Safety controller design for incrementally stable switched systems using event-based symbolic models

Zohra Kader, Adnane Saoud, Antoine Girard

Safety controller design for incrementally stable switched systems using event-based symbolic models

Zohra Kader[1], Adnane Saoud[1,2], Antoine Girard[1]

Abstract— **In this paper, we investigate the problem of lazy safety controllers synthesis for event-based symbolic models of incrementally stable switched systems with aperiodic time sampling. First of all, we provide a novel event-based scheme for symbolic models design. The obtained symbolic models are computed while considering all transitions of different durations satisfying a triggering condition. In addition, they are related to the original switched system by a feedback refinement relation and thus useful for control applications. Then, using the particular structure of the obtained event-based symbolic model, a lazy safety controller is designed while choosing transitions of longest durations. Secondly, for the same state sampling parameter and desired precision, we show that the obtained event-based symbolic model is related by a feedback refinement relation to the classical symbolic model designed for incrementally stable switched systems with periodic time sampling. Based on this relationship, we prove analytically that the size of the set of controllable states obtained with the lazy safety controller designed for an event-based symbolic model is larger than the one obtained with a safety controller designed for the classical symbolic model. Finally, an illustrative example is proposed in order to show the efficiency of the proposed method and simulations are performed for a Boost DC-DC converter structure.**

I. INTRODUCTION

Switched systems have attracted a wide interest of the control community during the last decades [9]. The heterogeneous nature of this class of hybrid systems renders their study more complex and thus limits the investigated problems to stability and stabilization [12], [7]. Recently, several approaches based on the use of symbolic models, also called discrete abstractions, for controller design have been proposed [13]. These studies have been motivated by technology advances which demand that more complex control objectives like safety properties, language and logic specifications be considered. Moreover, the use of discrete abstraction for control design becomes more interesting when the obtained symbolic model is finite. Indeed, in this case, the problem of controller design can be efficiently solved using the mature methods obtained for supervisory control design for discrete-event systems.

Based on the Lyapunov theory, several constructive approaches of symbolic models for incrementally stable switched systems have been proposed last years. For instance, we can cite the work proposed in [6] where a symbolic model has been designed using both state and time discretization. In that paper, the obtained symbolic model is related to the original system by an approximate bisimulation relation.

Here, we are interested in lazy safety controllers synthesis for symbolic models of switched systems with aperiodic time sampling. First of all, we provide a novel event-based scheme for symbolic models design. Contrarily to the event-based symbolic approach proposed in [8] where only transitions of shorter durations are considered, here the symbolic model is computed while considering all transitions of different durations satisfying a triggering condition. In this paper, we show that the obtained symbolic abstraction is related to the original switched system by a feedback refinement relation [11] and is thus useful for control applications. Then, using the particular structure of the obtained event-based symbolic model a lazy safety controller that keeps the trajectory of the closed-loop system in the safe set while choosing transitions of longest durations is designed. Secondly, for the same sampling state parameter and desired precision, we show that the obtained event-based symbolic model is related by a feedback refinement relation to the classical symbolic model designed for switched systems with periodic time sampling. Based on this relationship, we provide an analytic proof of the fact that the set of controllable states obtained with a safety controller designed for the classical symbolic model with a periodic time sampling is included in the one obtained with the lazy safety controller designed for the event-based symbolic model. This result has not been shown in the literature.

This paper is structured as follows. In Section II, the class of switched systems under study is described and some required preliminaries and definitions are provided. A novel event-based scheme for symbolic models design for incrementally stable switched systems is proposed in Section III. In addition, a feedback refinement relation from the obtained event-based symbolic model to the classical symbolic model designed for incrementally stable switched systems with periodic time sampling is provided in the same section. In Section IV, a lazy safety controller is designed for the event-based symbolic model. Moreover, using the result obtained in Section III, we provide analytic proof of the fact

*This work has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No 725144). This research has been partially supported by Labex DigiCosme (project ANR-11-LABEX-0045-DIGICOSME) operated by ANR as part of the program "Investissement d'Avenir" Idex Paris Saclay (ANR-11-IDEX-0003-02).

[1]Laboratoire des Signaux et Systèmes (L2S), CNRS, CentraleSupélec, Université Paris-Sud, Université Paris-Saclay, 3, rue Joliot-Curie, 91192 Gif-sur-Yvette, cedex, France. {zohra.kader,antoine.girard}@l2s.centralesupelec.fr

[2]Laboratoire Spécification et Vérification, CNRS, ENS Paris-Saclay, 61, avenue du Président Wilson, 94235 Cachan Cedex, France. {adnane.saoud}@l2s.centralesupelec.fr

that the set of the controllable states obtained with the lazy safety controller is larger than the one obtained with a safety controller designed for the classical symbolic model. In Section V, an illustrative example is proposed in order to show the efficiency of the proposed method and simulations are performed for a Boost DC-DC converter structure. Section VI ends the paper with concluding remarks. Proofs of all theorems and lemmas can be find in the Appendices.

Notations.: In this paper we use the notations $\mathbb{R}$, $\mathbb{R}_0^+$ and $\mathbb{R}^+$ to refer to the set of real, non-negative real, and positive real numbers, respectively. $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{N}^+$ refer to the sets of integers, of non-negative integers and of positive integers, respectively. card($\mathscr{S}$) refers to the cardinal of a set $\mathscr{S}$. $\|x\|$ denotes the Euclidean norm of a vector $x \in \mathbb{R}^n$ and $x_{(i)}$ refers to its i-th row. A continuous function γ is said to belong to class $\mathscr{K}$ if it is strictly increasing and $\gamma(0) = 0$. It is said to belong to class $\mathscr{K}_\infty$ if γ is $\mathscr{K}$ and $\gamma(r)$ goes to infinity as r tends to infinity. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathscr{KL}$ if : for any fixed r, the map $\beta(.,s)$ belongs to the class $\mathscr{K}$, and for each fixed s the map $\beta(r,.)$ is strictly decreasing and $\beta(r,.)$ goes to zero as s tends to infinity.

