Safety Controller Synthesis for Incrementally Stable Switched Systems Using Multiscale Symbolic Models
Antoine Girard, Gregor Gössler, Sebti Mouelhi

To cite this version:
hal-01197426v2

HAL Id: hal-01197426
https://hal.archives-ouvertes.fr/hal-01197426v2
Submitted on 19 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Safety Controller Synthesis for Incrementally Stable Switched Systems using Multiscale Symbolic Models

Antoine Girard, Gregor Gössler and Sebti Mouelhi

Abstract—We propose an approach to the synthesis of safety controllers for a class of switched systems, based on the use of multiscale symbolic models that describe transitions of various durations and whose sets of states are given by a sequence of embedded lattices approximating the state-space, the finer lattices being accessible only by transitions of shorter duration. We prove that these multiscale symbolic models are approximately bisimilar to the original switched system provided it enjoys an incremental stability property attested by the existence of a common Lyapunov function or of multiple Lyapunov functions with a minimal dwell-time. Then, for specifications given by a safety automaton, we present a controller synthesis algorithm that exploits the specificities of multiscale symbolic models. We formalize the notion of maximal lazy safety controller which gives priority to transitions of longer durations; the shorter transitions and thus the finer scales of the symbolic model are effectively explored only when safety cannot be ensured at the coarser level and fast switching is needed. We propose a synthesis algorithm where symbolic models can be computed on the fly, this allows us to keep the number of symbolic states as low as possible. We provide computational evidence that shows drastic improvements of the complexity of controller synthesis using multiscale symbolic models instead of uniform ones.

I. INTRODUCTION

Symbolic control approaches, based on the use of discrete abstractions, have become quite popular in the area of hybrid systems (see e.g. [18] and the references therein). In symbolic control, continuous behaviors are abstracted over a finite set of symbols, each symbol representing infinitely many states. The main advantage of these approaches is that they offer the possibility to leverage controller synthesis techniques developed in the area of discrete-event dynamic systems (see e.g. [8]). Also, these approaches allow one to address specifications that are often different from traditional properties in control theory (e.g. stability, controllability, observability...): such specifications can for instance be given by some logic formula or by an automaton describing the acceptable temporal behaviors of the system.

A recent trend in symbolic control is to use discrete abstractions, also called symbolic models, that are related to the original system by some approximate equivalence relationship such as approximate bisimulation [9]. It has been shown that such abstractions are computable for several classes of control systems including incrementally stable switched systems [10], nonlinear systems with or without disturbances [14], [16], [20], time delay systems [15], networked control systems [5] and stochastic systems [22]. These approaches are based on sampling of time and space where the sampling parameters must satisfy some relation in order to obtain abstractions of a prescribed precision. Particularly, the faster the time sampling, the finer the lattice approximating the state-space has to be, resulting in symbolic models with a large number of states.

In this paper, we present a class of multiscale symbolic models for incrementally stable switched systems that allows us to deal with fast time sampling while keeping the number of symbolic states at a reasonable level. Following the self-triggered control paradigm [21], [2], we assume that the controller has to decide the control mode and the duration during which it will be applied. Then, it is natural to consider discrete abstractions where transitions have various durations. For transitions of longer duration, it is sufficient to consider abstract states on a coarse lattice. For transitions of shorter duration, it becomes necessary to use finer lattices. These finer lattices are effectively used only on a restricted area of the state-space where fast time sampling is needed. We prove that these multiscale symbolic models are approximately bisimilar to the original incrementally stable switched system under the existence of a common Lyapunov function or of multiple Lyapunov functions with a minimal dwell-time. Moreover, we show that any precision can be achieved. The concept of approximately bisimilar multiscale abstractions has also been explored in [19] where the multiscale feature is used for accommodating locally the precision of the abstraction while the time sampling period remains constant. On the contrary, our approach seeks for a uniform precision but varying time sampling periods.

In the second part of the paper, we propose to use these multiscale symbolic models for the synthesis of safety controllers for switched systems. For specifications given by safety automata, we introduce the notion of maximal lazy safety controller which exploits the specificities of multiscale symbolic models: it gives priority to transitions of longer durations; the faster transitions and thus the finer scales of the symbolic models are effectively explored only when safety cannot be ensured at the coarser level and fast switching is needed. We present an algorithm computing symbolic models on the fly during controller synthesis, and therefore dynamics at the finest scales are explored only when necessary. We provide experimental results, obtained by the toolbox CoSyMA [12] that show drastic improvements of the complexity of controller synthesis using multiscale models instead of uniform ones defined in [10]. Symbolic controller synthesis algorithms using on the fly computation of uniform symbolic models have also been considered in [13], for specifications described by a target deterministic transition system approximately simulating the observed behavior of the controlled system.

The results presented in this paper appeared partially and in a preliminary formulation in the conference papers [7], [6], [12]. We provide in the following a coherent and improved presentation of the main results of these papers with the following extensions. Firstly, the output of the symbolic models are continuous-time functions instead of sequences of states. While technically simple, this extension allows us to address specifications on continuous-time signals and to consider transitions of long duration without overlooking the behavior of the system between two samples; as far as we know, this is the first work on approximately bisimilar abstractions offering this possibility. Secondly, we address the case of switched systems with multiple Lyapunov functions and dwell-time when we previously
focused on the case of systems with common Lyapunov functions. Thirdly, instead of considering only simple safety specifications (i.e. keep the state of the system within a safe set), we extend our approach to handle more complex properties given by safety specification automata. Finally, we present improved experimental results.

**Notations:** \( \mathbb{N} \) and \( \mathbb{Z} \) denote the sets of nonnegative integers and of integers, respectively, \( \mathbb{R}, \mathbb{R}^+ \) and \( \mathbb{R}^+ \) denote the sets of real, of non-negative real and of positive real numbers, respectively. For \( x \in \mathbb{R}^n, x[i] \) denotes its i-th coordinate, \( i = 1, \ldots, n \); \( \|x\| = \sqrt{\sum_{i=1}^{n} x[i]^2} \) denotes the Euclidean norm of \( x \). Let \( I = [a, b] \) be a compact interval of \( \mathbb{R} \) with \( a < b \), we say that \( f \) is continuous on \( I \), if it is continuous on \( (a, b) \), right-continuous at \( a \) and left-continuous at \( b \). The set of continuous functions from \( I \rightarrow \mathbb{R}^n \) is denoted \( C(I, \mathbb{R}^n) \). For \( f \in C(I, \mathbb{R}^n) \), we define \( \|f\| = \sup_{x \in I} \|f(x)\| \). Given a function \( f : R_0^+ \rightarrow R_0^+ \), and \( r \in R_0^+ \), we denote by \( f_r \) the restriction of \( f \) to the interval \([0, r]\). A continuous function \( \gamma : R_0^+ \rightarrow R_0^+ \) is said to belong to class \( K \) if it is strictly increasing, and \( \gamma(0) = 0 \). It is of class \( K_\infty \) if it is of class \( K \) and \( \gamma(r) \rightarrow \infty \) as \( r \rightarrow \infty \). A continuous function \( \beta : R_0^+ \times R_0^+ \rightarrow R_0^+ \) is said to belong to class \( KL \) if for all fixed \( s \), the map \( r \rightarrow \beta(r, s) \) belongs to class \( K \) and for all fixed \( r > 0 \), the map \( s \rightarrow \beta(r, s) \) is strictly decreasing and \( \beta(r, s) \rightarrow 0 \) as \( s \rightarrow 0 \). Given two sets \( S_1 \) and \( S_2 \), and a relation \( R \subseteq S_1 \times S_2 \), we denote \( R^\delta(s_1) = \{ s_2 \in S_2 | (s_1, s_2) \in R \} \) and \( R^{-\delta}(s_2) = \{ s_1 \in S_1 | (s_1, s_2) \in R \} \). Let \( R \subseteq S_1 \times S_2 \) and \( s_2 \in S_2 \), we denote \( R(s_2) = \{ s_1 \in S_1 | (s_1, s_2) \in R \} \). Similarly for \( S_2 \). Let \( x \in R^n \) be a relation \( \subseteq \mathbb{R}^n \times \mathbb{R}^n \) that is a total preorder if and only if: (i) for all \( s_1, s_2, s_3 \in S, s_2 \leq s_3 \) and \( s_2 \leq s_3 \) implies \( s_1 \leq s_3 \); (ii) for all \( s_1, s_2 \in S, s_1 \leq s_2 \) or \( s_2 \leq s_1 \). We can define the associated equivalence relation \( \sim \) and strict weak order \( \prec \) given by \( s_1 \sim s_2 \) if and only if \( s_1 \leq s_2 \) and \( s_2 \leq s_1 \). A relation \( \prec \) and \( \sim \) is a total preorder if and only if \( s_1 \prec s_2 \) if and only if \( s_2 \sim s_1 \).

