Safety Controller Synthesis for Incrementally Stable Switched Systems Using Multiscale Symbolic Models

Antoine Girard, Gregor Gössler, Sebti Mouelhi

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

Antoine Girard is with Laboratoire des signaux et systèmes (L2S), CNRS, CentraleSupélec, Université Paris-Sud, Université Paris-Saclay, 3, rue Joliot-Curie, 91192 Gif-sur-Yvette, cedex, France antoine.girard@l2s.centralesupelec.fr.

G. Gössler is with INRIA Grenoble - Rhône-Alpes, France, gregor.goessler@inria.fr.

S. Mouelhi is with École Centrale d'Électronique (ECE Paris), F-75015, Paris, France, sebti.mouelhi@ece.fr.

This work was supported by the Agence Nationale de la Recherche (VEDECY project - ANR 2009 SEGI 015 01) and by the pole MSTIC of Université Joseph Fourier (SYMBAD project).

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. $\mathbb{R}$, $\mathbb{R}_0^+$ 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-continous at a and left-continuous at b. The set of continuous functions from I to $\mathbb{R}^n$ is denoted $\mathcal{C}(I, \mathbb{R}^n)$. For $f \in \mathcal{C}(I, \mathbb{R}^n)$, we define $\|f\| = \sup_{s \in I} \|f(s)\|$. Given a function $f : \mathbb{R}_0^+ \to \mathbb{R}^n$, and $\tau \in \mathbb{R}^+$, we denote by $f|_\tau$ the restriction of f to the interval $[0, \tau]$. A continuous function $\gamma : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{K}$ if it is strictly increasing, and $\gamma(0) = 0$. It is of class $\mathcal{K}_\infty$ if it is of class $\mathcal{K}$ and $\gamma(r) \to \infty$ when $r \to \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}$ if for all fixed s, the map $r \mapsto \beta(r, s)$ belongs to class $\mathcal{K}$ and for all fixed $r > 0$, the map $s \mapsto \beta(r, s)$ is strictly decreasing and $\beta(r, s) \to 0$ when $s \to \infty$. Given two sets S_1, S_2 and a relation $R \subseteq S_1 \times S_2$, we denote $R(s_1) = \{s_2 \in S_2 | (s_1, s_2) \in R\}$ and $R^{-1}(s_2) = \{s_1 \in S_1 | (s_1, s_2) \in R\}$; for $S_1' \subseteq S_1$, $R(S_1') = \bigcup_{s_1 \in S_1'} R(s_1)$ and similarly for $S_2' \subseteq S_2$, $R^{-1}(S_2') = \bigcup_{s_2 \in S_2'} R^{-1}(s_2)$. Given a set S and a relation $\preceq \subseteq S \times S$, $\preceq$ is a total preorder if and only if: (i) for all $s_1, s_2, s_3 \in S$, $s_1 \preceq s_2$ and $s_2 \preceq s_3$ implies $s_1 \preceq s_3$; (ii) for all $s_1, s_2 \in S$, $s_1 \preceq s_2$ or $s_2 \preceq s_1$. We can define the associated equivalence relation $\simeq$ and strict weak order $\prec$ given by $s_1 \simeq s_2$ if and only if $s_1 \preceq s_2$ and $s_2 \preceq s_1$; $s_1 \prec s_2$ if and only if $s_2 \not\preceq s_1$. 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 $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, where $\mathbb{R}^n$ is the state space; $P = \{1, \ldots, m\}$ is the finite set of modes; $\mathcal{P}$ is a subset of $\mathcal{S}(\mathbb{R}_0^+, P)$ which denotes the set of piecewise constant functions from $\mathbb{R}_0^+$ to P, continuous from the right and with a finite number of discontinuities on every bounded interval of $\mathbb{R}_0^+$; $F = \{f_1, \ldots, f_m\}$ is a collection of smooth vector fields indexed by P.*

A *switching signal* of Σ is a function $\mathbf{p} \in \mathcal{P}$, the discontinuities of $\mathbf{p}$ are called *switching times*. A continuous function $\mathbf{x} : \mathbb{R}_0^+ \to \mathbb{R}^n$ is said to be a *trajectory* of Σ if there exists a switching signal $\mathbf{p} \in \mathcal{P}$ such that, at each $t \in \mathbb{R}_0^+$ where the function $\mathbf{p}$ is continuous, $\mathbf{x}$ is continuously differentiable and satisfies:

$$\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)). \tag{1}$$

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 $\mathbf{p} \in \mathcal{P}$, there exists a unique trajectory of Σ, denoted $\mathbf{x}(., x, \mathbf{p})$ or by $\mathbf{x}(., x, p)$ if $\mathbf{p}$ is constantly 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. δ-GUAS [10]):

Definition 2.2: *A switched system Σ is incrementally globally uniformly asymptotically stable (δ-GUAS) if there exists a $\mathcal{KL}$ function β such that for all $t \in \mathbb{R}_0^+$, for all $x_1, x_2 \in \mathbb{R}^n$, for all switching signals $\mathbf{p} \in \mathcal{P}$, the following condition is satisfied:*

$$\|\mathbf{x}(t, x_1, \mathbf{p}) - \mathbf{x}(t, x_2, \mathbf{p})\| \leq \beta(\|x_1 - x_2\|, t).$$

Essentially, a switched system is incrementally stable if the distance between trajectories associated with the same switching signal converge asymptotically to zero independently of their initial condition. It implies global uniform asymptotic stability if and only if all vector fields share a common equilibrium (i.e. there exists $x \in \mathbb{R}^n$ such that for all $p \in P$, $f_p(x) = 0$).

