu}(|x_0|_D, \tau) - \widetilde{\phi}(\|u(\tau)\|)\right).
\end{aligned}$$

Since $\widetilde{\phi}(\|u(t)\|) < \epsilon\widetilde{\mu}(|x_0|_D, t)$ for all $t \geq 0$ (by hypothesis of the proposition on the admissibility of (x_0, u) with $\mu = \epsilon\widetilde{\mu}$ and $\widetilde{\phi} = \phi$), it follows from the above inequality that

$$|x(\tau)|_D > \epsilon\widetilde{\mu}(|x_0|_D, \tau),$$

which is a contradiction. Thus, we have that (23) holds for almost all $t \in [0, T_{1,\max})$.

Finally, we will derive the conservative lower bound of (23) such that it will no longer depend on η (which is currently dependent on x_0 and u as in (26)). By the definition of η in (26), it is trivial to check that $0 < \eta < 0.5$,

$$1 < \frac{1}{1-\eta} < 2 \text{ and } 0 > \frac{-\eta}{1-\eta} > -1.$$

Thus, (23) implies that

$$|x(t)|_D \geq \epsilon\widetilde{\mu}(|x_0|_D, t) - \widetilde{\phi}(\|u(t)\|) \tag{27}$$

for almost all $t \in [0, T_{1,\max})$.

On the other hand, by defining $\kappa := \min_{\xi \in \partial \mathcal{X}} |\xi|_D > 0$, we have that when $x(t) \notin \mathcal{X}$ (including for the second case when $x_0 \notin \mathcal{X}$),

$$|x(t)|_D \geq \kappa \geq \kappa - \widetilde{\phi}(\|u(t)\|). \tag{28}$$

Once x leaves $\mathcal{X}$ and enters again $\mathcal{X}$ at a later time interval, then we can use again the argument as before where the initial condition is taken in the neighborhood of the boundary of $\mathcal{X}$. Indeed, suppose that x enters again $\mathcal{X}$ at time $T_2 > T_{1,\max}$. Then, by following the same argument as before, we get

$$\begin{aligned} |x(t)|_D &\geq \epsilon\widetilde{\mu}(|x(T_2)|_D, t - T_2) - \widetilde{\phi}(\|u(t)\|) \\ &\geq \epsilon\widetilde{\mu}(\kappa, 0) - \widetilde{\phi}(\|u(t)\|), \end{aligned} \tag{29}$$

for almost all $t \in [T_2, T_{2,\max})$ where $T_{2,\max}$ is the maximum time where x remains in $\mathcal{X}$.

Since in all of these cases, $|x(t)|_D$ satisfies either (27), (28), or (29) in different time intervals, we can combine them by taking the minimum of their lower bounds. Thus, by defining $\delta := \epsilon\widetilde{\mu}(\kappa, 0)$ with κ as defined before (28),

$$\begin{aligned} |x(t)|_D &\geq \min\{\epsilon\widetilde{\mu}(|x_0|_D, t), \kappa, \epsilon\widetilde{\mu}(\kappa, 0)\} - \widetilde{\phi}(\|u(t)\|) \\ &= \min\{\epsilon\widetilde{\mu}(|x_0|_D, t), \delta\} - \widetilde{\phi}(\|u(t)\|) \end{aligned}$$

holds for almost all $t \in [0, \infty)$.

Hence, we have ISSf with $\mu = \epsilon\widetilde{\mu}$ and $\phi = \widetilde{\phi}$, where $\widetilde{\mu}$ and $\widetilde{\phi}$ are as in (18) and (19), respectively, and δ as defined above. Note that the choice of $\epsilon \in (0, 1)$ is, in this case, independent of admissible tuple (x_0, u). □

The ISS assumption in this proposition can be relaxed by weaker conditions that can guarantee the boundedness of $|x(t)|_D$ so that inequality (24) in the proof of Proposition 1 holds. For instance, we can assume that the system is integral input-to-state stable or it is practically input-to-state stable.