Given a finite set \( S \), \( |S| \) denotes its cardinality.

**II. PRELIMINARIES**

**A. Incrementally stable switched systems**

We briefly introduce the class of systems that we consider in this paper.

**Definition 2.1:** A switched system is a quadruple \( \Sigma = (\mathbb{R}^n, P, \mathcal{F}, F) \), where \( \mathbb{R}^n \) is the state space; \( P = \{1, \ldots, m\} \) is the finite set of modes; \( \mathcal{F} \) is a subset of \( \mathbb{R}^n \times \mathbb{R}^n \) which denotes the set of piecewise constant functions from \( \mathbb{R}^n \) to \( \mathbb{R}^n \), continuous from the right and with a finite number of discontinuities on every bounded interval of \( \mathbb{R}^n \); \( F = \{ f_1, \ldots, f_m \} \) is a collection of smooth vector fields indexed by \( P \).

A switching signal of \( \Sigma \) is a function \( p \in \mathcal{P} \), the discontinuities of \( p \) are called switching times. A continuous function \( x : R_0^+ \rightarrow \mathbb{R}^n \) is said to be a trajectory of \( \Sigma \) if there exists a switching signal \( p \in \mathcal{P} \) such that, at each \( t \in R_0^+ \), the function \( p \) is continuous, \( x \) is continuously differentiable and satisfies:

\[
x(t) = f_{p(t)}(x(t)).
\]

We make the assumption that the vector fields \( f_p \) are such that for all initial conditions \( x \in \mathbb{R}^n \), for all switching signals \( p \in \mathcal{P} \), there exists a unique trajectory of \( \Sigma \) denoted \( x(.; x, p) \) or by \( x(.; x, p) \) if \( p \) is constant equal to \( p \in P \). Necessary and sufficient conditions to be satisfied by \( f_p \) can be found in [1].

The results presented in this paper apply to switched systems satisfying the incremental stability property (i.e. \( \delta\)-GUAS [10]):

**Definition 2.2:** A switched system \( \Sigma \) is incrementally globally uniformly asymptotically stable (\( \delta\)-GUAS) if there exists a \( K \) \( \subseteq \mathbb{R}^n \) function \( \beta \) such that for all \( t \in R_0^+ \), for all \( x_1, x_2 \in \mathbb{R}^n \), for all switching signals \( p \in P \), the following condition is satisfied:

\[
\|x(t, x_1, p) - x(t, x_2, p)\| \leq \beta(\|x_1 - x_2\|, t).
\]
outputs $Y$ is equipped with a metric $d$, symbolic if $X$ and $U$ are finite or countable sets.

The transition $(x, u, x', y) ∈ Δ$ will be denoted $(x', y) ∈ Δ(x, u)$; this means that the system can evolve from state $x$ to state $x'$ under the input $u$, while producing output $y$. An input $u ∈ U$ belongs to the set of enabled inputs at state $x$, denoted $enab(x)$, if $Δ(x, u) ≠ ∅$. If $enab(x) = ∅$, then $x$ is said to be blocking, otherwise it is said to be non-blocking. The transition system is said to be deterministic if for all $x ∈ X$ and $u ∈ enab(x)$, $Δ(x, u)$ has only one element; in that case, we shall write with a slight abuse of notation $(x', y) = Δ(x, u)$.

A trajectory of the transition system is a finite or infinite sequence of transitions $σ = (x_0^0, u_0^0, y_0^0)(x_1^0, u_1^0, y_1^0)(x_2^0, u_2^0, y_2^0)…$ where $(x_i^0, y_i^0) ∈ Δ(x_{i-1}^0, u_{i-1}^0)$, for all $i ≥ 0$. It is initialized if $x_0^0 ∈ X^0$, it is maximal if it is infinite or it is finite and ends in a blocking state. A state $x ∈ X$ is reachable if there exists an initialized trajectory reaching $x$. The transition system is said to be non-blocking if for all initialized maximal trajectories are infinite or equivalently if all reachable states are non-blocking. The output behavior associated to the trajectory $σ$ is the sequence of outputs $y_0^0, y_1^0, y_2^0…$.

In the following, we will consider approximation relationships between transition systems in the sense of approximate bisimulation [9].

**Definition 2.6:** Let $T_i = (X_i, U, Y, Δ_i, X_i^0)$, with $i = 1, 2$ be metric transition systems with the same sets of inputs $U$ and outputs $Y$ equipped with the metric $d$. Let $ε ∈ R_+^d$, $R ⊆ X_1 × X_2$ is said to be an $ε$-approximate bisimulation relation between $T_1$ and $T_2$ if for all $(x_1, x_2) ∈ R$, $u ∈ U$:

1. $∀(x_1', y_1) ∈ Δ_1(x_1, u), ∃(x_2', y_2) ∈ Δ_2(x_2, u), d(y_1, y_2) ≤ ε$ and $(x_1', x_2') ∈ R$;
2. $∀(x_2', y_2) ∈ Δ_2(x_2, u), ∃(x_1', y_1) ∈ Δ_1(x_1, u), d(y_1, y_2) ≤ ε$, and $(x_1', x_2') ∈ R$.

The transition systems $T_1$ and $T_2$ are said to be $ε$-approximately bisimilar, denoted $T_1 ≃_ε T_2$, if $X_1^0 ⊆ R^{-1}(X_2^0)$ and $X_2^0 ⊆ R(X_1^0)$.

Let us give the following result characterizing approximate bisimulation for deterministic systems. It is a simple particularization of the previous definition to the deterministic case; the proof is straightforward and therefore omitted.

**Lemma 2.7:** If $T_1$ and $T_2$ are deterministic, $R ⊆ X_1 × X_2$ is an $ε$-approximate bisimulation relation if and only if for all $(x_1, x_2) ∈ R$, $enab(x_1) = enab(x_2)$ and for all $u ∈ enab(x_1)$,

$$d(y_1, y_2) ≤ ε \text{ and } (x_1', x_2') ∈ R,$$

where $(x_1', y_1) = Δ_1(x_1, u)$, $(x_2', y_2) = Δ_2(x_2, u)$.

**Remark 2.8:** The definitions of transition systems and approximate bisimulation relations introduced in this section slightly differ from those given in [9] where outputs are only related to states by an output map. In the current work, the outputs are related to transitions and the output map is implicitly encoded in the transition relation. The definitions used in [9] can be shown to be particular cases of Definitions 2.5 and 2.6. The current generalization allows us, in the following, to define transition systems describing the dynamics of switched systems where the outputs are continuous-time signals whereas the approaches presented in [10], [7], [6] are based on the framework [9] and output sequences of states.