As shown in [10], incremental stability of a switched system can be characterized using Lyapunov functions:

Definition 2.3: *A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ is a common δ-GUAS Lyapunov function for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x_1, x_2 \in \mathbb{R}^n$, and for all $p \in P$:*

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|); \tag{2}$$

$$\tfrac{\partial V}{\partial x_1}(x_1, x_2) f_p(x_1) + \tfrac{\partial V}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V(x_1, x_2). \tag{3}$$

Theorem 1: *[10] Consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ with a common δ-GUAS Lyapunov function, then Σ is δ-GUAS.*

The previous result establishes incremental stability for all sets of switching signal $\mathcal{P} \subseteq \mathcal{S}(\mathbb{R}_0^+, P)$. Sometimes, incremental stability only holds for a restricted set of switching signals, e.g. satisfying a minimum dwell-time assumption. $\mathbf{p} \in \mathcal{S}(\mathbb{R}_0^+, P)$ has *minimum dwell time* $\tau_d \in \mathbb{R}^+$ if the switching times t_1, $t_2, \ldots$ satisfy $t_1 \geq \tau_d$ and $t_i - t_{i-1} \geq \tau_d$, for all $i \geq 2$. Let $\mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$ denote the set of switching signals with minimum dwell time $\tau_d \in \mathbb{R}^+$. For such switching signals, incremental stability can be characterized using multiple Lyapunov functions:

Definition 2.4: *Smooth functions $V_p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$, $p \in P$ are multiple δ-GUAS Lyapunov functions for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$, $\kappa, \mu \in \mathbb{R}^+$ with $\mu \geq 1$ such that for all $x_1, x_2 \in \mathbb{R}^n$, for all $p, p' \in P$:*

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V_p(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|); \tag{4}$$

$$\tfrac{\partial V_p}{\partial x_1}(x_1, x_2) f_p(x_1) + \tfrac{\partial V_p}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V_p(x_1, x_2); \tag{5}$$

$$V_p(x_1, x_2) \leq \mu V_{p'}(x_1, x_2). \tag{6}$$

Theorem 2: *[10] Let $\tau_d \in \mathbb{R}^+$ and consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ with $\mathcal{P} \subseteq \mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$ and multiple δ-GUAS Lyapunov functions. If $\tau_d > \frac{\log \mu}{\kappa}$, then Σ is δ-GUAS.*

We would like to point out that in Definitions 2.3 and 2.4, V and V_p, $p \in P$ actually need to be differentiable only at $(x_1, x_2) \in \mathbb{R}^n \times \mathbb{R}^n$ with $x_1 \neq x_2$. Similarly, (3) and (5) need to hold only for $x_1 \neq x_2$. In the following sections, we will make the supplementary assumption on the δ-GUAS Lyapunov functions that there exists a $\mathcal{K}_\infty$ function γ such that for all $x_1, x_2, x_3 \in \mathbb{R}^n$

$$|V(x_1, x_2) - V(x_1, x_3)| \leq \gamma(\|x_2 - x_3\|); \tag{7}$$

$$|V_p(x_1, x_2) - V_p(x_1, x_3)| \leq \gamma(\|x_2 - x_3\|), \quad \forall p \in P; \tag{8}$$

for the case of common or multiple δ-GUAS Lyapunov functions, respectively. As shown in [10], this assumption is not restrictive provided we are interested in the dynamics of Σ on a bounded subset of $\mathbb{R}^n$, which is often the case in practice.

B. Approximate bisimulation

We present the notion of approximate equivalence which will relate a switched system to the symbolic models that we construct. We start by introducing transition systems, which allow us to describe switched systems and symbolic models in a common mathematical framework.

Definition 2.5: *A transition system is a tuple $T = (X, U, Y, \Delta, X^0)$ consisting of a set of states X; a set of inputs U; a set of outputs Y; a transition relation $\Delta \subseteq X \times U \times X \times Y$; a set of initial states $X^0 \subseteq X$. T is said to be metric if the set of*

outputs Y is equipped with a metric d, symbolic if X and U are finite or countable sets.

The transition $(x, u, x', y) \in \Delta$ will be denoted $(x', y) \in \Delta(x, u)$; this means that the system can evolve from state x to state x' under the input u, while producing output y. An input $u \in U$ belongs to the set of *enabled inputs* at state x, denoted enab(x), if $\Delta(x, u) \neq \emptyset$. If enab$(x) = \emptyset$, 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 $x \in X$ and $u \in$ enab(x), $\Delta(x, u)$ has only one element; in that case, we shall write with a slight abuse of notation $(x', y) = \Delta(x, u)$.

A *trajectory* of the transition system is a finite or infinite sequence of transitions $\sigma = (x^0, u^0, y^0)(x^1, u^1, y^1)(x^2, u^2, y^2)\dots$ where $(x^{i+1}, y^i) \in \Delta(x^i, u^i)$, for all $i \geq 0$. It is *initialized* if $x^0 \in X^0$, it is *maximal* if it is infinite or it is finite and ends in a blocking state. A state $x \in X$ is *reachable* if there exists an initialized trajectory reaching x. The transition system is said to be *non-blocking* if 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 $y^0 y^1 y^2 \dots$

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

Definition 2.6: *Let $T_i = (X_i, U, Y, \Delta_i, X_i^0)$, with $i = 1, 2$ be metric transition systems with the same sets of inputs U and outputs Y equipped with the metric d. Let $\varepsilon \in \mathbb{R}_0^+$, $R \subseteq X_1 \times X_2$ is said to be an ε-approximate bisimulation relation between T_1 and T_2 if for all $(x_1, x_2) \in R$, $u \in U$:*

$$\begin{aligned} &\forall (x_1', y_1) \in \Delta_1(x_1, u), \exists (x_2', y_2) \in \Delta_2(x_2, u), \\ &\qquad d(y_1, y_2) \leq \varepsilon \text{ and } (x_1', x_2') \in R; \end{aligned} \tag{9}$$

$$\begin{aligned} &\forall (x_2', y_2) \in \Delta_2(x_2, u), \exists (x_1', y_1) \in \Delta_1(x_1, u), \\ &\qquad d(y_1, y_2) \leq \varepsilon \text{ and } (x_1', x_2') \in R. \end{aligned} \tag{10}$$

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

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, $R \subseteq X_1 \times X_2$ is an ε-approximate bisimulation relation if and only if for all $(x_1, x_2) \in R$, enab(x_1) = enab(x_2) and for all $u \in$ enab(x_1),*

$$\begin{aligned} &d(y_1, y_2) \leq \varepsilon \text{ and } (x_1', x_2') \in R, \\ &\text{where } (x_1', y_1) = \Delta_1(x_1, u),\ (x_2', y_2) = \Delta_2(x_2, u). \end{aligned} \tag{11}$$

If T_1 and T_2 are ε-approximately bisimilar, it can be shown that the distance between output behaviors of T_1 and those of T_2 is bounded by ε:

Theorem 3: *[9] If $T_1 \sim_\varepsilon T_2$, then, for any initialized trajectory of T_1 (respectively T_2), $(x_1^0, u^0, y_1^0)(x_1^1, u^1, y_1^1)(x_1^2, u^2, y_1^2)\dots$, there exists an initialized trajectory of T_2 (respectively T_1) with the same sequence of inputs, $(x_2^0, u^0, y_2^0)(x_2^1, u^1, y_2^1)(x_2^2, u^2, y_2^2)\dots$, such that $d(y_1^i, y_2^i) \leq \varepsilon$, for all $i \geq 0$.*

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 $\tau \in \mathbb{R}^+$ and $\eta \in \mathbb{R}^+$, respectively. It has been established that the resulting symbolic models are ε-approximately bisimilar to incrementally stable switched systems where the precision $\varepsilon \in \mathbb{R}^+$ 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. As 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 $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system where $\mathcal{P} = \mathcal{S}(\mathbb{R}_0^+, P)$. 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

$$\Theta_\tau^N = \{\theta_s = 2^{-s}\tau \mid s = 0, \dots, N\} \tag{12}$$

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

The dynamics of the switched system Σ is then naturally described by the transition system $T_\tau^N(\Sigma) = (X, U, Y, \Delta, X^0)$ where

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

$$x' = \mathbf{x}(\theta_s, x, p) \text{ and } y = \mathbf{x}|_{\theta_s}(., x, p)$$

i.e. the switched system moves from state x to state x' by applying the constant mode p for a duration θ_s; y is the continuous-time trajectory of the switched system connecting x to x';

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

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

$$d(y,y') = \begin{cases} \|y - y'\| & \text{if } \theta_s = \theta_{s'} \\ +\infty & \text{if } \theta_s \neq \theta_{s'} \end{cases} \tag{13}$$

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

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

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

where $\eta \in \mathbb{R}^+$ is a state space sampling parameter. Let us remark that we have $X_\eta^0 \subseteq X_\eta^1 \subseteq \cdots \subseteq X_\eta^N$. We associate a multiscale quantizer $Q_\eta^s : \mathbb{R}^n \to [\mathbb{R}^n]_{2^{-s}\eta}$ such that $Q_\eta^s(x) = q$ 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 $s = 0,\ldots,N$, $\|x - Q_\eta^s(x)\| \leq 2^{-s}\eta$.

Then, let us define the transition system $T_{\tau,\eta}^N(\Sigma) = (X_\eta^N, U, Y, \Delta_\eta, X_\eta^0)$, where

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

$$q' = Q_\eta^s\left(\mathbf{x}(\theta_s,q,p)\right) \text{ and } y = \mathbf{x}|_{\theta_s}(.,q,p);$$

- the set of initial states is $X_\eta^0 = [\mathbb{R}^n]_\eta$.

$T_{\tau,\eta}^N(\Sigma)$ 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 $T_{\tau,\eta}^N(\Sigma)$ is a sequence of continuous functions $y^0y^1y^2\ldots$ It should be noted that the concatenation of these functions may not be a continuous function. Hence, the trajectories of Σ 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 θ_s end in states belonging to X_η^s. 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 τ, that is if $N = 0$, $T_{\tau,\eta}^N(\Sigma)$ 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_η^s, $s = 0,\ldots,N$ 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. ∘

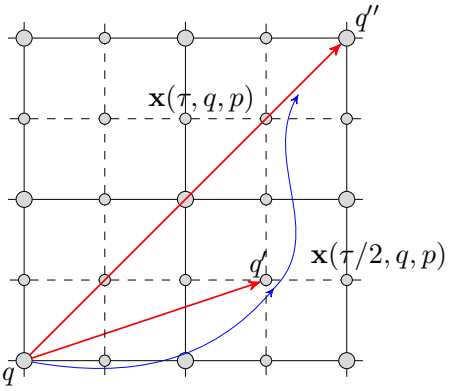

Fig. 1. Principle of the computation of the transition relation of multiscale symbolic models: $q' = \Delta_\eta(q,(p,\theta_1)) = Q_\eta^1(\mathbf{x}(\theta_1,q,p))$ and $q'' = \Delta_\eta(q,(p,\theta_0)) = Q_\eta^0(\mathbf{x}(\theta_0,q,p))$. The curves in blue represent the outputs associated with these transitions.

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 Σ admits a common δ-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 $\varepsilon \in \mathbb{R}^+$. If*

$$\eta \leq \min\left\{ \min_{s=0}^{s=N} \left[2^s \gamma^{-1}\left((1 - e^{-\kappa\theta_s})\underline{\alpha}(\varepsilon) \right) \right], \overline{\alpha}^{-1}\left(\underline{\alpha}(\varepsilon)\right) \right\} \tag{14}$$

then $T_\tau^N(\Sigma) \sim_\varepsilon T_{\tau,\eta}^N(\Sigma)$.

Proof: We start by showing that the relation R defined by

$$R = \left\{ (x,q) \in X \times X_\eta^N \mid V(x,q) \leq \underline{\alpha}(\varepsilon) \right\}$$

is an ε-approximate bisimulation relation between $T_\tau^N(\Sigma)$ and $T_{\tau,\eta}^N(\Sigma)$. 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 $u = (p,\theta_s) \in U$, $(x',y) = \Delta(x,u)$ and $(q',z) = \Delta_\eta(q,u)$. From (3), it holds for all $t \in [0,\theta_s]$,

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

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

$$\begin{aligned} \|y(t) - z(t)\| &= \|\mathbf{x}(t,x,p) - \mathbf{x}(t,q,p)\| \\ &\leq \underline{\alpha}^{-1}\left(V(\mathbf{x}(t,x,p),\mathbf{x}(t,q,p))\right) \leq \varepsilon. \end{aligned}$$

It follows that $d(y,z) \leq \varepsilon$. Since $q' = Q_\eta^s\left(\mathbf{x}(\theta_s,q,p)\right)$, equation (7) yields

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

Then, it holds

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

Then,

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

because of equation (14). Hence, $(x',q') \in R$ and R is an ε-approximate bisimulation relation between $T^N_\tau(\Sigma)$ and $T^N_{\tau,\eta}(\Sigma)$.