One can see from Proposition 1 that the inequalities in (13) and (14) are reminiscent to those used in the study of ISS Lyapunov function. In this context, inequality (14) resembles the dissipation inequality in the ISS Lyapunov function and the growth of B as in (13) can be linked to the growth of V as in (4), albeit they grow with different sign as well as with different metric norm.

4 | SIMULATION RESULT

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

$$\begin{aligned} \dot{x}_1 &= v_1 + u_1 \\ \dot{x}_2 &= v_2 + u_2, \end{aligned} \tag{30}$$

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 a bounded disturbance signal. Assume a given unsafe set $\mathcal{D} := \{x \in \mathbb{R}^2 | (x_1 - 4)^2 + (x_2 - 6)^2 < 4\}$ and $\mathcal{X} := \{x \in \mathbb{R}^2 | (x_1 - 4)^2 + (x_2 - 6)^2 < 9\}$.

For designing a safety control law in $\mathcal{X}$ that is robust with respect to u, ie, it is ISSf w.r.t. u, let us consider a gradient-based control law given by

$$\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = -\nabla_x B(x) = -\frac{\partial B(x)}{\partial x}^T \qquad \forall x \in \mathcal{X}, \tag{31}$$

where

$$B(x) = -|x|_D^2 = -(x_1-4)^2 - (x_2-6)^2 + 4\sqrt{(x_1-4)^2 + (x_2-6)^2} - 4.$$

The function B as above will later serve as our candidate for the ISSf barrier function. A routine computation on the gradient of $B(x)$ and its norm shows that

$$\frac{\partial B(x)}{\partial x} = \left[-2(x_1-4) + 2\frac{2(x_1-4)}{\sqrt{(x_1-4)^2+(x_2-6)^2}} \qquad -2(x_2-6) + 2\frac{2(x_2-6)}{\sqrt{(x_1-4)^2+(x_2-6)^2}} \right]$$

and

$$\begin{aligned} \left\| \frac{\partial B(x)}{\partial x} \right\|^2 &= 4(x_1-4)^2 - 16\frac{(x_1-4)^2}{\sqrt{(x_1-4)^2+(x_2-6)^2}} + 16\frac{(x_1-4)^2}{(x_1-4)^2+(x_2-6)^2} \\ &\quad + 4(x_2-6)^2 - 16\frac{(x_2-6)^2}{\sqrt{(x_1-4)^2+(x_2-6)^2}} + 16\frac{(x_2-6)^2}{(x_1-4)^2+(x_2-6)^2} \\ &= 4(x_1-4)^2 + 4(x_2-6)^2 - 16\sqrt{(x_1-4)^2+(x_2-6)^2} + 16 \\ &= 4|x|_D^2. \end{aligned}$$

From the construction of $B(x)$, we can immediately take $\alpha_1(|x|_D) = \alpha_2(|x|_D) = |x|_D^2$. Its time derivative satisfies

$$\dot{B}(x) = \frac{\partial B(x)}{\partial x}\left(-\frac{\partial B(x)}{\partial x}^T + u \right) \tag{32}$$

$$\leq -\left\|\frac{\partial B}{\partial x}\right\|^2 + \left\|\frac{\partial B}{\partial x}\right\| \|u\| \tag{33}$$

$$\leq -4|x|_D^2 + 2|x|_D^2 + \frac{1}{2}\|u\|^2 = -2|x|_D^2 + \frac{1}{2}\|u\|^2. \tag{34}$$

In other words, $\alpha_3(|x|_D) = -2|x|_D^2$ and $\alpha_4(\|u\|) = 0.5\|u\|^2$. Accordingly, the initial value problem of y in Proposition 1 is given by

$$\dot{y} = (1-\theta)2y.$$

By taking $\theta = 0.5$, we have that $\dot{y} = y$ and $y(t) = e^t y(0)$. Following the same notation as in Proposition 1, $\tilde{\alpha}(y(0), t) := y(t) = e^t y(0)$ for all $y(0) \geq 0$. Therefore, according to Proposition 1, we have that