III. MULTISCALE SYMBOLIC MODELS FOR SWITCHED SYSTEMS

In this section, we establish some results on the existence of approximately bisimilar symbolic models for incrementally stable switched systems. They extend the results of [10] in two ways. Firstly, the output of our symbolic models are continuous-time signals instead of sequences; thus they are more suitable for use in controller synthesis with continuous-time specifications. Moreover, they allow us to consider transitions of long duration without ignoring the behavior of the system on the time interval between the beginning and the end of the transition. Secondly, the symbolic models we consider here are defined in a multiscale setting. The approach presented in [10] is based on a uniform discretization of time and space with sampling parameters $τ ∈ R^+$ and $η ∈ R^+$, respectively. It has been established that the resulting symbolic models are $τ$-approximately bisimilar to incrementally stable switched systems where the precision $ε ∈ R^+$ is related to the values of $τ$ and $η$. In particular, the smaller $τ$, the smaller $η$ must be to guarantee a given precision $ε$. In practice, for a small time sampling parameter, symbolic models with an acceptable precision may have a very large number of states. There are number of applications where the switching has to be fast though this fast switching is generally necessary only on a restricted part of the state space. For instance, for safety controllers, fast switching is needed only when approaching the unsafe set. In order to enable fast switching while dealing with abstractions with a reasonable number of states, one may consider symbolic models enabling transitions of different durations. For transitions of long duration, it is sufficient to consider abstract states on a coarse lattice to meet the desired precision $ε$. We consider transitions of shorter durations, it becomes necessary to use finer lattices for the abstract state-space. These finer lattices are effectively used only on a restricted area of the state space, where the fast switching is necessary. This allows us to keep the number of states in the symbolic model at a reasonable level and results naturally in a notion of multiscale symbolic models presented in the following. Let us remark that uniform symbolic models coincide with our framework when considering only one scale.

A. Switched systems without dwell-time

Let $Σ = (R^n, P, P, F)$ be a switched system where $P = S(R^n, P, F)$. Let us assume that the switching in $Σ$ is determined by a self-triggered controller (see e.g. [21], [2]), which not only selects the mode of the switched system but also the duration during which the mode remains active. We assume that the controller can choose durations from a finite set

$$Θ^N_s = \{θ_s = 2^{-s}τ | s = 0, ..., N\}$$

consisting of dyadic fractions of a time sampling parameter $τ ∈ R^+$ up to some scale parameter $N ∈ N$. Let us remark that the shortest control cycle is $2^{-N}s$ while the longest one is $τ$.

The dynamics of the switched system $Σ$ is then naturally described by the transition system $T^N_s(Σ) = (X, U, Y, Δ, X^0)$ where

- the set of states is $X = R^n$;
- the set of inputs consists of pairs of mode and duration $U = P × Θ^N_s$;
- the set of outputs is the set of continuous functions $Y = \bigcup_{s=0}^{N} C([0, θ_s), R^n)$;
- the transition relation is given for $x ∈ X$ and $u = (p, θ_s) ∈ U$ by $(x', y) = Δ(x, u)$ if and only if

$$x' = x(θ_s, x, p) \text{ and } y = x|_{θ_s}((., x, p)$$
i.e. the switched system moves from state $x$ to state $x'$ by applying the constant mode $p$ for a duration $\theta_i$; $y$ is the continuous-time trajectory of the switched system connecting $x$ to $x'$;

- the set of initial states is $X^0 = \mathbb{R}^n$.

$T_N^\tau(\Sigma)$ is deterministic and metric when the set of outputs $Y$ is equipped with the following metric $d$: for $y \in C([0, \theta_\tau], \mathbb{R}^n)$, $y' \in C([0, \theta_\tau], \mathbb{R}^n)$

$$d(y, y') = \begin{cases} \|y - y'\| & \text{if } \theta_s = \theta_{s'}, \\
+\infty & \text{if } \theta_s \neq \theta_{s'}.
\end{cases}$$

(13)

Note that the state space of $T_N^\tau(\Sigma)$ is uncountable. Let us remark that an output behavior of $T_N^\tau(\Sigma)$ is a sequence of continuous functions $y^0 y^1 y^2 \ldots$. The concatenation of these functions is itself a continuous function which is a trajectory of switched system $\Sigma$.

The computation of a multiscale symbolic model approximating $T_N^\tau(\Sigma)$ can be done using the following approach. We approximate the set of states $\mathbb{R}^n$ by a sequence of embedded multiscale lattices $X^s = [\mathbb{R}^n]_{2^{-s}n}$, $s = 0, \ldots, N$ where

$$[\mathbb{R}^n]_{2^{-s}n} = \left\{ q \in \mathbb{R}^n \mid q[i] = k_i \frac{2^{s+1} \eta}{\sqrt{n}}, k_i \in \mathbb{Z}, \; i = 1, \ldots, n \right\}$$

where $\eta \in \mathbb{R}^+$ is a state space sampling parameter. Let us remark that we have $X^0_n \subseteq X^1_n \subseteq \cdots \subseteq X^N_n$. We associate a multiscale quantizer $Q^s : \mathbb{R}^n \rightarrow [\mathbb{R}^n]_{2^{-s}n}$ such that $Q^s(x) = q$ if and only if

$$q[i] - \frac{2^{-s} \eta}{\sqrt{n}} \leq x[i] < q[i] + \frac{2^{-s} \eta}{\sqrt{n}}, \; i = 1, \ldots, n.$$ 

By simple geometrical considerations, we can check that for all $x \in \mathbb{R}^n$ and $s = 0, \ldots, N$, $\| x - Q^s(x) \| \leq 2^{-s} \eta$.

Then, let us define the transition system $T_{r,\eta}^N(\Sigma) = (X^s_{\eta}, U, Y, \Delta_\eta, X^s_{\eta})$, where

- the set of states is $X^s_{\eta} = [\mathbb{R}^n]_{2^{-s}n}$;
- the set of inputs consists of pairs of mode and duration $U = P \times \Theta_\eta^s$;
- the set of outputs is the set of continuous functions $Y = \bigcup_{s=0}^{\infty} C([0, \theta_\eta], \mathbb{R}^n)$;
- the transition relation is given for $q \in X^s_{\eta}$ and $u = (p, \theta_s) \in U$ by $(q', y) = \Delta_\eta(q, u)$ if and only if

$$q' = Q^s_\eta(x(\theta_s, q, p)) \quad \text{and} \quad y = x|_{\theta_s}(...) \; q, p;$$

- the set of initial states is $X^s_{\eta} = [\mathbb{R}^n]_{\eta}$.

$T_{r,\eta}^N(\Sigma)$ is deterministic and metric when the set of outputs $Y$ is equipped with metric defined in (13). Note that it is symbolic since its sets of states and inputs are respectively countable and finite. An output behavior of $T_{r,\eta}^N(\Sigma)$ is a sequence of continuous functions $y^0 y^1 y^2 \ldots$. It should be noted that the concatenation of these functions may not be a continuous function. Hence, the trajectories of $\Sigma$ are approximated by piecewise continuous functions.

The approximation principle is illustrated in Figure 1. It is important to remark that all the transitions of duration $\theta_s$ end in states belonging to $X^s_{\eta}$. This means that the states on the finer lattices are only accessible by transitions of shorter duration. Also, if we only consider transitions of duration $\tau$, that is if $N = 0$, $T_{r,\eta}^\tau(\Sigma)$ is similar to the uniform abstraction defined in [10].

 Remark 3.1: In [10], the proposed abstraction approach may produce non-deterministic symbolic models. In this paper, the transition relation is defined using the quantizers $Q^s_{\eta}$, $s = 0, \ldots, N$ that ensure determinism of the symbolic model. This is important as the controller synthesis algorithm presented in the next section assumes determinism of the transition system.

Remark 3.2: The computation of the transition relation of the symbolic models involves the resolution of the differential equation (1). The exact computation of the solutions may not be possible but these can be approached arbitrarily close using standard numerical algorithms. In the following, we omit the error due to numerical computations for the sake of simplicity; though, these could be easily taken into account.