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

$$V(x,q) \leq \overline{\alpha}(\|x-q\|) \leq \overline{\alpha}(\eta) \leq \underline{\alpha}(\varepsilon)$$

because of equation (14). Hence, $X^0 \subseteq R^{-1}(X^0_\eta)$. Conversely, for all $q \in X^0_\eta$, $x = q \in X^0$ satisfies $V(x,q) = 0$. Hence, $X^0_\eta \subseteq R(X^0)$. Therefore, $T^N_\tau(\Sigma)$ and $T^N_{\tau,\eta}(\Sigma)$ are ε-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 multiscale 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 $\mathcal{P} = \mathcal{S}_{\tau_d}(\mathbb{R}^+_0, P)$. Let Θ^N_τ 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 $\tau_d = \theta_{N_d} = 2^{-N_d}\tau$. Then, let $\Theta^{N_d}_\tau$ be defined as in (12); we have $\Theta^{N_d}_\tau \subseteq \Theta^N_\tau$.

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

- the set of states is $X = \mathbb{R}^n \times P$, for $z = (x,p) \in X$, $x \in \mathbb{R}^n$ and $p \in P$ represent the state and the active mode of the switched system respectively;
- the set of inputs consists of pairs of mode and duration $U = P \times \Theta^N_\tau$;
- the set of outputs is the set of continuous functions $Y = \bigcup_{s=0}^{s=N} \mathcal{C}([0,\theta_s], \mathbb{R}^n)$;
- the transition relation is given for $z = (x,p) \in X$ and $u = (p',\theta_s) \in \text{enab}(z)$ by $(z',y) = \Delta(x,u)$ if and only if

  $$z' = (x',p') \text{ and } x' = \mathbf{x}(\theta_s, x, p') \text{ and } y = \mathbf{x}|_{\theta_s}(.,x,p').$$

  The set of enabled inputs is $\text{enab}(z) = \{p\} \times \Theta^N_\tau \cup (P \setminus \{p\}) \times \Theta^{N_d}_\tau$, i.e. if the current mode is p and a mode $p' \neq p$ is applied, it needs to be held for a period of at least $\theta_{N_d} = \tau_d$;
- the set of initial states is $X^0 = \mathbb{R}^n \times P$.

$T^N_\tau(\Sigma_{\tau_d})$ is deterministic and metric when the set of outputs Y is equipped with the metric given by (13). Note that the state space of $T^N_\tau(\Sigma_{\tau_d})$ is uncountable.

The construction of the approximating symbolic model follows the same line as before and is given by the transition system $T^N_{\tau,\eta}(\Sigma_{\tau_d}) = (X^N_\eta, U, Y, \Delta_\eta, X^0_\eta)$, where

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

  $$r' = (q',p') \text{ and } q' = Q^s_\eta\left(\mathbf{x}(\theta_s, q, p')\right) \text{ and } y = \mathbf{x}|_{\theta_s}(.,q,p').$$

  The set of enabled inputs is $\text{enab}(r) = \{p\} \times \Theta^N_\tau \cup (P \setminus \{p\}) \times \Theta^{N_d}_\tau$;
- the set of initial states is $X^0_\eta = [\mathbb{R}^n]_\eta \times P$.

$T^N_{\tau,\eta}(\Sigma_{\tau_d})$ 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 us assume that the switched system Σ_{τ_d} admits multiple δ-GUAS Lyapunov functions V_p, $p \in P$, 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 $\tau_d > \frac{\log \mu}{\kappa}$ and*

$$\eta \leq \min\left\{ \min_{s=0}^{s=N_d}\left[2^s\gamma^{-1}\left(\left(\frac{1}{\mu} - e^{-\kappa\theta_s}\right)\underline{\alpha}(\varepsilon)\right)\right], \min_{s=0}^{s=N}\left[2^s\gamma^{-1}\left(\frac{1-e^{-\kappa\theta_s}}{\mu}\underline{\alpha}(\varepsilon)\right)\right], \overline{\alpha}^{-1}\left(\frac{1}{\mu}\underline{\alpha}(\varepsilon)\right)\right\} \tag{15}$$

then $T^N_\tau(\Sigma_{\tau_d}) \sim_\varepsilon T^N_{\tau,\eta}(\Sigma_{\tau_d})$.

Proof: We start by showing that the relation R defined by

$$R = \left\{ (z,r) \in X \times X^N_\eta \;\middle|\; \begin{array}{c} z = (x,p),\ r = (q,p) \\ V_p(x,q) \leq \frac{1}{\mu}\underline{\alpha}(\varepsilon) \end{array} \right\}$$

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

$$\begin{array}{rcl} V_p(\mathbf{x}(t,x,p), \mathbf{x}(t,q,p)) & \leq & e^{-\kappa t}V_p(x,q) \leq V_p(x,q) \\ & \leq & \frac{1}{\mu}\underline{\alpha}(\varepsilon) \leq \underline{\alpha}(\varepsilon). \end{array}$$

Then, (4) gives for all $t \in [0,\theta_s]$,

$$\begin{array}{rcl} \|y(t) - z(t)\| & = & \|\mathbf{x}(t,x,p) - \mathbf{x}(t,q,p)\| \\ & \leq & \underline{\alpha}^{-1}\left(V_p(\mathbf{x}(t,x,p), \mathbf{x}(t,q,p))\right) \leq \varepsilon. \end{array}$$

It follows that $d(y,z) \leq \varepsilon$. Also, similar to the proof of Theorem 4, we can show that

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

Then, (15) yields

$$V_p(x',q') \leq e^{-\kappa\theta_s}\frac{1}{\mu}\underline{\alpha}(\varepsilon) + \gamma(2^{-s}\eta) \leq \frac{1}{\mu}\underline{\alpha}(\varepsilon)$$

and $(z',r') \in R$. If $p' \neq p$, then $\theta_s \in \Theta^{N_d}_\tau$ and from (5) and (6), it holds for all $t \in [0,\theta_s]$,

$$\begin{array}{rcl} V_{p'}(\mathbf{x}(t,x,p'), \mathbf{x}(t,q,p')) & \leq & e^{-\kappa t}V_{p'}(x,q) \leq e^{-\kappa t}\mu V_p(x,q) \\ & \leq & \mu V_p(x,q) \leq \underline{\alpha}(\varepsilon). \end{array}$$