$$\sigma(|x(t)|_D) \geq \min\{\mu(|x_0|_D, t), \delta\} - \phi(\|u(t)\|), \tag{35}$$

where $\sigma(|x(t)|_D) = |x(t)|_D$, $\delta = \min_{x\in\partial\mathcal{X}} \epsilon|x|_D = 0.5$. By letting $\epsilon = 0.5$ and $\theta = 0.5$, it follows from the result in Proposition 1 that

$$\begin{aligned} \mu(|x_0|_D, t) &= \epsilon\alpha_1^{-1}(\tilde{\alpha}(\alpha_2(|x_0|_D), t)) = 0.5\alpha_1^{-1}\left(e^t|x_0|_D^2\right) \\ &= 0.5e^{0.5t}|x_0|_D \end{aligned}$$

and

$$\phi(\|u(t)\|) = \alpha_2^{-1}\circ\alpha_1\circ\alpha_3^{-1}\circ\frac{\alpha_4(\|u(t)\|)}{\theta} = \frac{1}{\sqrt{2}}\|u(t)\|.$$

Therefore, the ISSf barrier function B fulfills all hypotheses in Proposition 1 and we have

$$|x(t)|_D \geq \min\left\{0.5e^{0.5t}|x_0|_D, 0.5\right\} - \frac{1}{\sqrt{2}}\|u(t)\|. \tag{36}$$

For numerical simulation, let us consider an initial condition $x_0 = (6.1, 6)$. In this case, $|x_0|_D = 0.1$ and according to our previous estimate in (36), the state trajectory x satisfies

$$|x(t)|_D \geq \min\left\{0.05e^{0.5t}, 0.5\right\} - \frac{1}{\sqrt{2}}\|u(t)\|. \tag{37}$$

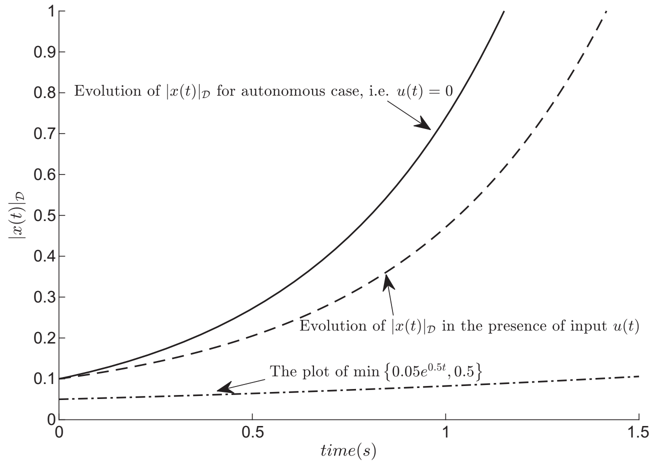

FIGURE 1 The numerical simulation results of the closed-loop system (30) with the control law (31) with $x_0 = (6.1, 6)$. The solid line shows the evolution of $|x(t)|_D$ without any presence of disturbance u. The dash-dotted line is the plot of $\min\{0.05e^{0.5t}, 0.5\}$ (ie, the first term on the RHS of (37)). The dashed line is the evolution of $|x(t)|_D$ under the presence of u as given in (38)

In Figure 1, the trajectory in solid line shows the evolution of $|x(t)|_D$ without any presence of disturbance input u, ie, $u(t) = 0$. In this Figure, the estimate of $\min\{0.05e^{0.5t}, 0.5\}$ (the first term on the RHS of (37)) is shown in dashed line and we can see that $|x(t)|_D$ remains always greater than our lower-bound estimate. In order to show the influence of disturbance input u while guaranteeing the closed-loop systems' safety according to (37), let us consider the following disturbance signal:

$$u(t) = \begin{bmatrix} -0.07\min\{e^{0.5t}, 10\} \\ 0 \end{bmatrix} \qquad \forall t \geq 0. \tag{38}$$

Using the above u, it can be computed that the right-hand side of (37) remains positive for all time. The resulting trajectory x with such disturbance u is shown in Figure 1 in dash-dotted line. We can see that the disturbance u has an influence to the growth of $|x(t)|_D$. In particular, it counteracts the safety control law in (31) and the use of ISSf has allowed us to certify the safety of the closed-loop system under such input signal, as also verified by the numerical simulation. The numerical simulation also shows that our computation for the lower-bound is a conservative estimate.