Theorem 4: Let us assume that the switched system $\Sigma$ admits a common $\delta$-GUAS Lyapunov function $V$ satisfying (7). Let us consider time and state space sampling parameters $\tau, \eta \in \mathbb{R}^+$, scale parameter $N \in \mathbb{N}$, and a desired precision $\varepsilon \in \mathbb{R}^+$. Then $T_{r,\eta}^N(\Sigma)$ is $\varepsilon$-approximate bisimulation relation between $T_N^\tau(\Sigma)$ and $T_N^{\tau,\eta}(\Sigma)$. We start by remarking that the transition systems are deterministic. Therefore Lemma 2.7 applies. Let $(x, q) \in R$, we have $\text{enab}(x) = \text{enab}(q) = U$; then let $u = (p, \theta_s) \in U$, $(x', y) = \Delta_\eta(x, u)$ and $(q', z) = \Delta_\eta(q, u)$. From (3), it holds for all $t \in [0, \theta_s]$,

$$V(x(t, x, p), x(t, q, p)) \leq e^{-\kappa t} V(x, q) \leq V(x, q) \leq \alpha_\varepsilon(x).$$

Then, (2) gives for all $t \in [0, \theta_s]$.

$$\|y(t) - z(t)\| = \|x(t, x, p) - x(t, q, p)\| \leq \gamma \varepsilon \lesssim V(x(t, x, p), x(t, q, p)) \leq \varepsilon.$$ 

It follows that $d(y, z) \leq \varepsilon$. Since $q' = Q^s_\eta(x(\theta_s, q, p))$, equation (7) yields

$$|V(x', q') - V(x', x(\theta_s, q, p))| \leq \gamma(|q' - x(\theta_s, q, p)|) \leq \gamma(2^{-s} \eta).$$

Then, it holds

$$V(x', q') \leq V(x', x(\theta_s, q, p)) + \gamma(2^{-s} \eta) \leq V(x(q, x, p), x(\theta_s, q, p)) + \gamma(2^{-s} \eta) \leq e^{-\kappa \theta_s} V(x, q) + \gamma(2^{-s} \eta).$$

Then,

$$V(x', q') \leq e^{-\kappa \theta_s} \alpha_\varepsilon(x) + \gamma(2^{-s} \eta) \leq \alpha_\varepsilon(x)$$
because of equation (14). Hence, $(x', q') \in R$ and $R$ is an $\varepsilon$-approximate bisimulation relation between $T^N_{\tau}(\Sigma)$ and $T^N_{\tau,q}(\Sigma)$.

For all $x \in X^0 = \mathbb{R}^n$, $q = Q^0_\eta(x) \in X^0_\eta$ satisfies $\|x - q\| \leq \eta$. Then,

$$V(x, q) \leq \overline{\alpha}(\|x - q\|) \leq \overline{\alpha}(\eta) \leq \overline{\alpha}(\varepsilon)$$
ecuase of equation (14). Hence, $X^0 \subseteq \mathbb{R}^n(X^0_\eta)$. Conversely, for all $q \in X^0_\eta$, $x = q \in X^0$ satisfies $V(x, q) = 0$. Hence, $X^0 \subseteq \mathbb{R}^n(X^0)$. Therefore, $T^N_{\tau}(\Sigma)$ and $T^N_{\tau,q}(\Sigma)$ are $\varepsilon$-approximately bisimilar.

It is interesting to note that given a time sampling parameter $\tau > 0$ and a scale parameter $N \in \mathbb{N}$, for any desired precision $\varepsilon > 0$, there always exists $\eta > 0$ such that equation (14) holds. This essentially means that approximately bisimilar symbolic models of arbitrary precision can be computed for $T^N_{\tau}(\Sigma)$. Let us remark that for $N = 0$ we obtain a result that is similar to that in [10] with the difference that the symbolic models here have continuous-time outputs.

### B. Switched systems with dwell-time

We now consider the case of switched systems with minimum dwell-time. Let $\Sigma_{\tau,d} = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system where $\mathcal{P} = \mathcal{S}_{\tau,d}(\mathbb{R}^n, P)$. Let $\Theta^N_{\tau}$ be given as before by (12) where the time sampling parameter $\tau \in \mathbb{R}^+$ and the scale parameter $N \in \mathbb{N}$. For simplicity, we make the assumption that there exists $N_d \in \{0, \ldots, N\}$ such that the minimum dwell-time $\tau_{\min} = \theta_{N_d} = 2^{-N_d}\tau$. Then, let $\Theta^N_{\tau,d}$ be defined as in (12); we have $\Theta^N_{\tau,d} \subseteq \Theta^N_{\tau}$.

The dynamics of the switched system $\Sigma_{\tau,d}$ can then be described by the transition system $T^N_{\tau,d}(\Sigma_{\tau,d}) = (X, U, Y, \Delta, X^0)$ where

- the set of states is $X = \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n$,
- the set of inputs consists of pairs of mode and duration $U = \mathbb{R}^n \times \mathbb{R}^n$,
- the set of outputs is the set of continuous functions $Y = \bigcup_{\varepsilon > 0} \mathbb{C}([0, \theta_\varepsilon], \mathbb{R}^n)$,
- the transition relation is given for $x = (x, p) \in X$ and $u = (p', \theta_\varepsilon) \in \Theta^N_{\tau,d}$, $x' = \Delta(x, u)$ if only if $x' = (x', p')$ and $x' = x(\theta_\varepsilon, x, p')$ and $y = x|_{\varepsilon}(x, x, p')$.

The set of enabled inputs is $\Theta(x \in \Theta^N_{\tau,d}) \times \Theta^N_{\tau,d}$; the set of initial states is $X^0 = \mathbb{R}^n \times \mathbb{R}^n$.

$T^N_{\tau,d}(\Sigma_{\tau,d})$ is deterministic and metric when the set of outputs $Y$ is equipped with the metric defined in (13). It is symbolic since its sets of states and inputs are respectively countable and finite.

**Theorem 5**: Let $\mu$ assume that the switched system $\Sigma_{\tau,d}$ admits multiple $\delta$-GUAS Lyapunov functions $V_{\tau,d} \in \mathcal{P}$, satisfying (8). Let us consider time and state space sampling parameters $\tau, \eta \in \mathbb{R}^+$, scale parameter $N \in \mathbb{N}$, and a desired precision $\varepsilon \in \mathbb{R}^+$. If $\tau_d > \log \frac{\mu}{\varepsilon}$ and

$$\eta \leq \min \left\{ \min_{s=0}^{N_d} \left[ \frac{2^s - 1}{\mu} \right] \right\} \leq \frac{\mu}{\varepsilon} \varepsilon \leq \overline{\alpha}(\varepsilon)$$

Then $T^N_{\tau,d}(\Sigma_{\tau,d}) \sim_{\varepsilon} T^N_{\tau,q}(\Sigma_{\tau,d})$.

**Proof:** We start by showing that the relation $R$ is defined by

$$R = \left\{(z, r) \in X \times X^0 \mid z = (x, p), r = (q, p) \right\}$$

is an $\varepsilon$-approximate bisimulation relation between $T^N_{\tau,d}(\Sigma_{\tau,d})$ and $T^N_{\tau,q}(\Sigma_{\tau,d})$. The transition systems are deterministic, therefore Lemma 2.7 applies. Let $(z, r) \in R$, $z = (x, p)$, $r = (q, p)$, we have $e_{\tau}(z, r) = e_{\tau}(\{p\} \times \Theta^N_{\tau} \cup \{P \setminus \{p\}\} \times \Theta^N_{\tau,d})$. Let $u = (p', \theta_\varepsilon) \in \Theta(x, u)$, $(z', y) = \Delta(x, u)$, $z' = (x', p')$ and $(r', z) = \Delta(y, u)$, $r' = (q', p')$. If $p' = p$, from (5) and since $\mu \geq 1$, it holds for all $t \in [0, \theta_\varepsilon]$.

$$V_{\tau,d}(x(t, x, p), x(t, q, p)) \leq \left| e^{-\gamma} V_{\tau,d}(x(t, x, p), q(2^{-s})) \right| \leq \frac{\mu}{\varepsilon} \overline{\alpha}(\varepsilon) \leq \overline{\alpha}(\varepsilon).$$

Then, (4) gives for all $t \in [0, \theta_\varepsilon]$.

$$\|x(t) - z(t)\| \leq \|x(t, x, p) - x(t, q, p)\| \leq \alpha^{-1}(V_{\tau,d}(x(t, x, p), x(t, q, p))) \leq \varepsilon.$$
multiscale symbolic models of arbitrary precision can be computed for $T^N_v(\Sigma_{\mathcal{M}_v})$.