II. Preliminaries and problem statement

A. System description

In this paper we consider the class of switched systems defined as follows:

Definition 1: A switched system is a quadruple $\Sigma = (\mathbb{R}^n, P, \mathscr{P}, F)$, where:

- $\mathbb{R}^n$ is the state space;
- P is the finite set of modes $P = \{1, \ldots, m\}$;
- $\mathscr{P}$ is a subset of $S(\mathbb{R}_0^+, P)$ which denotes the set of piecewise constant and right continuous functions σ from $\mathbb{R}_0^+$ to the finite set of modes P, with a finite number of discontinuities on every bounded interval of $\mathbb{R}_0^+$. This guarantees the absence of Zeno behaviors.
- $F = \{f_1, \ldots, f_m\}$ is a collection of vector fields indexed by P.

The continuous subsystems Σ_p of the switched system Σ are defined by the following differential equation:

$$\dot{\mathtt{x}}(t) = f_p(\mathtt{x}(t)), \forall p \in P. \tag{1}$$

We assume that for all $p \in P$ the vector field $f_p : \mathbb{R}^n \to \mathbb{R}^n$ is locally Lipschitz continuous map and forward complete. Under this assumption, solutions of (1) are unique and defined for all $t \in \mathbb{R}_0^+$. Necessary and sufficient conditions for forward completeness of a system have been provided in [2]. From now on, $\mathtt{x}(t, x, \sigma)$ will denote the point reached by the trajectory of Σ at time $t \in \mathbb{R}_0^+$ from the initial state x under the switching signal σ.

B. Incremental stability of switched systems

In order to construct symbolic models for switched systems, we use the notion of incremental stability [1], [6]. Loosely speaking, incremental stability means that independently of their initial states, all the trajectories induced by the same switching signal converge to the same reference trajectory. In [6], the notion of incremental stability of switched systems has been characterized using Lyapunov functions as follows:

Definition 2: A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ is a *common δ-GUAS Lyapunov function* for system Σ if there exist $\mathscr{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x, y \in \mathbb{R}^n$, for all $p \in P$

$$\underline{\alpha}(\|x-y\|) \leq V(x,y) \leq \overline{\alpha}(\|x-y\|); \tag{2}$$

and

$$\frac{\partial V}{\partial x}(x,y) f_p(x) + \frac{\partial V}{\partial y}(x,y) f_p(y) \leq -\kappa V(x,y). \tag{3}$$

In the sequel we assume that:

A-1 There exists a common δ-GUAS Lyapunov function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ for subsystems Σ_p;

A-2 There exists a $\mathscr{K}_\infty$ function γ such that

$$\forall x, y, z \in \mathbb{R}^n, |V(x,y) - V(x,z)| \leq \gamma(\|x-y\|). \tag{4}$$

Assumption A-2 has been already used in [6]. It has been shown that this assumption is satisfied provided that the dynamics of the switched system are considered on a compact set $\mathscr{S} \subset \mathbb{R}^n$ and the Lyapunov function V is of class C^1 on $\mathscr{S}$. In this case, we have

$$\forall x, y, z \in \mathscr{S}, \ |V(x,y) - V(x,z)| \leq c\|x-y\|, \tag{5}$$

with $c = \max_{x,y \in \mathscr{S}} \|\frac{\partial V}{\partial y}(x,y)\|$. Thus, (4) is verified for linear $\mathscr{K}_\infty$ function given by $\gamma(s) = cs$. Moreover, note that for all $x \in \mathbb{R}^n$ we have $V(x,x) = 0$, then

$$V(x,y) \leq |V(x,y) - V(x,x)| \leq \gamma(\|x-y\|), \tag{6}$$

for all $x, y \in \mathbb{R}^n$. Thus, considering that the right inequality in (2) holds with $\overline{\alpha} = \gamma$ does not induce any loss of generality.

C. Transition systems

In what follows, we recall the concept of transition systems that allows to describe both switched systems and symbolic models in the same framework:

Definition 3: A transition system is a tuple $T = (Q, U, O, \Delta)$ where Q is a set of states, U is a set of inputs, O is a set of outputs, and $\Delta \subseteq Q \times U \times Q \times O$ is a transition relation. T is said to be *metric* if the set of outputs O is equipped with a metric d such that $d(o_1, o_2) = \|o_1 - o_2\|$, *symbolic* if Q and U are finite or countable sets.

In this paper, $(q', o) \in \Delta(q, u)$ will denote the transition $(q, u, q', o) \in \Delta$. This means that under the input u the trajectory of the transition system starting from the state q will evolve to the state q' while providing the output o. Here, we consider that the set of initial states for the transition system coincide with the set of states Q. Given a state $q \in Q$, an input $u \in U$ is said to belong to the set of *enabled* inputs, denoted by $\mathrm{Enab}_\Delta(q)$, if $\Delta(q,u) \neq \emptyset$. A state $q \in Q$ is said to be blocking if $\mathrm{Enab}_\Delta(q) = \emptyset$, it is said non-blocking otherwise. T is said to be *deterministic* if for all $q \in Q$ and for all $u \in \mathrm{Enab}_\Delta(q)$, $\mathrm{card}(\Delta(q,u)) = 1$, *non-blocking* if all its states are non-blocking. In this paper, only deterministic transition systems are considered.

The dynamics of the switched system (1) can be described by a transition system. Indeed, to the switched system $\Sigma = (\mathbb{R}^n, P, \mathscr{P}, F)$ we can associate the transition system $T(\Sigma) = (Q, U, O, \Delta)$ where $Q = \mathbb{R}^n$ is the set of states, $U = P \times \mathbb{R}^+$ is the set of labels, O is the set of outputs, Δ is the transition relation defined as follows: $\forall q, q' \in Q, \forall (p,\tau) \in U$, $\forall o \in O$, $(q', o) \in \Delta(q,(p,\tau))$ if and only if $\mathtt{x}(\tau, q, p) = q'$ and $o = q$, i.e., when the mode p is active for a duration τ, the trajectory of the switched system Σ starting from q evolves to the state q'. Note that the transition system $T(\Sigma)$ is not *symbolic* (U and Q are not finite sets).

In order to design symbolic models for switched systems, we consider the *ε-approximate feedback refinement relation*. This relation is a simulation relation and it is suitable for controllers design.