Then, we can show as above that $d(y,z) \leq \varepsilon$. Also, similar to the proof of Theorem 4, we can show that

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

Then, from (6) and (15)

$$\begin{array}{rcl} V_{p'}(x',q') & \leq & e^{-\kappa\theta_s}\mu V_p(x,q) + \gamma(2^{-s}\eta) \\ & \leq & e^{-\kappa\theta_s}\underline{\alpha}(\varepsilon) + \gamma(2^{-s}\eta) \leq \frac{1}{\mu}\underline{\alpha}(\varepsilon). \end{array}$$

Therefore, $(z',r') \in R$ and R is an ε-approximate bisimulation relation between $T^N_\tau(\Sigma_{\tau_d})$ and $T^N_{\tau,\eta}(\Sigma_{\tau_d})$. ∎

Let us point out that the dwell-time condition $\tau_d > \frac{\log \mu}{\kappa}$ guarantees that for all $s = 0,\ldots,N_d$, $e^{-\kappa\theta_s} \leq \frac{1}{\mu}$. Then, it follows 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 (15) holds. Thus, approximately bisimilar

multiscale symbolic models of arbitrary precision can be computed for $T_\tau^N(\Sigma_{\tau_d})$.

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 $y \in \mathcal{C}([0, \theta_y], \mathbb{R}^n)$ 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 $S = (Q, E, I, G, Q^0)$ 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 succesive transitions: there exists $\epsilon > 0$ such that, for all $e = (q, q'), e' = (q', q'') \in E$,*

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

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 $S = (Q, E, I, G, Q^0)$ is the transition system $T||S = (X_S, U_S, Y, \Delta_S, X_S^0)$ 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 $X_S^0 = Q^0 \times X^0$; 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 $u \in$ 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 $0 = t_0 \leq t_1 \leq \cdots \leq t_N \leq t_{N+1} = \theta_y$ and $e_i = (q_i, q_{i+1}) \in E$, $i = 0, \ldots, N-1$ 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 $u \in$ enab(x), but none of the previous conditions hold with $(x', y) = \Delta(x, u)$ and $q' = q''$, or if $u \notin$ 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 [4]) can be written under the form of a safety specification automaton. ∘

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

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

Proof: The fact that $T||S$ 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 $T||S$ 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 $T||S$, $\sigma_S = (z^0, v^0, y^0), (z^1, v^1, y^1), (z^2, v^2, y^2) \ldots$ with $z^i = (q^i, x^i)$, $v^i = (q'^i, u^i)$, for all $i \geq 0$. A safety controller is then a controller that prevents $T||S$ from reaching a blocking state.

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

- *$C(z) \subseteq$ 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 dom$(C) = \{z \in X_S |\ C(z) \neq \emptyset\}$. The controlled system is given by the transition system $T||S/C = (X_S, U_S, Y, \Delta_{S/C}, X_{S/C}^0)$ where the transition relation is given for $z \in X_S$, $v \in U_S$ by $(z', y) \in \Delta_{S/C}(z, v)$ if and only if $v \in C(z)$ and $(z', y) = \Delta_S(z, v)$; the set of initial states is $X_{S/C}^0 = X_S^0 \cap$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 $X_{S/C}^0$, all inital 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 $T||S$ 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 $z \in dom(C^*)$. The set of safety controllable states is denoted $cont(T||S)$.*

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 $z \in X_S$:

$$C^*(z) = \left\{ v \in \text{enab}(z) \;\middle|\; \begin{array}{c} z' \in \text{cont}(T||S) \\ \text{with } (z', y) = \Delta_S(z, v) \end{array} \right\}. \quad (16)$$

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 $I = \{I_q = I_S\}$, $G = \emptyset$, 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 $\preceq \subseteq U \times U$.*

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

We lift the preorder $\preceq \subseteq U \times U$ 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 $\simeq$ and strict weak order $\prec$ are lifted similarly. Since U_S is finite, we can define for any subset $V \subseteq U_S$,

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

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

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

- *all safety controllable initial states are in dom(C):*

$$X_S^0 \cap cont(T||S) \subseteq dom(C);$$

- *all states $z \in dom(C)$ are reachable in $T||S/C$;*
- *for all states $z \in dom(C)$:*
  1) *if $v \in C(z)$, then for all $v' \in enab(z)$ with $v \simeq v'$, $(z', y) = \Delta_S(z, v')$, it holds that $v' \in C(z)$ if and only if $z' \in cont(T||S)$;*
  2) *if $v \in C(z)$, then for all $v' \in enab(z)$ with $v \prec v'$, $(z', y) = \Delta_S(z, v')$, it holds that $z' \notin cont(T||S)$.*

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

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

Now let C be the controller defined from $\bar{C}^*$ by $C(z) = \bar{C}^*(z)$ if z is reachable in $T||S/\bar{C}^*$ and $C(z) = \emptyset$ otherwise. It is clear that the reachable states in $T||S/\bar{C}^*$ 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 $\bar{C}^*$ that C is a safety controller for $T||S$, and that C satisfies conditions (1) and (2) of Definition 4.12. Let $z \in X_S^0 \cap \text{cont}(T||S) = X_S^0 \cap \text{dom}(\bar{C}^*) = X^0_{S/\bar{C}^*}$. Since any initial state is reachable, z is reachable in $T||S/\bar{C}^*$. Therefore, we have $C(z) = \bar{C}^*(z) \neq \emptyset$ 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 $v_1 \notin C_2(z)$. 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 $\Delta_S(z, v_2) \in \text{dom}(C_2) \subseteq \text{cont}(T||S)$. 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 $v_1 \simeq v_2$, 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 $C_1(z) \neq \emptyset$ and $C_2(z) = \emptyset$. $z \in \text{dom}(C_1) \subseteq \text{cont}(T||S)$ therefore z cannot be in X_S^0 otherwise we would have $C_2(z) \neq \emptyset$. 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 $z^N = z$.