IV. SAFETY CONTROLLER SYNTHESIS USING MULTISCALE SYMBOLIC MODELS

In this section, we present controller synthesis techniques based on the use of the multiscale symbolic models defined in the previous section. We focus on a class of safety specifications. The principle of the proposed solution is to exploit the specific properties of multiscale abstractions: i.e. we give higher priority to transitions of longer duration in order to keep the state of the system as much as possible at the coarser scale. Then, the finer scales are explored only when the specification cannot be met at the coarser level. The symbolic models need not be computed prior to controller synthesis. Their computation can be handled on the fly, thus keeping the effective number of symbolic states at a reasonable level.

In the following, let us consider a transition system $T = (X, U, Y, \Delta, X^0)$ which can be, for instance, one of the multiscale symbolic models defined in the previous section.

A. Safety controllers

In this section, we formalize the problem of safety controller synthesis. We make the following assumption on $T$:

**Assumption 1:** We assume that $T$ is symbolic and deterministic. We assume that the set of outputs $Y$ consists of continuous functions $y \in C([0, \theta_y], \mathbb{R}^n)$ for some $\theta_y \in \mathbb{R}^+$. Assumption 1 is satisfied by the multiscale symbolic models defined in the previous section.

**Definition 4.1:** A safety specification automaton is a tuple $T = (Q, E, I, G, Q^0)$ consisting of a finite set of states $Q; a$ transition relation $E \subseteq Q \times Q$; a set of invariants $I = \{I_q \subseteq \mathbb{R}^n, q \in Q\}; a$ set of guards $G = \{G_e \subseteq \mathbb{R}^n, e \in E\}; a$ set of initial states $Q^0 \subseteq Q$.

We shall make the following assumptions on the specification automaton:

**Assumption 2:** There is a minimum separation between guards of successive transitions: there exists $\epsilon > 0$ such that, for all $e = (q, q'), e' = (q'', q'') \in E$,

$$\inf \{|x - x'| \mid x \in G_e, x' \in G_{e'}\} \geq \epsilon.$$  

We now define the composition of a transition system with a safety specification automaton:

**Definition 4.2:** Under Assumptions 1 and 2, the composition of the transition system $T = (X, U, Y, \Delta, X^0)$ with the safety automaton $T = (Q, E, I, G, Q^0)$ is the transition system $T||T = (X_S, U_S, Y, \Delta_S, X^0_S)$ where the set of states $X_S = Q \times X$; the set of inputs is $U_S = Q \times U$; the set of outputs is $Y$; the set of initial states is $X^0_S = Q^0 \times X^0$; the transition relation is given for $z = (q, x), z' = (q', x') \in X_S, v = (q', u) \in U_S, y \in Y$ by $(z', y) \in \Delta_S(z, v)$ if and only if $u \in \text{enab}(x)$, $(x', y) = \Delta(x, u)$, $q' = q''$, and one of the following conditions holds:

- $q = q'$ and $\forall t \in [0, \theta_y], y(t) \in I_q$;
- there exists $0 = t_0 \leq t_1 \leq \cdots \leq t_M \leq t_{N+1} = \theta_y$ and $e_i = (q_i, q_{i+1}) \in E$, $i = 0, \ldots, N$ with $q_0 = q, q_N = q'$ and
  \[
  \begin{cases}
  \forall t \in [t_i, t_{i+1}], y(t) \in I_{q_i}, & i = 0, \ldots, N; \\
  y(t_{i+1}) \in G_{e_i}, & i = 0, \ldots, N - 1.
  \end{cases}
  \]

If $u \in \text{enab}(x)$, but none of the previous conditions hold with $(x', y) = \Delta(x, u)$ and $q' = q''$, or if $u \notin \text{enab}(x)$, then $\Delta_S(z, v) = \emptyset$.

**Remark 4.3:** For the second type of transitions defined above, we would like to point out that $y$ is continuous on the compact set $[0, \theta_y]$, therefore it is uniformly continuous, then Assumption 2 on minimum separation of guards of successive transitions implies that there exists $h > 0$ such that $t_{i+1} - t_i \geq h$, for $i = 1, \ldots, N - 1$. Hence, $N$ is bounded above by $1 + \theta_y/h$ thus ruling out potential Zeno behaviors (see e.g. [23]).

**Remark 4.4:** The specification formalism of safety specification automata is derived from the classical notion of hybrid automata [11], also used as a specification formalism in [3]. It can be shown that any regular safety property over state predicates (i.e. whose set of bad prefixes is recognized by a finite state automaton, as defined in [41]) can be written under the form of a safety specification automaton.

We claim the following properties of the transition system $T||T$:

**Lemma 4.5:** $T||T$ is a symbolic and deterministic transition system.

**Proof:** The fact that $T||T$ is symbolic is a consequence of $T$ being symbolic and $Q$ finite. To show that it is deterministic, let $z = (q, x), v = (q', u) \in U_S$ such that $\Delta_S(z, v) \neq \emptyset$ then let $(z', y) \in \Delta_S(z, v)$ with $z' = (q', x')$. From the Definition 4.2, it follows that $q' = q''$ and $(x', y) = \Delta(x, u)$. Thus, $(z', y)$ is uniquely determined and $T||T$ is deterministic.

A trajectory of $T$, $\sigma = (x^0, u^0, y^0), (x^1, u^1, y^1), (x^2, u^2, y^2) \ldots$ is safe according to the safety specification automaton $S$ if it is infinite and there exists a trajectory of $T||T, \sigma_S = (x^0, u^0, y^0), (z^1, v^1, y^1), (z^2, v^2, y^2) \ldots$ with $z^i = (q', x')$, $v^i = (q', u')$, for all $i \geq 0$. A safety controller is then a controller that prevents $T||T$ from reaching a blocking state.

**Definition 4.6:** A safety controller for $T||T = (X_S, U_S, Y, \Delta_S, X^0_S)$ is a relation $C \subseteq X_S \times U_S$ such that for all $z \in X_S$:

- $C(z) \subseteq \text{enab}(z)$;
- if $C(z) \neq \emptyset$, then for all $v \in C(z)$ with $\Delta_S(z, v) = (z', y)$, it holds that $C(z') \neq \emptyset$.

We denote the domain of $C$ as $\text{dom}(C) = \{z \in X_S \mid C(z) \neq \emptyset\}$. The controlled system is given by the transition system $T||S/C = (X_S, U_S, Y, \Delta_S/C, X^0_{S/C})$ where the transition relation is given for $z \in X_S, v \in U_S, y \in Y$ by $(z', y) \in \Delta_S/C(z, v)$ if and only if $u \in C(z)$ and $(z', y) = \Delta_S(z, v)$; the set of initial states is $X^0_{S/C} = X^0_S \cap \text{dom}(C)$.

**Lemma 4.7:** $T||S/C$ is a symbolic, deterministic, and non-blocking transition system.

**Proof:** The fact that it is symbolic and deterministic comes directly from Lemma 4.5. From the first point of Definition 4.6 and by definition of $\Delta_S/C$, a state $z \in X_S$ of $T||S/C$ is non-blocking if and only if $C(z) \neq \emptyset$. Then, by definition of $X^0_{S/C}$, all initial states of $T||S/C$ are non-blocking. Also, by the second point of Definition 4.6 and by definition of the transition relation $\Delta_S/C$, all reachable states of $T||S/C$ are non-blocking.

Thus, the previous lemma shows that all maximal trajectories of $T||S/C$ are infinite trajectories of $T||T$ and thus generates safe trajectories of the transition system $T$. There are in general several safety controllers, however, one can show that there exists one that is maximal:

**Lemma 4.8:** There exists a unique maximal safety controller $C^* \subseteq X_S \times U_S$ such that for all safety controllers $C, C \subseteq C^*$.