Definition 4: Let $T_i = (Q_i, U, O, \Delta_i)$, with $i = 1, 2$ be two metric transition systems with the same input set U and the same output set O equipped with the metric d. Let $\varepsilon > 0$ be a given precision. A relation $\mathscr{R} \subseteq Q_1 \times Q_2$ is said to be an *ε-approximate feedback refinement relation* from T_1 to T_2 if for all $(q_1, q_2) \in \mathscr{R}$

$$Enab(q_2) \subseteq Enab(q_1);$$

for all $u \in Enab(q_2)$

$$\forall (q_1', o_1) \in \Delta_1(q_1, u), \exists (q_2', o_2) \in \Delta_2(q_2, u)$$
$$\text{such that } d(o_1, o_2) \leq \varepsilon \text{ and } (q_1', q_2') \in \mathscr{R};$$

and for all $q_1 \in Q_1$

$$\exists q_2 \in Q_2, \text{ such that } (q_1, q_2) \in \mathscr{R}.$$

When $\varepsilon = 0$, $\mathscr{R}$ is said to be a *feedback refinement relation*.

D. Safety controller synthesis

Let the transition system $T = (Q, U, O, \Delta)$ and $Q_s \subseteq Q$ be a safe set. We consider the synthesis problem that consists in determining a controller that keeps the states of the system inside the set of safety specification Q_s. For the system T and the set Q_s, a state $q \in Q_s$ is controllable if there exists an infinite sequence of transitions of T initialized in q and remaining in Q_s for all time. This set can be formally defined as follows.

Definition 5: A state q of a deterministic transition system T is controllable with respect to the safe set Q_s if $q \in Q_s$ and for all $r \in \mathbb{N}^+$, there exists a sequence of inputs $u_0, \ldots, u_r$ with $(q_{i+1}, o_{i+1}) \in \Delta(q_i, u_i)$ for all $i \in \{1, \ldots, r\}$, where $q_0 = q$ and $q_i \in Q_s$ for all $i \in \{1, \ldots, r\}$. The set of controllable states is denoted $\mathrm{Cont}(Q_s)$.

Consider a transition system $T = (Q, U, O, \Delta)$, a controller for T is a map $\mathscr{C} : Q \rightrightarrows U$ such that for all $q \in Q$, $\mathscr{C}(q) \subseteq \mathrm{Enab}_\Delta(q)$. We define the domain of the controller as $\mathrm{dom}(\mathscr{C}) = \{q \in Q \mid \mathscr{C}(q) \neq \emptyset\}$. The controlled transition system $T/\mathscr{C}$ is defined by the tuple $T/\mathscr{C} = (Q \cap \mathrm{dom}(\mathscr{C}), U, O, \Delta_{\mathscr{C}})$, where the sets U and O are inherited from the transition system T, and the transition relation is given by:

$$(q', o) \in \Delta_{\mathscr{C}}(q, u) \text{ iff } (q', o) \in \Delta(q, u) \text{ and } u \in \mathscr{C}(q). \quad (7)$$

Definition 6: A safety controller for the transition system T and the safe set Q_s satisfies:

(i) $\mathrm{dom}(\mathscr{C}) \subseteq \mathrm{Cont}(Q_s)$;

(ii) for all $q \in \mathrm{dom}(\mathscr{C})$ and for all $u \in \mathscr{C}(q)$, if $(q', o) \in \Delta_{\mathscr{C}}(q, u)$, then $q' \in \mathrm{dom}(\mathscr{C})$.

There are in general several controllers that solve the safety problem. A suitable solution to the safety problem is a controller that enables as many actions as possible. This controller $\mathscr{C}^*$ is said to be *a maximal safety controller*, in the sense that for any other controller $\mathscr{C}$ and for all $q \in Q$, we have $\mathscr{C}(q) \subseteq \mathscr{C}^*(q)$. Given the set of controllable states $\mathrm{Cont}(Q_s)$, the *maximal safety controller* can be defined as follows:

- for all $q \notin \mathrm{Cont}(Q_s)$, $\mathscr{C}^*(q) = \emptyset$;
- for all $q \in \mathrm{Cont}(Q_s)$, $\mathscr{C}^*(q) = \{u \in \mathrm{Enab}(q) \mid \text{for } (q', o) \in \Delta(q, u),\ q' \in \mathrm{Cont}(Q_s)\}$.

Let us remark that for any safety controller $\mathscr{C}$ we have that $\mathrm{dom}(\mathscr{C}) \subseteq \mathrm{Cont}(Q_s)$, while for the *maximal safety controller* $\mathscr{C}^*$, we have $\mathrm{dom}(\mathscr{C}^*) = \mathrm{Cont}(Q_s)$.

III. Event-based symbolic models

Let $\Sigma = (\mathbb{R}^n, P, \mathscr{P}, F)$ be a switched system for which the switching is periodically controlled with a period $\tau^* \in \mathbb{R}^+$. Then, a transition system T^{τ^*} can be associated to Σ by selecting all its transitions of duration $\tau^* > 0$. The transition system $T^{\tau^*} = (Q^{\tau^*}, U, O, \Delta^{\tau^*})$ is defined by:

- $Q^{\tau^*} = \mathbb{R}^n$ is the set of states;
- $U = P \times \{\tau^*\}$ is the set of inputs;
- $O = \mathbb{R}^n$ is the set of outputs;
- the transition relation $\Delta^{\tau^*} \subseteq Q^{\tau^*} \times U \times Q^{\tau^*} \times O$ is given as follows: $\forall x, x' \in Q^{\tau^*}$, $\forall u \in U$, $\forall o_1 \in O$, $(x', o_1) \in \Delta^{\tau^*}(x, u)$ if and only if
$$x' = \mathtt{x}(\tau^*, x, p) \text{ and } o_1 = x.$$