Algorithm 1: MLS controller synthesis

Input: Transition system $T||S = (X_S, U_S, Y, \Delta_S, X_S^0)$, priority relation $\preceq \subseteq U_S \times U_S$
Output: MLS controller $C \subseteq X_S \times U_S$
1 **Global variables:** controllable states $X_c \subseteq X_S$, uncontrollable states $X_u \subseteq X_S$
2 **begin**
3 $(X_c, X_u, C) := (\emptyset, \emptyset, \emptyset)$;
4 **for** $z \in X_S^0$ **do**
5 explore $(z, \emptyset)$;
6 **return** C

$z^0 \in \text{dom}(C_1)$ is a controllable initial states and therefore $C_2(z^0) \neq \emptyset$. Then, there exists $i \in \{0, \ldots, N-1\}$ such that $C_2(z^i) \neq \emptyset$ and $v_i \notin C_2(z^i)$ (otherwise we would have $C_2(z) \neq \emptyset$). Therefore, there exists $z^i \in X_S$, such that $C_1(z^i) \neq C_2(z^i)$ and both $C_1(z^i)$ and $C_2(z^i)$ are not empty. We have already proved that in this case one of the controllers is not a MLS controller. ■

In the proof of Theorem 6, we give a construction of the MLS controller. Intuitively, the MLS controller for $T||S$ can be obtained from the maximal safety controller by selecting the enabled inputs of higher priority and by removing the states that are not reachable. Of course, this construction does not lead to an efficient algorithm for the computation of the MLS since it needs first to compute the maximal safety controller. In the following section, we address the problem of computing effectively the MLS controller.

C. 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 $explore(z, \emptyset)$ on each initial state $z \in X_S^0$; the second argument X_v of the function $explore$ is the set of states already visited by the current trajectory. The global variables are X_c, X_u, and C for the sets of controllable and uncontrollable states and the controller, respectively. Function $explore(z, X_v)$ 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 X_v contains, at each call to $explore$, the set of states visited along one path from some initial state z^0 in X_S^0 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 X_v are added recursively to the set of controllable states X_c;
- has already been visited along the current path X_v (i.e. $z \in X_v$) (line 8) — hence, lying on a cyclic path of safe states, in that case all states in X_v (including z) are added recursively to the set of controllable states X_c.

In contrast, z is determined controllable if all its successors are uncontrollable (line 22), in that case z is added to the set of uncontrollable states X_u. Hence, X_c and X_u contains all the controllable and uncontrollable states that have been explored, respectively. Let us also remark that $C(z) \neq \emptyset$ if and only if $z \in X_c$.

Algorithm 2: explore(z, X_v)

Input: state $z \in X_S$, visited states $X_v \subseteq X_S$
Output: *true* if and only if z is safety controllable
1 **Local variables:** unexplored inputs $V_u \subseteq U_S$
2 **begin**
3 **if** $z \in X_u$ **then**
4 **return** *false*
5 **if** $z \in X_c$ **then**
6 **return** *true*
7 **if** $z \in X_v$ **then**
8 **return** *true*
9 $V_u := \text{enab}(z)$;
10 **while** $V_u \neq \emptyset$ **do**
11 foundSucc := *false*;
12 **for** $v \in \max_{\preceq}(V_u)$ **do**
13 $(z', y) := \Delta_S(z, v)$;
14 **if** *explore* $(z', X_v \cup \{z\})$ **then**
15 $C := C \cup \{(z, v)\}$;
16 foundSucc := *true*;
17 **if** foundSucc **then**
18 $X_c := X_c \cup \{z\}$;
19 **return** *true*
20 $V_u := V_u \setminus \max_{\preceq}(V_u)$;
21 $X_u := X_u \cup \{z\}$;
22 **return** *false*

Let us verify that C is a safety controller. By construction (line 9), we have $C(z) \subseteq \text{enab}(z)$. Then, assume $C(z) \neq \emptyset$, and let $v \in C(z)$, $(z', y) = \Delta_S(z, v)$, then it holds that z' is controllable (line 14). Thus $z' \in X_c$ and $C(z') \neq \emptyset$.

We now prove that C is the MLS controller. In Algorithm 1, the function $explore$ is called for all initial states in X_S^0. Then, it follows that all controllable initial states are in X_S^0, the first point of Definition 4.12 holds. Since Algorithm 1 explores trajectories starting from initial states, all states in $\text{dom}(C) = X_c$ are reachable in $T||S/C$, the second point of Definition 4.12 holds. As for the third point, let $z \in \text{dom}(C)$ and $v \in C(z)$. The outer loop of the function $explore$ (lines 10 to 20) explores trajectories using inputs of higher priority first. Hence, if $v \in C(z)$ then all inputs $v' \in \text{enab}(z)$ with $v \prec v'$ 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 $v \in C(z)$ then all inputs $v' \in \text{enab}(z)$ with $v \simeq v'$ have been explored and $v' \in C(z)$ 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 U_S, 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 $|X'_S| \times |U_S|$ where X'_S 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 $\dot{\mathbf{x}}(t) = A_{\mathbf{p}(t)}\mathbf{x}(t) + b$ for $\mathbf{p}(t) \in \{1, 2\}$ (see [10] for numerical values). It can be shown that it has a common δ-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 $T^0_{\tau_1,\eta_1}(\Sigma)$ 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 $T^6_{\tau_2,\eta_2}(\Sigma)$ for parameters $\tau_2 = 64\tau_1$ and $\eta_2 = 64\eta_1$ (containing transitions of durations in $\Theta^6_\tau = \{32, 16, 8, 4, 2, 1, 0.5\}$). The set of states of $T^6_{\tau_2,\eta_2}(\Sigma)$ consists of a set of 7 embedded lattices whose finest one coincides with the set of states of $T^0_{\tau_1,\eta_1}(\Sigma)$. 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 $T^0_{\tau_1,\eta_1}(\Sigma)$ and $T^6_{\tau_2,\eta_2}(\Sigma)$. 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 $T^0_{\tau_1,\eta_1}(\Sigma)$ and $T^6_{\tau_2,\eta_2}(\Sigma)$). 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 $T^0_{\tau_1,\eta_1}(\Sigma)$ and $T^6_{\tau_2,\eta_2}(\Sigma)$). 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 $|\text{dom}(C) \cap X^0_S|/|X^0_S \cap I_S|$) comparable to that of their its uniform counterparts. Figure 2 depicts the maximal lazy safety controller for $T^6_{\tau_2,\eta_2}(\Sigma)$ and a trajectory of the controlled switched system.