5 | CONCLUSION

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

ACKNOWLEDGEMENTS

This project is supported by the Indonesian government, Dutch SNN project on Region of Smart Factories and by the Ministry of Research, Technology and Higher Education of the Republic of Indonesia.

ORCID

Muhammad Zakiyullah Romdlony https://orcid.org/0000-0003-3576-2120

REFERENCES

1. Banerjee A, Venkatasubramanian KK, Mukherjee T, Gupta SKS. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proc IEEE*. 2011;100(1):283-299.
2. Ames AD, Grizzle JW, Tabuada P. Control barrier function based quadratic programs with application to adaptive cruise control. In: Proceedings of the 53rd IEEE Conference on Decision and Control; 2014; Los Angeles, CA.

3. Romdlony MZ, Jayawardhana B. Passivity-based control with guaranteed safety via interconnection and damping assignment. Paper presented at: 5th IFAC Conference on Analysis and Design of Hybrid Systems; 2015; Atlanta, GA.
4. Xu X, Tabuada P, Grizzle JW, Ames AD. Robustness of control barrier functions for safety critical control. Paper presented at: 5th IFAC Conference on Analysis and Design of Hybrid Systems; 2015; Atlanta, GA.
5. Romdlony MZ, Jayawardhana B. Stabilization with guaranteed safety using control Lyapunov–barrier function. *Automatica*. 2016;66:39-47.
6. Primbs JA, Nevistić V, Doyle JC. Nonlinear optimal control: a control Lyapunov function and receding horizon perspective. *Asian J Control*. 1999;1(1):14-24.
7. Mehra A, Ma W-L, Berg F, Tabuada P, Grizzle JW, Ames AD. Adaptive cruise control: experimental validation of advanced controllers on scale-model cars. In: Proceedings of 2015 American Control Conference (ACC); 2015; Chicago, IL.
8. Romdlony MZ, Jayawardhana B. Uniting control Lyapunov and control Barrier functions. Paper presented at: 53rd IEEE Conference on Decision and Control; 2014; Los Angeles, CA.
9. Jayawardhana B, Weiss G. State convergence of passive nonlinear systems with an L^2 input. *IEEE Trans Autom Control*. 2009;54(7):1723-1727.
10. van der Schaft AJ. *L_2-Gain and Passivity Techniques in Nonlinear Control*. London, UK: Springer-Verlag London Limited; 2000.
11. Jayawardhana B, Logemann H, Ryan EP. The circle criterion and input-to-state stability. *IEEE Control Syst Mag*. 2011;31(4):32-67.
12. Sontag ED, Wang Y. New characterization of input-to-state stability. *IEEE Trans Autom Control*. 1996;41(9):1283-1294.
13. Sontag ED. Smooth stabilization implies coprime factorization. *IEEE Trans Autom Control*. 1989;34(4):435-443.
14. Angeli D, Efimov D. Characterizations of input-to-state stability for systems with multiple invariant sets. *IEEE Trans Autom Control*. 2015;60(12):3242-3256.
15. Romdlony MZ, Jayawardhana B. On the new notion of input-to-state safety. Paper presented at: 2016 IEEE 55th Conference on Decision and Control (CDC); 2016; Las Vegas, NV.
16. Jiang ZP, Teel AR, Praly L. Small-gain theorem for ISS systems and applications. *Math Control Signals Syst*. 1994;7(2):95-120.
17. Jayawardhana B, Ryan EP, Teel AR. Bounded-energy-input convergent-state property of dissipative nonlinear systems: an iISS approach. *IEEE Trans Autom Control*. 2010;55(1):159-164.
18. Prajna S, Jadbabaie A. Safety verification of hybrid systems using barrier certificates. In: *Hybrid Systems: Computation and Control*. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2004;477-492. *Lecture Notes in Computer Science*; vol 2993.
19. Khalil HK. *Nonlinear Systems*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall; 2000.
20. Wieland P, Allöwer F. Constructive safety using control barrier functions. In: Proceedings of the 7th IFAC Symposium on Nonlinear Control Systems; 2007; Pretoria, South Africa.