In this context, an approach for designing approximately bisimilar symbolic models with $T^{\tau^*}(\Sigma)$ has been presented in [6]. This method is based on the approximation of the state space by the lattice:

$$[\mathbb{R}^n]_\eta = \left\{ q \in \mathbb{R}^n \middle| q_i = k_i \frac{2\eta}{\sqrt{n}},\ k_i \in \mathbb{Z},\ i = 1, \ldots, n \right\},$$

where $\eta \in \mathbb{R}^+$ is the state space sampling parameter. The quantizer $\mathscr{Q}_\eta : \mathbb{R}^n \to [\mathbb{R}^n]_\eta$ is defined by $\mathscr{Q}_\eta(x) = q$ if and only if

$$\forall i = 1, \ldots, n,\ q_{(i)} - \frac{\eta}{\sqrt{n}} \leq x_{(i)} < q_{(i)} + \frac{\eta}{\sqrt{n}}. \quad (8)$$

It can be easily shown that for all $x \in \mathbb{R}^n$, $\|\mathscr{Q}_\eta(x) - x\| \leq \eta$. The symbolic abstraction $T_\eta^{\tau^*} = (Q_\eta^{\tau^*}, U, O, \Delta_\eta^{\tau^*})$ have been constructed as follows:

- $Q_\eta^{\tau^*} = [\mathbb{R}^n]_\eta$ is the set of states;
- $U = P \times \{\tau^*\}$ is the set of inputs;
- $O = \mathbb{R}^n$ is the set of outputs;
- the transition relation $\Delta_\eta^{\tau^*} \subseteq Q_\eta^{\tau^*} \times U \times Q_\eta^{\tau^*} \times O$ is given as follows: $\forall q, q' \in Q_\eta^{\tau^*}$, $\forall u \in U$, $\forall o_2 \in O$, $(q', o_2) \in \Delta_\eta^{\tau^*}(q, u)$ if and only if
$$q' = \mathscr{Q}_\eta(\mathtt{x}(\tau^*, q, p)) \text{ and } o_2 = q.$$

It has been shown in [6] that if Assumptions A-1 and A-2 are satisfied and if for a desired precision $\varepsilon \geq 0$ the state space sampling parameter η is such that $\eta \leq \gamma^{-1}((1-e^{-\kappa\tau})\underline{\alpha}(\varepsilon))$, then $T^{\tau^*}(\Sigma)$ is ε-*approximately bisimilar* to $T_\eta^{\tau^*}(\Sigma)$.

Here, we are interested in the symbolic models construction for switched systems for which the switching does not occur periodically. This can be the case when fast switching is needed. In this case we assume that the transition duration can be chosen from a finite set of durations $\mathscr{T}_{\tau^*}^N = \{\frac{\tau^*}{N}, \frac{2\tau^*}{N}, \ldots, \tau^*\}$ where $N \in \mathbb{N}^+$ is a subsampling parameter. To the switched system $\Sigma = (\mathbb{R}^n, P, \mathscr{P}, F)$, we associate the transition system $T^e = (Q^e, U^e, O^e, \Delta^e)$ where:

- $Q^e = \mathbb{R}^n$ is the set of states;
- $U^e = P \times \mathscr{T}_{\tau^*}^N$ is the set of inputs;
- $O^e = \mathbb{R}^n$ is the set of outputs;
- $\Delta^e \subseteq Q^e \times U^e \times Q^e \times O^e$ is the transition relation defined as follows: $\forall x, x^{'} \in Q^e$, $\forall (p,\tau) \in U^e$, $\forall o \in O^e$, $(x^{'}, o) \in \Delta^e(x,u)$ if and only if $\mathtt{x}(\tau, x, p) = x^{'}$, $o = x$.

Let $\varepsilon \in \mathbb{R}^+$ be the desired precision of the symbolic model. We first approximate the state space by the lattice $[\mathbb{R}^n]_\eta$ where $\eta \in \mathbb{R}^+$, and we define the transition system $T_\eta^e(\Sigma) = (Q_\eta^e, U^e, O^e, \Delta_\eta^e)$ where:

- $Q_\eta^e = [\mathbb{R}^n]_\eta$ is the set of states;
- $U^e = P \times \mathscr{T}_{\tau^*}^N$ is the set of inputs;
- $O^e = \mathbb{R}^n$ is the set of outputs;
- $\Delta_\eta^e \subseteq Q_\eta^e \times U^e \times Q_\eta^e \times O^e$ is the transition relation defined by: $\forall q, q^{'} \in Q_\eta^e$, $\forall u = (p,\tau) \in U^e$, $\forall o \in O^e$, $(q^{'}, o) \in \Delta_\eta^e(q,u)$ if and only if

$$g(\tau, q, p) \leq 0 \tag{9}$$

where

$$g(\tau, q, p) := \gamma(\|\mathtt{x}(\tau, q, p) - q'\|) - (1 - e^{-\kappa\tau})\underline{\alpha}(\varepsilon), \tag{10}$$

and $q^{'} = \mathscr{Q}_\eta(\mathtt{x}(\tau, q, p))$, $o = q$.

One can easily check that the obtained symbolic model $T_\eta^e(\Sigma)$ is deterministic.

One may remark that if the subsampling parameter is fixed to $N = 1$, then by computing T_η^e one retrieve the symbolic model $T_\eta^{\tau^*}$. Moreover, in this case, one can provide an ε-*approximate bisimulation relation* between T_η^e and T^e [6]. Here, we are interested in the case where $N \geq 1$ such that the symbolic model allows all the transitions of durations $\tau \in \mathscr{T}_{\tau^*}^N$ satisfying (10). In this case, we are able to provide an ε-*approximate feedback refinement relation* from T^e to T_η^e which is useful for control design. This is shown in the following Theorem.

Theorem 1: Consider a switched system Σ and assume that A-1 and A-2 hold. Let us consider a desired precision $\varepsilon > 0$ and a state sampling parameter $\eta > 0$ such that

$$\eta \leq \gamma^{-1}((1 - e^{-\kappa\tau^*})\underline{\alpha}(\varepsilon)). \tag{11}$$

Then, the relation

$$\mathscr{R} = \{(x,q) \in Q^e \times Q_\eta^e | V(x,q) \leq \underline{\alpha}(\varepsilon)\} \tag{12}$$

is an ε-*approximate feedback refinement relation* from T^e to T_η^e.