**Proof:** We can check from Definition 4.6 that the union of safety controllers is again a safety controller. Then, the union of all safety controllers is a safety controller which contains all the others, it is clearly unique.

The previous result justifies the following notion of controllability:
Definition 4.9: A state $z \in X_S$ of $T||S$ is safety controllable if and only if $z \in \text{dom}(C^*)$. The set of safety controllable states is denoted $\text{cont}(T||S)$.

Of course from the previous definition, it follows that $\text{cont}(T||S) = \text{dom}(C^*)$. Also, it can be easily established (see e.g. [18]) that for all $z \in X_S$:

$$C^*(z) = \left\{ v \in \text{enab}(z) \mid z' \in \text{cont}(T||S) \text{ with } (z', y) = \Delta_S(z, v) \right\}.$$ (16)

Remark 4.10: A classical safety specification consists in keeping the output values of $T$ in a given set $I_S \subseteq \mathbb{R}^n$. This is a special case of Definition 4.1 corresponding to the safety specification automaton $S = (Q, E, I, G, Q_0)$ with a single state $Q = \{ q \}$, no transitions $E = \emptyset$, the invariant $I = \{ I_S = I_S \}$, $G = \emptyset$, and $Q_0 = Q$.

Remark 4.11: Continuous-time outputs do not play a role in the characterization of a safety controller given by Definition 4.6. Then, as far as controller synthesis is concerned, the transition system $T||S$ can be considered as a purely discrete transition system (without outputs) and any discrete controller synthesis technique can be used. In the following, we propose an approach exploiting the properties of multi-scale symbolic models.

B. Maximal lazy safety controller

Let us remark that the maximal safety controller $C^*$ is computable using a simple fixed point algorithm (see e.g. [17], [18]). Termination of the algorithm is guaranteed if the number of non-blocking states of $T||S$ is finite. This is the case for the symbolic models defined in Section III provided that invariants and guards of the safety specification automaton are bounded sets. However, the larger the number of states in the symbolic models, the more expensive the computation.

For that reason, we want to exploit multiscale symbolic models to propose a more efficient algorithm for the synthesis of safety controllers. The lazy safety synthesis problem consists in controlling the system $T||S$ so as to prevent trajectories from reaching a blocking state, while applying at each step a transition of the longest duration for which safety can be guaranteed.

Assumption 3: We assume that the set of inputs $U$ is finite and equipped with a priority relation given by a total preorder $\preceq U \times U$.

For the multiscale symbolic models where $U = P \times \Theta^N$, for $u = (p, \theta_1), u' = (p', \theta_2) \in U$, we give priority to transitions of longer duration by defining $u \preceq u'$ if and only if $\theta_2 \preceq \theta_1$. The associated equivalence relation $\equiv$ and strict weak order $\prec$ are then given by $u \equiv u'$ if and only if $\theta_2 = \theta_1$ and $u \prec u'$ if and only if $\theta_2 \prec \theta_1$.

We lift the preorder $\preceq U \times U$ to the set $U_S = Q \times U$ as follows, for $v = (q, u), v' = (q', u') \in U_S$, $v \preceq v'$ if and only if $u \preceq u'$. The associated equivalence relation $\equiv$ and strict weak order $\prec$ are lifted similarly. Since $U_S$ is finite, we can define for any subset $V \subseteq U_S$:

$$\max_{\preceq}(V) = \{ v \in V \mid \forall v' \in V, v' \preceq v \}.$$

We can now formalize the notion of maximal lazy safety controller:

Definition 4.12: A maximal lazy safety (MLS) controller for $T||S = (X_S, U, Y, \Delta_S, X^0_S)$ is a safety controller $C \subseteq X_S \times U_S$ such that:

- all safety controllable initial states are in $\text{dom}(C)$:

$$X^0_S \cap \text{cont}(T||S) \subseteq \text{dom}(C);$$

- all states $z \in \text{dom}(C)$ are reachable in $T||S/C$;

- for all states $z \in \text{dom}(C)$:

1) if $v \in C(z)$, then for all $v' \in \text{enab}(z)$ with $v \preceq v'$, $(z', y) = \Delta_S(z, v')$, it holds that $v' \in C(z)$ if and only if $z' \in \text{cont}(T||S)$;

2) if $v \in C(z)$, then for all $v' \in \text{enab}(z)$ with $v \prec v'$, $(z', y) = \Delta_S(z, v')$, it holds that $z' \not\in \text{cont}(T||S)$.

The term maximal comes from the fact that all safety controllable initial states are in $\text{dom}(C)$, and if the controller enables an input, it also enables all inputs with the same priority and which preserve safety. The term lazy refers to the fact that when several inputs can preserve safety, the controller enables only inputs with highest priority (i.e. with longer duration for our multiscale symbolic models). Hence, the maximal lazy safety controller $C$ represents a trade-off between maximal permissiveness and efficiency.

Theorem 6: There exists a unique MLS controller for $T||S$.

Proof: We first prove existence and then uniqueness.

Existence: Let $C^*$ be the maximal (non-lazy) safety controller for $T||S$. Let $C^*$ be the controller defined from $C^*$ as follows: for all $z \in X_S$, $C^*(z) = \max_{\preceq} C^*(z)$. Then, we have $\text{dom}(C^*) = \text{cont}(T||S)$.

Let us show that $C^*$ is a safety controller for $T||S$. Let $z \in X_S$, we have $C^*(z) \subseteq C^*(z) \subseteq \text{enab}(z)$; hence the first condition of Definition 4.6 holds. If $C^*(z) \neq \emptyset$, then for all $v \in C^*(z)$, we also have $v \in C^*(z)$ and therefore for $(z', y) = \Delta_S(z, v)$ it holds $C^*(z') \neq \emptyset$ which yields $C^*(z') \neq \emptyset$; hence the second condition of Definition 4.6 holds as well. Now let us show that $C^*$ satisfies conditions (1) and (2) of Definition 4.12. Let $z \in \text{dom}(C^*)$, $v \in C^*(z)$, and $v' \in \text{enab}(z)$ with $v \preceq v'$, $(z', y) = \Delta_S(z, v')$. If $v' \in C^*(z)$ then since $C^*$ is a safety controller, we have $z' \in \text{dom}(C^*) = \text{cont}(T||S)$. If $z' \not\in \text{cont}(T||S)$, it follows from (16) that $z' \in C^*(z)$. Since $v \in \max_{\preceq} C^*(z)$ and $v \prec v'$, it follows that $v' \in \max_{\preceq} C^*(z)$. Hence, $v' \in C^*(z)$ and condition (1) of Definition 4.12 holds. Let $z \in \text{dom}(C^*)$, $v \in C^*(z)$, and $v' \in \text{enab}(z)$ with $v \prec v'$, $(z', y) = \Delta_S(z, v')$. Since $C^*(z) = \max_{\preceq} C^*(z)$, it follows from $v \prec v'$ that $v' \not\in C^*(z)$. From (16), we have $z' \not\in \text{cont}(T||S)$. Hence, condition (2) of Definition 4.12 holds as well.

Now let $C'$ be the controller defined from $C^*$ by $C'(z) = \max_{\preceq} C^*(z)$ if $z$ is reachable in $T||S/C^*$ and $C'(z) = \emptyset$ otherwise. It is clear that the reachable states in $T||S/C^*$ and $T||S/C$ are the same. Hence, for all $z \in \text{dom}(C)$, $z$ is reachable in $T||S/C$. Moreover, it follows from the properties of $C^*$ that $C$ is a safety controller for $T||S$, and that $C$ satisfies conditions (1) and (2) of Definition 4.12. Let $z \in X^0_S \cap \text{cont}(T||S) = X^0_S \cap \text{dom}(C^*) = X^0_S \cap C^*$. Since any initial state is reachable, $z$ is reachable in $T||S/C^*$. Therefore, we have $C(z) = C^*(z) = \emptyset$ and $z \in \text{dom}(C)$.