	Uniform symbolic model $N = 0$, $\tau = 0.5$ $\eta = 0.0003$, $\varepsilon = 0.05$	Multiscale symbolic model $N = 6$, $\tau = 32$ $\eta = 0.018$, $\varepsilon = 0.05$
Time	9.2s	0.6s
Size (10^3)	936	6
Durations	0.5 (100%)	4 (33%) 2 (9%) 1 (50% 0.5 (8%)
Cont. Ratio	93%	92%

TABLE I
Experimental results for the MLS controller synthesis for the boost DC-DC converter

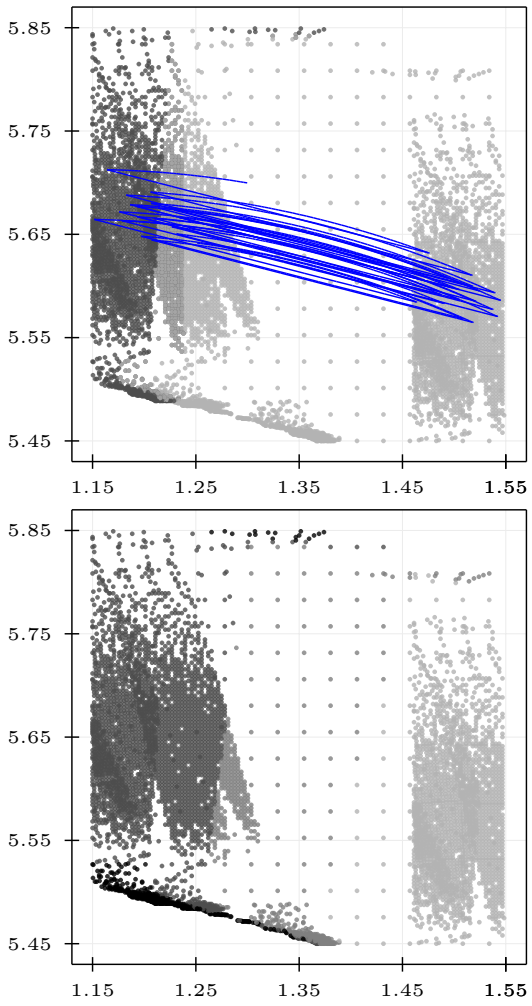

Fig. 2. The MLS controller for $T^6_{\tau_2,\eta_2}(\Sigma)$ and I_S. Top: mode 1 is enabled (light gray); mode 2 is enabled (dark gray); modes 1 and 2 are enabled (medium gray); and a trajectory. Bottom: duration 4 (light gray), 2 (medium gray), 1 (dark gray), 0.5 (black) are enabled.

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 $\mathbf{T}_i(t)$ of the room i, $1 \leq i \leq n$, is defined by the differential equation

$$\begin{aligned}\dot{\mathbf{T}}_i(t) \quad = \quad & \alpha(\mathbf{T}_{i+1}(t) + \mathbf{T}_{i-1}(t) - 2\mathbf{T}_i(t)) \\ & +\beta(t_e - \mathbf{T}_i(t)) + \gamma(t_h - \mathbf{T}_i(t))\mathbf{u}_i(t)\end{aligned}$$

where $\mathbf{T}_{i-1}(t)$ is the temperature of the room $i-1$; $\mathbf{T}_{i+1}(t)$ the temperature of the room $i+1$ (with the convention that $\mathbf{T}_0(t) = \mathbf{T}_n(t)$ and $\mathbf{T}_{n+1}(t) = \mathbf{T}_1(t)$); t_e is the temperature of the external environment of the building; t_h is the temperature of the heater; α is the conduction factor between the rooms $i \pm 1$ and the room i; β is the conduction factor between the external environment and the room i; γ is the conduction factor between the heater and the room i; $\mathbf{u}_i(t)$ 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 α, β, γ, t_e, and t_h are respectively

	Multiscale symbolic models $N = 4$, $\tau = 80$, $\eta = 0.28$, $\varepsilon = 0.4$		
	$n = 3$	$n = 4$	$n = 5$
Time	0.2s	6s	312s
Size (10^3)	2	45	1 077
Durations	40 (1%) 20 (37%) 10 (62%)	20 (25%) 10 (73%) 5 (2%)	20 (6%) 10 (92%) 5 (2%)
Cont. Ratio	99.99%	99.89%	99.79%

TABLE II

EXPERIMENTAL RESULTS FOR THE SYNTHESIS OF THE MLS CONTROLLER FOR TEMPERATURE REGULATION IN A BUILDING OF THREE, FOUR, AND FIVE ROOMS.

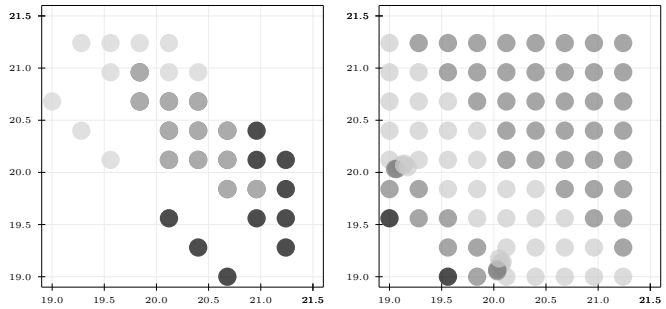

Fig. 3. Partial view of the MLS controller for $T^4_{\tau,\eta}(\Sigma)$ and I_S for the 4 room building in the plane (T_1, T_2) with $T_3 = T_4 = 19$. Left: mode 1 is enabled (light gray); mode 2 is enabled (black); modes 1 and 2 are enabled (gray); other modes are not displayed. Right: duration 20 (light gray), 10 (gray), 5 (black) are enabled.

1/20, 1/200, 1/100, 10, and 50. The resulting switched system has a common δ-GUAS Lyapunov function and thus approximately bisimilar symbolic models exist.

We increase the system dimension to test the limits of the tool in terms of memory usage and computation time. Given the safety specification $I_S = [19.0, 21.5]^n$ for $n \in \{3, 4, 5\}$, we synthesize safety controllers for buildings of three, four, and five rooms. The values of N, τ, η and ε are given in Table II. By looking at the results, we can see multiscale symbolic models do not prevent the combinatorial explosion of the complexity when increasing the system dimension from 3 to 5. They allow us, however, to handle dimensions that are out of reach using uniform symbolic models. Figure 3 gives a partial view of the MLS controller for the transition system $T^4_{\tau,\eta}(\Sigma)$ for the 4 room building.