Note that the result of Theorem 1 is constructive. For a desired precision $\varepsilon > 0$ and a chosen state sampling parameter η satisfying (11), the transitions durations can be computed numerically while computing the symbolic model since they correspond to the values of $\tau \in \mathscr{T}_{\tau^*}^N$ for which the function g changes sign. Contrarily to the event-based scheme for symbolic models design proposed in [8] where the symbolic model is designed while choosing only transitions of shorter durations, the proposed symbolic model proposed above provides all the transitions with durations $\tau \in \mathscr{T}_{\tau^*}^N$ satisfying (9)-(10).

The choice of the state sampling parameter η in (11), provide us with a useful property relating the event-based symbolic model proposed above and the symbolic model obtained with a fixed time sampling period proposed in [6]. This property is shown in the following Lemma.

Lemma 1: Consider a switched system Σ and assume that A-1 and A-2 hold. Let $\varepsilon > 0$ be a desired precision and $\eta > 0$ a state sampling parameter such that

$$\eta \leq \gamma^{-1}((1 - e^{-\kappa\tau^*})\underline{\alpha}(\varepsilon)). \tag{13}$$

Then, the relation

$$\mathscr{R}' = \{(q_1, q_2) \in Q_\eta^e \times Q_\eta | q_1 = q_2\} \tag{14}$$

is a *feedback refinement relation* from T_η^e to $T_\eta^{\tau^*}$.

One may remark that a direct consequence of Lemma 1 is the fact that the event-based symbolic model T_η^e is non-blocking. Indeed, any transition of the transition system $T_\eta^{\tau^*}$ is a transition of the symbolic model T_η^e.

The result of Lemma 1 is very interesting in the sense that any controller $\mathscr{C}_{\tau^*}$ designed for $T_\eta^{\tau^*}$ is a controller for T_η^e. This is utilized to prove the main result of the next section.

IV. Lazy computation of symbolic safety controllers

Motivated by the properties of the event-based symbolic model proposed above and inspired from the self-trigger control strategy where the controller determines the mode of the switched system and the duration during which the mode is active [3], this section is dedicated to the synthesis of lazy safety controllers for event-based symbolic models. Here, using Lemma 1, we show that the size of the set of controllable states obtained with a safety controller designed for a symbolic model with a periodic time sampling is included in the set of controllable states obtained with a lazy safety controller designed for the event-based symbolic model.

The classical approach to compute the maximal safety controller $\mathscr{C}^*$ is based on a fixed point algorithm [13]. However, the computational complexity grows exponentially with state and input spaces dimension. A lazy safety controller is a controller that keeps all trajectories of the transition system within the safe set, while applying for each state a transition of longest possible duration. For this reason, we introduce a priority relation over the set of inputs, for which we give

priority to transitions of longer duration. For $u_1 = (p_1, \tau_1)$, $u_2 = (p_2, \tau_2) \in U$, priority is given to transitions of longer durations where: $u_1 \preccurlyeq u_2$ if and only if $\tau_1 \leq \tau_2$, $u_1 \prec u_2$ if and only if $\tau_1 < \tau_2$ and $u_1 \approx u_2$ if and only if $\tau_1 = \tau_2$. Using the fact that U is finite and for a given subset $U' \subseteq U$, we define:

$$\max_{\preccurlyeq}(U') = \{u' \in U' \mid \forall u \in U',\ u \preccurlyeq u'\}. \tag{15}$$

First, we define a lazy safety controller.

Definition 7: A lazy safety controller for the transition system T and the safe set Q_s is a safety controller such that

(i) for all $q \in \mathrm{dom}(\mathscr{C})$, if $u \in \mathscr{C}(q)$, then for any $u' \in \mathrm{Enab}(q)$ with $u \prec u'$, $(q', o) = \Delta(q, u')$, it holds that $q' \notin \mathrm{dom}(\mathscr{C})$.

Secondly, let us recall the notion of maximal lazy safety controller introduced in [5]:

Definition 8: A maximal lazy safety controller for the transition system $T = (Q, U, O, \Delta)$ and safety specification Q_s is a safety controller $\mathscr{C}^l : X \rightrightarrows U$ such that:

- all controllable states are in $\mathrm{dom}(\mathscr{C}^l)$:

$$\mathrm{Cont}(Q_s) = \mathrm{dom}(\mathscr{C}^l);$$

- for all states $q \in \mathrm{dom}(\mathscr{C}^l)$:
  1) if $u \in \mathscr{C}^l(q)$, then for any $u' \in \mathrm{Enab}(q)$ with $u \prec u'$, $(q', o) = \Delta(q, u')$, it holds that $q' \notin \mathrm{Cont}(Q_s)$;
  2) if $u \in \mathscr{C}^l(q)$, then for any $u' \in \mathrm{Enab}(q)$ with $u \approx u'$, $(q', o) = \Delta(q, u')$, it holds that $u' \in \mathscr{C}^l(q)$ if and only if $q' \in \mathrm{Cont}(Q_s)$.

It was shown in [5], that if the set of inputs is finite and equipped with a priority relation, then there exists a unique maximal lazy safety controller. Interestingly, the domain of the maximal lazy safety controller satisfies $\mathrm{dom}(\mathscr{C}^l) = \mathrm{dom}(\mathscr{C}^*) = \mathrm{Cont}(Q_s)$. An algorithm for synthesizing the maximal lazy safety controller was given in [5], it is based on depth first search, where transitions of higher priority are explored first. While in classical safety fixed points algorithms [13] the abstraction needs to be pre-computed, in the lazy algorithm the abstraction is computed on-the-fly [10]. The maximal lazy safety controller is a compromise between permissiveness and computational complexity, and represents a suitable solution when computational resources are not sufficient to use classical safety algorithms.

Given a switched system Σ and its periodic and event-based abstractions $T_\eta^{\tau^*}(\Sigma)$ and $T_\eta^e(\Sigma)$, and given a safety specification Q_s. Our objective is to provide a theoretical comparison between the maximal safety controller for $T_\eta^{\tau^*}(\Sigma)$ and Q_s, and the maximal lazy safety controller for $T_\eta^e(\Sigma)$ and Q_s. Interestingly, we show that the size of the set of controllable states obtained with the lazy safety controller of the event-based symbolic model is much larger than the one of the safety controller designed for the symbolic model with periodic time sampling.