Uniqueness: Let $C_1$ and $C_2$ be two MLS controllers and assume that there exists $z \in X_S$ such that $C_1(z) \neq C_2(z)$.

If both $C_1(z)$ and $C_2(z)$ are not empty, we can assume without loss of generality that there exists $v_1 \in C_1(z)$ such that $v_1 \not\in C_2(z)$. Then, let $v_2 \in C_2(z)$. If $v_1 \prec v_2$ then condition (2) of Definition 4.12 does not hold for $C_1$ since $\Delta_S(z, v_2) \in \text{cont}(T||S)$. If $v_2 \prec v_1$ then condition (2) of Definition 4.12 does not hold for $C_2$ since $\Delta_S(z, v_1) \in \text{dom}(C_1) \subseteq \text{cont}(T||S)$. If $v_1 \approx v_2$, then condition (1) of Definition 4.12 does not hold for $C_2$ since $\Delta_S(z, v_1) \in \text{dom}(C_1) \subseteq \text{cont}(T||S)$.

In all the cases one of the controllers is not a MLS controller.

If one of $C_1(z)$ and $C_2(z)$ is empty, we can assume without loss a generality that $C_1(z) = \emptyset$ and $C_2(z) = \emptyset$. $z \in \text{dom}(C_1) \subseteq \text{cont}(T||S)$ therefore $z$ cannot be in $X^0_S$ otherwise we would have $C_2(z) = \emptyset$. Since $z \in \text{dom}(C_1)$, $z$ is reachable in $T||S/C_1$. Let us consider the initialized trajectory of $T||S/C_1$, $(z^0, v^0, y^0)(z^1, v^1, y^1)\ldots(z^n, v^n, y^n)$ with $z^n = z$. 
Controller synthesis

In this section, we present an algorithm for synthesizing the maximal lazy safety controller. It is based on a depth first search exploration of the trajectories, starting from initial states and exploring transitions of higher priority first.

More precisely, the MLS controller is computed by Algorithm 1 which calls the function explore(z, 0) on each initial state z ∈ X₀; the second argument Xv of the function explore is the set of states already visited by the current trajectory. The global variables are Xv, Xu, and C for the sets of controllable and uncontrollable states and the controller, respectively. Function explore(z, Xv) returns whether z is controllable. This is done by recursively exploring the paths starting from z until either a controllable or an uncontrollable state is reached; or a state already visited by the current trajectory is reached, which means that a circular path containing z has been found, and therefore the state z is controllable. The outer loop explores inputs of decreasing priority as long as no controllable successor of z has been found.

Theorem 7: Let C be computed by Algorithm 1. Then, C is the MLS controller for T||S.

Proof: The set of visited states Xv contains, at each call to explore, the set of states visited along one path from some initial state z₀ in X₀ to (excluding) the current state z. A state z is determined controllable if it:

- has one immediate controllable successor (line 19), in that case z and all states in Xu are added recursively to the set of controllable states Xc;
- has already been visited along the current path Xv (i.e. z ∈ Xv) (line 8) — hence, lying on a cyclic path of safe states, in that case all states in Xv (including z) are added recursively to the set of controllable states Xc.

In contrast, z is determined uncontrollable if all its successors are uncontrollable (line 22), in that case z is added to the set of uncontrollable states Xu. Hence, Xc and Xu contains all the controllable and uncontrollable states that have been explored, respectively. Let us also remark that C(z) = Ø if and only if z ∈ Xc.

Let us verify that C is a safety controller. By construction (line 9), we have C(z) ⊆ enab(z). Then, assume C(z) ≠ Ø, and let v ∈ C(z), (z′, y) = ΔS(z, v), then it holds that z′ is controllable (line 14). Thus z′ ∈ Xc and C(z′) ≠ Ø.

We now prove that C is the MLS controller. In Algorithm 1, the function explore is called for all initial states in X₀; Then, it follows that all controllable initial states are in X₀, the first point of Definition 4.12 holds. Since Algorithm 1 explores trajectories starting from initial states, all states in dom(C) = Xc are reachable in T||S/C, the second point of Definition 4.12 holds. As for the third point, let z ∈ dom(C) and v ∈ C(z). The outer loop of the function explore (lines 10 to 20) explores trajectories using inputs of higher priority first. Hence, if v ∈ C(z) then all inputs v′ ∈ enab(z) with v ≼ v′ have been explored and none of them leads to a controllable state. Hence, 2) in the third point of Definition 4.12 holds. The inner loop of the function explore (lines 12 to 16) explores trajectories using all inputs with the same level of priority. Hence, if v ∈ C(z) then all inputs v′ ∈ enab(z) with v ≃ v′ have been explored and v′ ∈ C(z) if an only if it leads to a controllable state. Hence, 1) in the third point of Definition 4.12 holds. Thus, C is the MLS controller for T||S.

In Algorithm 1, each transition initiating from a non-blocking state is explored at most once. Hence, termination of Algorithm 1 is guaranteed if the sets of inputs US and of non-blocking states are finite: note that this is the case for our multiscale symbolic models when invariants and guards of the safety specification automaton are bounded sets. In the worst case, (when all non-blocking states are reachable but none is controllable), all the transitions initiating from a non-blocking state need to be explored. This provides us with a
worst-case (time and space) complexity given by $|X_S^b| \times |U_S|$ where $X_S^b$ denote the set of non-blocking states. However, in practice this upper-bound is not attained.

V. COMPUTATIONAL RESULTS

In this section, we show some computational results of our approach obtained using CoSyMA [12], a tool for automatic controller synthesis for incrementally stable switched systems based on multiscale symbolic models. It is written in OCaml and provides an implementation of Algorithm 1 for symbolic models of switched systems (with or without dwell time) and simple safety specifications (see Remark 4.10). The results reported in the following have been obtained on a laptop with i7 processor and 4 GB RAM.

A. DC-DC Converter

As a first case study, we apply our approach to a boost DC-DC converter. It is a switched system with two modes, the two dimensional dynamics associated with both modes are affine of the form $\dot{x}(t) = A_p(t)x(t) + b$ for $p(t) \in \{1, 2\}$ (see [10] for numerical values). It can be shown that it has a common $\delta$-GUAS Lyapunov function and thus approximately bisimilar symbolic models can be computed. We consider the problem of keeping the state of the system in a desired region of operation given by the safe set $I_S = [1.15, 1.55] \times [5.45, 5.85]$.

We use approximately bisimilar symbolic models to synthesize MLS controllers for the DC-DC converter. We compare the cost of controller synthesis for the uniform symbolic model $T_{\tau_1, \eta_1}^0(\Sigma)$ for parameters $\tau_1 = 0.5$ and $\eta_1 = 3 \times 10^{-4}$ (containing only transitions of duration 0.5s) and the multi-scale symbolic model $T_{\tau_2, \eta_2}^0(\Sigma)$ for parameters $\tau_2 = 64\tau_1$ and $\eta_2 = 64\eta_1$ (containing transitions of durations in $\Theta^b = \{32, 16, 8, 4, 2, 1, 0.5\}$). The set of states of $T_{\tau_2, \eta_2}^0(\Sigma)$ consists of a set of 7 embedded lattices whose finest one coincides with the set of states of $T_{\tau_1, \eta_1}^0(\Sigma)$. These two symbolic models have the same precision $\varepsilon = 0.05$, according to Theorem 4.