How to cite this article: Romdlony MZ, Jayawardhana B. Robustness analysis of systems' safety through a new notion of input-to-state safety. *Int J Robust Nonlinear Control*. 2019;29:2125–2136. https://doi.org/10.1002/rnc.4482

APPENDIX

Lemma 2. *Consider a nonautonomous system described by*

$$\dot{w} = h(t, w) \qquad w(t_0) = w_0, \tag{A1}$$

where h is continuous in t and locally Lipschitz in w, for all $t \geq t_0$. Assume that the solution of (A1) is complete, ie, its maximal interval is $[t_0, \infty)$. Let z be an absolutely continuous function such that its upper right-hand derivative $D^+z(t)$ satisfies

$$D^+z(t) \geq h(t, z(t)) \qquad z(t_0) \geq w_0. \tag{A2}$$

Then, $z(t) \geq w(t)$ for all $t \geq t_0$.

Proof. For a given constant $\lambda > 0$, let us consider the solution $y(t, \lambda)$ of

$$\dot{y} = h(t, y) - \lambda,$$

which evolves in a "tube" around w for a sufficiently small λ and y_0 in the neighborhood of w_0. Following theorem 3.5 in the work of Khalil,[19] on any compact interval $[t_0, t_1]$, for any $\epsilon > 0$, there is $\delta > 0$ such that if $\lambda < \delta$, then $y(t, \lambda)$ is defined on $[t_0, t_1]$ and

$$|y(t, \lambda) - w(t)| < \epsilon \qquad \forall t \in [t_0, t_1].$$

Firstly, it can be shown that within this time interval, $z(t) \geq y(t, \lambda)$. Indeed, by contradiction, suppose that there is a time interval $[t_2, t_3] \subset [t_0, t_1]$ such that $z(t_2) = y(t_2, \lambda)$ and $z(t) < y(t, \lambda)$ for all $t_2 < t \geq t_3$. This implies that

$$z(t) - z(t_2) < y(t, \lambda) - y(t_2, \lambda) \qquad \forall t \in (t_2, t_3]$$

and thus $D^+z(t_2) \leq \dot{y}(t_2, \lambda) = h(t_2, y(t_2, \lambda)) - \lambda < h(t_2, y(t_2, \lambda)) = h(t_2, z(t_2))$. This contradicts (A2) and thus $z(t) \geq y(t, \lambda)$ for all $t \in [t_0, t_1]$.

We can now show that $z(t) \geq w(t)$ for all $t \in [t_0, t_1]$. We prove this again by contradiction. Suppose that there is a time $t_4 \in [t_0, t_1]$ such that $z(t_4) < w(t_4)$. Let us take $\epsilon = (w(t_4) - z(t_4))/2$. Using the previous "tube" solution, it follows that

$$y(t_4, \lambda) - z(t_4) = y(t_4, \lambda) - w(t_4) + w(t_4) - z(t_4) \geq \epsilon,$$

which contradicts the previous claim that $z(t) \geq y(t, \lambda)$ for all $t \in [t_0, t_1]$.

We have shown that $z(t) \geq w(t)$ for all $t \in [t_0, t_1]$. In order to show that t_1 can be extended to ∞, let us assume that $t_5 < \infty$ be the first time that this inequality is violated such that $z(t_5) = w(t_5)$ and $z(t) < w(t)$ for some time $t > t_5$. As we have that $z(t_5) = w(t_5)$, we can again use the same arguments as before to extend inequality $z(t) \geq w(t)$ for all $t \in [t_5, t_6]$ for some $t_6 > t_5$, which is a contradiction. Therefore, $z(t) \geq w(t)$ for all $t \geq t_0$. □