Theorem 2: Let the transition systems $T_\eta^{\tau^*}(\Sigma)$ and $T_\eta^e(\Sigma)$ for which (11) holds. Consider the safety specification $Q_s \subseteq Q_\eta^{\tau^*} = Q_\eta^e$. Let $\mathscr{C}_e^* : Q_\eta^e \rightrightarrows U_\eta^e$ be a maximal safety controller for $T_\eta^e(\Sigma)$ and safety specification Q_s, $\mathscr{C}_e^l : Q_\eta^e \rightrightarrows U_\eta^e$ be a maximal lazy safety controller for $T_\eta^e(\Sigma)$ and safety specification Q_s, and $\mathscr{C}_{\tau^*}^* : Q_\eta^e \rightrightarrows U_\eta^e$ be a maximal safety controller for $T_\eta^{\tau^*}(\Sigma)$ and safety specification Q_s. Then, for all $q \in Q_\eta^e$,

$$\mathscr{C}_{\tau^*}^*(q) \subseteq \mathscr{C}_e^l(q) \subseteq \mathscr{C}_e^*(q). \tag{16}$$

A direct implication of Theorem 2, is that any transition allowed by the maximal safety controller designed for a symbolic model with periodic time sampling is also enabled by the lazy safety controller designed for an event-based symbolic model. Thus, the size of the set of controllable states obtained with a lazy safety controller designed for an event-based symbolic model is much larger compared to the one obtained with a safety controller designed for a classical symbolic model. One may remark also that we can not compare with the symbolic model with a periodic time sampling $\frac{\tau^*}{N}$, since the systems $T_\eta^e(\Sigma)$ and $T_{\eta'}^{\frac{\tau^*}{N}}(\Sigma)$ did not have the same state space ($T_\eta^e(\Sigma)$ is constructed using a discretization parameter $\eta = \gamma^{-1}((1 - e^{-\kappa\tau^*})\underline{\alpha}(\varepsilon))$ and $T_{\eta'}^{\frac{\tau^*}{N}}(\Sigma)$ is contructed using the discretization parameter $\eta' = \gamma^{-1}((1 - e^{\frac{-\kappa\tau^*}{N}})\underline{\alpha}(\varepsilon))$).

V. Illustrative example

We consider the boost DC-DC converter which is mathematically modeled as a switched affine system given by:

$$\dot{\mathrm{x}}(t) = A_{\mathbf{p}(t)}\mathrm{x}(t) + b \tag{17}$$

where $\mathrm{x}(t) = \begin{bmatrix} i_L(t) & v_c(t) \end{bmatrix}^T$ is the state vector with $i_l(t)$ is the current in the inductor and v_c is the voltage in the capacitor, b and A_p, $p \in \{1, 2\}$ are matrices of appropriate dimension and the numerical values of their parameters have been provided in [4]. It has been shown in [6] the boost DC-DC converter is an incrementally stable system. In order to design our symbolic model we consider the Lyapunov function and the parameters provided [6]. We consider the time sampling parameter $\tau^* = 0.5sec$ and the subsampling parameter $N = 50$. Let us consider a desired precision for the symbolic model as $\varepsilon = 0.1$ and the state sampling parameter is such that $\eta = \gamma^{-1}((1 - e^{-\kappa\tau^*})\underline{\alpha}(\varepsilon)) = 9.7 \times 10^{-4}$. Let the safe set of the symbolic abstraction $Q_s = [\mathbb{R}^2]_\eta \cap [1.3\ 1.6] \times [5.6\ 5.8]$. For the obtained symbolic model we apply a lazy safety control strategy. Simulations results are presented in Figures 2, 3. Moreover, in order to illustrate the result of Theorem 2, we have designed a symbolic model with a fixed time sampling period $\tau^* = 0.5sec$ and the same desired precision $\varepsilon = 0.1$. To the obtained symbolic model we have designed a safety controller to ensure the same control objective as for the lazy safety controller. The obtained symbolic controller is shown in Figure 1. From Figures 2-3, we can observe that the control objective is satisfied and the trajectories of the closed-loop system remain inside the safe set. We can see from Figures 2-3 that when the trajectory of the closed-loop system is far from the boundary of the safe set the time sampling parameter is equal to τ^* and as the trajectory get closer to the unsafe set the sampling parameter becomes smaller ($\tau < \tau^*$) in order to allow fast switching

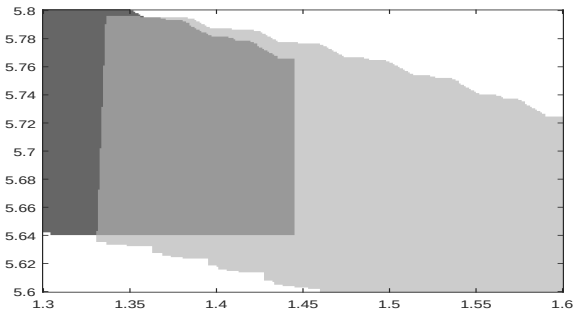

Fig. 1. Safety controller designed for a symbolic model of the boost DC-DC converter with a fixed time sampling period $\tau^* = 0.5sec$ (dark gray: mode 1, light gray: mode 2, medium gray: both modes are acceptable, white: uncontrollable states).

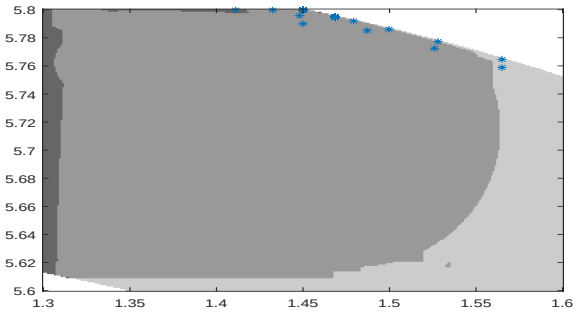

Fig. 2. Lazy safety controller for the event-based symbolic model of the boost DC-DC converter (dark gray: mode 1, light gray: mode 2, medium gray: both modes are acceptable, white: uncontrollable states); Symbolic states of the closed-loop boost DC-DC converter (blue stars).