Table I details the experimental results obtained for the synthesis of the $T_{\tau_1, \eta_1}^0(\Sigma)$ and $T_{\tau_2, \eta_2}^0(\Sigma)$. We can see that there is a noteworthy reduction of the time used to compute the controller using a multiscale symbolic model instead of using a uniform one (up to a 93% improvement between $T_{\tau_1, \eta_1}^0(\Sigma)$ and $T_{\tau_2, \eta_2}^0(\Sigma)$). This is due to the fact that the size of uniform symbolic models grows exponentially with higher resolutions, whereas multiscale symbolic models are refined only when we get closer to unsafe regions (size reduced by more than 99% between $T_{\tau_1, \eta_1}^0(\Sigma)$ and $T_{\tau_2, \eta_2}^0(\Sigma)$). Interestingly, this reduction in computation time and size does not affect the performance of the multi-scale controllers, which yield a ratio of controllable initial states (defined as $|\text{dom}(C) \cap X_S^b|/|X_S^b \cap I_S|$) comparable to that of their uniform counterparts. Figure 2 depicts the maximal lazy safety controller for $T_{\tau_2, \eta_2}^0(\Sigma)$ and a trajectory of the controlled switched system.

![Fig. 2. The MLS controller for $T_{\tau_2, \eta_2}^0(\Sigma)$ and $I_S$. Top: mode 1 is enabled (light gray); mode 2 is enabled (dark gray); modes 1 and 2 are enabled (medium gray); and a trajectory. Bottom: duration 4 (light gray), 2 (medium gray), 1 (dark gray), 0.5 (black) are enabled.](image)

<table>
<thead>
<tr>
<th>Uniform symbolic model</th>
<th>Multiscale symbolic model</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N = 0, \tau = 0.5$</td>
<td>$N = 6, \tau = 32$</td>
</tr>
<tr>
<td>$\eta = 0.0003, \varepsilon = 0.05$</td>
<td>$\eta = 0.018, \varepsilon = 0.05$</td>
</tr>
</tbody>
</table>

**Table I**

<table>
<thead>
<tr>
<th>Time</th>
<th>9.2s</th>
<th>0.6s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size ($10^5$)</td>
<td>936</td>
<td>6</td>
</tr>
<tr>
<td>Durations</td>
<td>0.5 (100%)</td>
<td>4 (33%)</td>
</tr>
<tr>
<td>Cont. Ratio</td>
<td>95%</td>
<td>92%</td>
</tr>
</tbody>
</table>

**Experimental results for the MLS controller synthesis for the boost DC-DC converter**

B. Temperature regulation in an n-room building

The second case study deals with temperature regulation in a circular building with $n$ rooms. Each room is equipped with a heater and at a given instant at most one heater is switched on. The temperature $T_i(t)$ of the room $i$, $1 \leq i \leq n$, is defined by the differential equation

$$
T_i(t) = \alpha(T_{i+1}(t) + T_{i-1}(t) - 2T_i(t)) + \beta(t_e - T_i(t)) + \gamma(t_h - T_i(t))u_i(t)
$$

where $T_{i-1}(t)$ is the temperature of the room $i - 1$, $T_{i+1}(t)$ the temperature of the room $i + 1$ (with the convention that $T_0(t) = T_n(t)$ and $T_{n+1}(t) = T_1(t)$); $t_e$ is the temperature of the external environment of the building; $t_h$ is the temperature of the heater; $\alpha$ is the conduction factor between the rooms $i \pm 1$ and the room $i$; $\beta$ is the conduction factor between the external environment and the room $i$; $\gamma$ is the conduction factor between the heater and the room $i$; $u_i(t)$ equals to 1 if the room $i$ is heated, or 0 otherwise.

Given a number $n \geq 2$ of rooms, we distinguish $n + 1$ switching modes. For $1 \leq i \leq n$, the mode $p_i$ represents the mode of activating the heater of room $i$. The mode $p_{n+1}$ represents that no heater is activated. The values of $\alpha$, $\beta$, $\gamma$, $t_e$, and $t_h$ are respectively...
Multiscale symbolic models

| $N = 4$, $\tau = 80$, $\eta = 0.28$, $\varepsilon = 0.4$ | $n = 3$ | $n = 4$ | $n = 5$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>0.25</td>
<td>6s</td>
<td>31.25</td>
</tr>
<tr>
<td>Size ($10^6$)</td>
<td>2</td>
<td>45</td>
<td>1077</td>
</tr>
<tr>
<td>Durations</td>
<td>40 (1%)</td>
<td>20 (25%)</td>
<td>20 (6%)</td>
</tr>
<tr>
<td></td>
<td>20 (37%)</td>
<td>10 (73%)</td>
<td>10 (92%)</td>
</tr>
<tr>
<td></td>
<td>10 (62%)</td>
<td>5 (2%)</td>
<td>5 (2%)</td>
</tr>
<tr>
<td>Cont. Ratio</td>
<td>99.99%</td>
<td>99.89%</td>
<td>99.79%</td>
</tr>
</tbody>
</table>

**Table II**

Experimental results for the synthesis of the MLS controller for temperature regulation in a building of three, four, and five rooms.

Fig. 3. Partial view of the MLS controller for $T^I_{\tau, \eta}(\Sigma)$ and $I_S$ for the 4 room building in the plane $(T_1, T_2)$ with $T_3 = T_4 = 10$. Left: mode 1 is enabled (light gray); mode 2 is enabled (black); modes 1 and 2 are enabled (gray); other modes are not displayed. Right: duration 20 (light gray), 10 (gray), 5 (black) are enabled.

Following the approach in [10] (extended to deal with continuous-time outputs), a controller is computed using a uniform symbolic model with dwell-time for time and state sampling parameters $\tau_1 = 0.5$ and $\eta_1 = 1/(100\sqrt{2})$. Let us remark that the uniform abstraction with dwell time can not be defined as described in Section III-B since we have $\tau_d > \tau_1$. The computation of the controller using a Matlab script takes 160 seconds. The resulting controller contains 5228091 states.

We computed the MLS controller for the multiscale symbolic model $T^I_{\tau_2, \eta_2}(\Sigma_{rd})$ for parameters $\tau_2 = 8\tau_1$, $\eta_2 = 8\eta_1$ (containing transitions of durations in $\Theta^3_{rd} = \{4, 2, 1, 0.5\}$). The set of states of $T^I_{\tau_2, \eta_2}(\Sigma_{rd})$ consists of a set of 4 embedded lattices whose finest one coincides with the set of states of the uniform abstraction. The two symbolic models have the same precision $\varepsilon = 0.4$. The computation of the MLS controller took 7.3 seconds. The resulting controller contains 33826 states, a notable reduction compared to the uniform symbolic model. The controllability ratio is 79.38% and the proportion of transitions of duration 4, 2, 1 and 0.5 are 26%, 54%, 11% and 9% respectively. Figure 4 shows the mode map of the MLS controller. A controlled trajectory of the switched system is shown on Figure 5.

VI. Conclusion

In this paper we have proposed the use of multiscale symbolic models for the computation of controllers for switched systems, by applying them to the specific case of safety problems. We have proposed a construction of multiscale symbolic models and proved...
that they are approximately bisimilar to the original switched systems under the existence of (common or multiple) 6-GUAS Lyapunov functions. We have considered the use of these models for synthesizing controllers enforcing properties given by safety specification automata. An appropriate formulation of the synthesis problem and an algorithm have been proposed, exploiting the characteristics of the multiscale symbolic models. Experimental results show a major improvement of computational complexity when using multiscale symbolic models instead of uniform ones.

REFERENCES

Sebti Mouelhi received the M.S. degree in computer science from the University of Lorraine, Nancy, France, in 2007 and the Ph.D. in computer science from the University of Franche-Comté, Besançon, France, in 2011. From October 2011 to September 2012, he was hired as a postdoctoral researcher at INRIA Grenoble, France. From October 2012 to May 2015, he was research and development engineer at SafeRiver, Montrouge, France. During Summer 2015, he was engineer in safety assurance at ALSTOM Transport, Saint-Ouen, France. Since September 2015, he is teacher and researcher at École Centrale d’Électronique (ECE Paris), member of Laureate International Universities.

His activities are mainly in the topic of the formal design and verification of component-based, real-time, and safety-critical embedded systems, especially railway and automotive systems. He is also interested in the use of formal methods for the control of hybrid and cyber-physical systems.