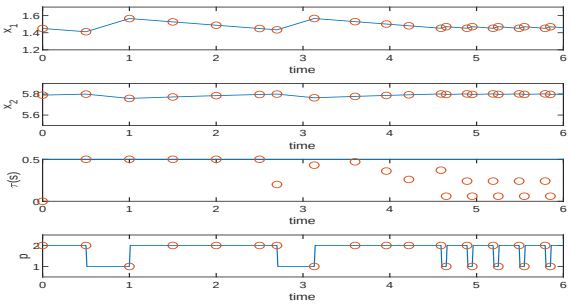

Fig. 3. Evolution of the state variables of the boost DC-DC converter with the lazy safety controller starting at $x = [1.45, 5.77]^T$; The sampling instants generated while computing the lazy safety controller; Switching signal generated by the lazy safety controller

and keep the trajectory in the safe set. Comparing Figures 2 and 1, we can observe that all the transitions allowed by the safety controller designed for the symbolic model with a periodic time sampling are enabled by the lazy safety controller designed for the event-based symbolic model. It can be seen clearly that the size of the set of the controllable states obtained with the event-based approach is much larger than the one obtained with the classical abstraction method. This observations are consistent with the theoretical result.

VI. Conclusion

This paper has provided a novel event-based scheme for symbolic models design. The obtained symbolic models have been shown to be related to the original switched system by a feedback refinement relation. Then, using the particular structure of the obtained event-based symbolic model, a lazy safety controller has been designed while choosing transitions of longest durations. We then prove analytically that the size of the set of controllable states obtained with the lazy safety controller designed for the event-based symbolic model is larger than the one obtained with a safety controller designed for the classical symbolic model has been provided. Finally, simulations have been performed for a Boost DC-DC converter structure in order to show the efficiency of the proposed method.

Appendix I
Proof of Theorem 1

Proof: In order to prove Theorem 1, we will follow the statements of Definition 4. First let us remark that for all $(x,q) \in \mathscr{R}$, we have $\text{Enab}_{\Delta^e_\eta}(q) \subseteq \text{Enab}_{\Delta^e}(x) = U^e$. Thus, the first condition of Definition 4 holds.

Let us consider $(x,q) \in \mathscr{R}$, from the left inequality in (2) we obtain

$$\underline{\alpha}(\|x-q\|) \leq V(x,q) \leq \underline{\alpha}(\varepsilon). \tag{18}$$

This leads to

$$\|x-q\| \leq \underline{\alpha}^{-1}(V(x,q)) \leq \varepsilon. \tag{19}$$

Therefore, $d(x,q) \leq \varepsilon$.

Now, let $u \in Enab_{\Delta^e_\eta}(q)$ and $(x',o) \in \Delta^e(x,u)$. There exists $q' \in [\mathbb{R}^n]_\eta$ such that $\|\mathtt{x}(\tau,q,p) - q'\| \leq \eta$. In order to demonstrate that $(x',q') \in \mathscr{R}$, it is sufficient to prove that

$$V(x',q') \leq \underline{\alpha}(\varepsilon). \tag{20}$$

From (4), we obtain

$$V(x',q') \leq V(x',\mathtt{x}(\tau,q,p)) + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|). \tag{21}$$

Using the fact that V is a δ-GUAS Lyapunov function for the switched system Σ that satisfies (3), we obtain

$$\begin{aligned} V(x',q') &\leq V(x',\mathtt{x}(\tau,q,p)) + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|) \\ &\leq V(\mathtt{x}(\tau,x,p),\mathtt{x}(\tau,q,p)) + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|) \\ &\leq V(x,q)e^{-\kappa\tau} + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|). \end{aligned} \tag{22}$$

Since $(x,q) \in \mathscr{R}$, the last inequality leads to

$$\begin{aligned} V(x',q') &\leq V(x,q)e^{-\kappa\tau} + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|) \\ &\leq \underline{\alpha}(\varepsilon)e^{-\kappa\tau} + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|). \end{aligned} \tag{23}$$

From (9) and (10), (23) becomes

$$\begin{aligned} V(x',q') &\leq \underline{\alpha}(\varepsilon)e^{-\kappa\tau} + \gamma(\|\mathtt{x}(\tau,q,p) - q'\|) \\ &\leq \underline{\alpha}(\varepsilon). \end{aligned} \tag{24}$$

Therefore, (20) is verified. Thus, $(x',q') \in \mathscr{R}$. Finally, the last requirement in Definition 4 can be shown directly from the

construction of the state space approximation $[\mathbb{R}^n]_\eta$. Indeed, we have that for all $x \in Q^e$ there exists $q \in Q^e_\eta$ given by $q = \mathscr{Q}(x)$ such that $\|x-q\| \leq \eta$. Assuming that the right inequality of (2) holds for $\overline{\alpha} = \gamma$, we obtain

$$V(x,q) \leq \gamma(\|x-q\|) \leq \gamma(\eta). \tag{25}$$

Using (11), we obtain

$$V(x,q) \leq \gamma(\|x-q\|) \leq \gamma(\eta) \leq (1-e^{-\kappa\tau^*})\underline{\alpha}(\varepsilon) \leq \underline{\alpha}(\varepsilon). \tag{26}$$

Thus, $(x,q) \in \mathscr{R}$, which ends the proof. ■

APPENDIX II
PROOF OF LEMMA 1

Proof: First let us show that for all $(q_1,q_2) \in \mathscr{R}^{'}$, $Enab_{\Delta^{\tau^*}_\eta}(q_2) \subseteq Enab_{\Delta^e_\eta}(q_1)$. We have $(q_1,q_2) \in \mathscr{R}^{'}$. Thus $q_1 = q_2 = q$. Let $u = (p,\tau^*) \in Enab_{\Delta^{\tau^*}_\eta}(q)$. Therefore, $\Delta^{\tau^*}_\eta(q,u) \neq \emptyset$. Then, there exists $q^{'} \in [\mathbb{R}^n]_\eta$ such that $q^{'} = \mathscr{Q}_\eta(\mathrm{x}(\tau^*,q,p))$ and

$$\|\mathrm{x}(\tau^*,q,p) - q^{'}\| \leq \eta. \tag{27}$$

Now let us verify that $g(\tau^*,q,p) \leq 0$ with the function g defined in (10) and

$$g(\tau^*,q,p) = \|\mathrm{x}(\tau^*,q,p) - q^{'}\| - (1-e^{\kappa\tau^*})\underline{\alpha}(\varepsilon).$$

Using (27), we obtain

$$g(\tau^*,q,p) \leq \gamma(\eta) - (1-e^{\kappa\tau^*})\underline{\alpha}(\varepsilon)$$

From (13), the last inequality leads to

$$g(\tau^*,q,p) \leq \gamma(\eta) - (1-e^{\kappa\tau^*})\underline{\alpha}(\varepsilon) \leq 0. \tag{28}$$

Therefore, $(q^{'},o) \in \Delta^e_\eta(q,u)$. Thus, $u = (p,\tau^*) \in Enab_{\Delta^e_\eta}(q)$, which proves the first requirements of Definition 4.

Now let $u = (p,\tau^*) \in Enab_{\Delta^{\tau^*}_\eta}(q)$. Consider $(q^{'}_1,o_1) \in \Delta^e_\eta(q,u)$. Then, there exists $q^{'}_1 = \mathscr{Q}_\eta(\mathrm{x}(\tau^*,q,p))$ and $o_1 = q$. On the other hand, since $u = (p,\tau^*) \in Enab_{\Delta^{\tau^*}_\eta}(q)$ there exists $q^{'}_2 = \mathscr{Q}_\eta(\mathrm{x}(\tau^*,q,p)) = q^{'}_1$ and $o_2 = q = o_1$. Therefore, $(q^{'}_1,q^{'}_2) \in \mathscr{R}^{'}$. Moreover, $d(o_1,o_2) = 0$.

Finally, thanks to the fact that $Q^{\tau^*}_\eta = Q^e_\eta$ the third condition in Definition 4 is satisfied for all $q \in Q^e_\eta$. ■

APPENDIX III
PROOF OF THEOREM 2

Proof: Let us remark that the inclusion of $\mathscr{C}^l_e$ in $\mathscr{C}^*_e$ follows directly from the fact that the maximal lazy safety controller is a safety controller.

For the first inclusion, we first prove that $\mathrm{dom}(\mathscr{C}^*_{\tau^*}) \subseteq \mathrm{dom}(\mathscr{C}^l_e)$. We have from Lemma 1 that the relation $\mathscr{R}'$ defined in (14) is a feedback refinement relation from T^e_η to $T^{\tau^*}_\eta$. Since $\mathscr{C}^*_{\tau^*}$ is the maximal safety controller for $T^{\tau^*}_\eta(\Sigma)$ and safety specification Q_s and using the fact that $\mathscr{R}'$ is a feedback refinement relation [11], we have that $\mathscr{C}^*_{\tau^*}$ is a safety controller for $T^e_\eta(\Sigma)$ and safety specification Q_s. Hence, for all $q \in Q^e_\eta$, $\mathscr{C}^*_{\tau^*}(q) \subseteq \mathscr{C}^*_e(q)$, which implies that $\mathrm{dom}(\mathscr{C}^*_{\tau^*}) \subseteq \mathrm{dom}(\mathscr{C}^*_e) = \mathrm{dom}(\mathscr{C}^l_e)$.

We have that $\mathscr{C}^*_{\tau^*}$ is a safety controller, then conditions (i) and (ii) of Definition 6 are directly satisfied. Now let $q \in Q^{\tau^*}_\eta$, and $u = (p,\tau^*) \in \mathrm{Enab}_{\Delta^{\tau^*}_\eta}(q)$. In addition, since there are no $u' \in \mathrm{Enab}_{\Delta^{\tau^*}_\eta}(q)$ such that $u \prec u'$, the condition (i) of Definition 7 is immediately satisfied. Then, $\mathscr{C}^*_{\tau^*}$ is a lazy safety controller for T^e_η and Q_s. Therefore, for all $q \in Q^e_\eta$, $\mathscr{C}^*_{\tau^*}(q) \subseteq \mathscr{C}^l_e(q)$. Which ends the proof. ■

REFERENCES

[1] D. Angeli, "A Lyapunov approach to incremental stability properties," *IEEE Transactions on Automatic Control*, vol. 47, no. 3, pp. 410–421, 2002.

[2] D. Angeli and E. D. Sontag, "Forward completeness, unboundedness observability, and their lyapunov characterizations," *Systems & Control Letters*, vol. 38, no. 4, pp. 209–217, 1999.

[3] A. Anta and P. Tabuada, "To sample or not to sample: Self-triggered control for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2030–2042, 2010.

[4] A. G. Beccuti, G. Papafotiou, and M. Morari, "Optimal control of the boost dc-dc converter," in *44th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2005, pp. 4457–4462.

[5] A. Girard, G. Gössler, and S. Mouelhi, "Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models," *IEEE Transactions on Automatic Control*, vol. 61, no. 6, pp. 1537–1549, 2016.

[6] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2010.

[7] L. Hetel and E. Bernuau, "Local stabilization of switched affine systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1158–1163, 2015.

[8] Z. Kader, A. Girard, and A. Saoud, "Symbolic models for incrementally stable switched systems with aperiodic time sampling," *6th IFAC Conference on Analysis and Design of Hybrid Systems*, vol. 51, no. 16, pp. 253–258, 2018.

[9] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2003.

[10] G. Pola, A. Borri, and M. D. Di Benedetto, "Integrated design of symbolic controllers for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 534–539, 2012.

[11] G. Reissig, A. Weber, and M. Rungger, "Feedback refinement relations for the synthesis of symbolic controllers," *IEEE Transactions on Automatic Control*, vol. 62, no. 4, pp. 1781–1796, 2017.

[12] R. Shorten, F. Wirth, O. Mason, K. Wulff, and C. King, "Stability criteria for switched and hybrid systems," *SIAM review*, vol. 49, no. 4, pp. 545–592, 2007.

[13] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.