C. Switched system with dwell-time

The third case study is taken from [10] and illustrates the case of switched systems without a common δ-GUAS Lyapunov function. The system has two modes and the state space is $\mathbb{R}^2$. The dynamics associated with both modes are affine of the form $\dot{\mathbf{x}}(t) = A_{\mathbf{p}(t)}\mathbf{x}(t) + b_{\mathbf{p}(t)}$ for $\mathbf{p}(t) \in \{1, 2\}$ with

$$A_1 = \begin{bmatrix} -0.25 & 1 \\ -2 & -0.25 \end{bmatrix}, \; A_2 = \begin{bmatrix} -0.25 & 2 \\ -1 & -0.25 \end{bmatrix},$$

$b_1 = \begin{bmatrix} -0.25 & -2 \end{bmatrix}^\top$, $b_2 = \begin{bmatrix} 0.25 & 1 \end{bmatrix}^\top$. The system does not have a common δ-GUAS Lyapunov function but admits multiple δ-GUAS Lyapunov functions (see [10] for details). Then, restricting the set of switching signals to those having dwell time $\tau_d = 2$, the switched system is incrementally stable and admits approximately bisimilar uniform and multiscale symbolic models. We consider the same safety specification as in [10] which consists in keeping the state in $I_S = [-6, 6] \times [-4, 4]$ while avoiding $I_U = [-1.5, 1.5] \times [-1, 1]$.

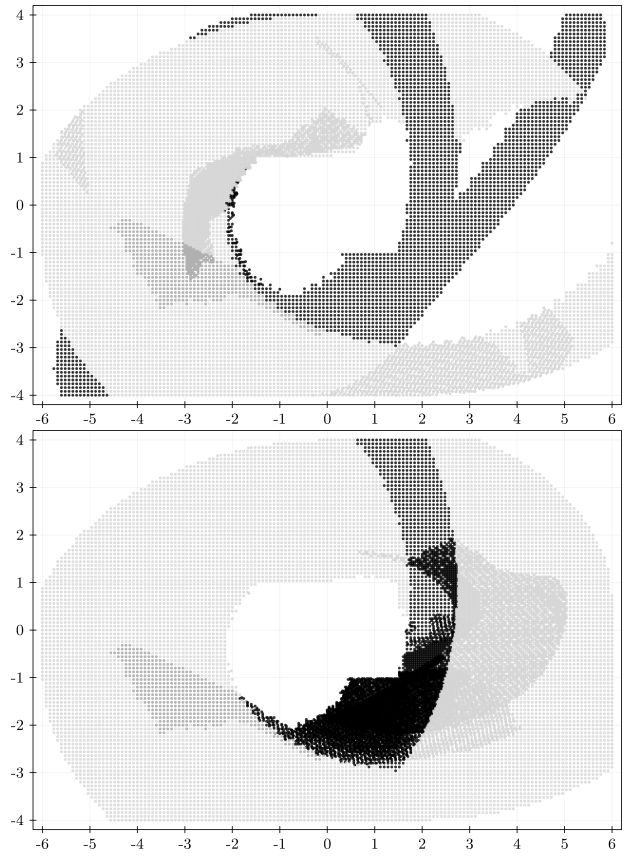

Fig. 4. Mode map of the MLS controller for $T^3_{\tau_2,\eta_2}(\Sigma_{\tau_d})$ and $I_S \setminus I_U$ for a switched system with dwell-time. Top: mode 1 is active. Bottom: mode 2 is active. Mode 1 is enabled (black), mode 2 is enabled (light gray), modes 1 and 2 are enabled (gray).

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 $T^3_{\tau_2,\eta_2}(\Sigma_{\tau_d})$ for parameters $\tau_2 = 8\tau_1$, $\eta_2 = 8\eta_1$ (containing transitions of durations in $\Theta^3_{\tau_2} = \{4, 2, 1, 0.5\}$). The set of states of $T^3_{\tau_2,\eta_2}(\Sigma_{\tau_d})$ 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

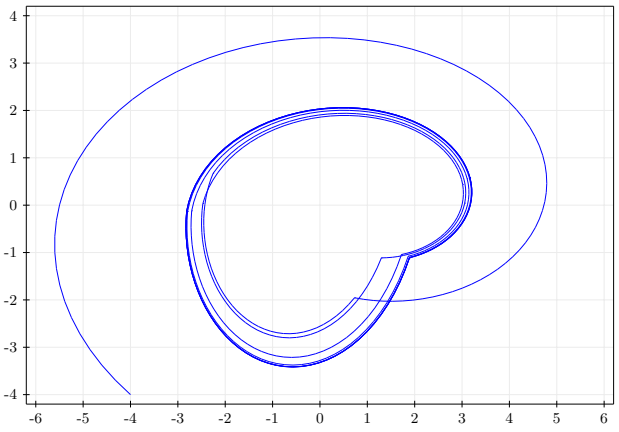

Fig. 5. Trajectory of the switched system with dwell-time controlled using the MLS controller shown in Figure 4.

that they are approximately bisimilar to the original switched systems under the existence of (common or multiple) δ-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

[1] D. Angeli and E.D. Sontag. Forward completeness, unboundedness observability, and their Lyapunov characterizations. *Systems and Control Letters*, 38(3):209–217, 1999.

[2] A. Anta and P. Tabuada. To sample or not to sample: self-triggered control for nonlinear systems. *IEEE Transactions on Automatic Control*, 55(9):2030–2042, 2010.

[3] E. Asarin, O. Bournez, T. Dang, O. Maler, and A. Pnueli. Effective synthesis of switching controllers for linear systems. *Proceedings of the IEEE*, 88(7):1011–1025, 2000.

[4] C. Baier and J.-P. Katoen. *Principles of model checking*, volume 26202649. MIT press Cambridge, 2008.

[5] A. Borri, G. Pola, and M.D. Di Benedetto. A symbolic approach to the design of nonlinear networked control systems. In *Hybrid Systems: Computation and Control*, pages 255–264, 2012.

[6] J. Cámara, A. Girard, and G. Gössler. Safety controller synthesis for switched systems using multi-scale symbolic models. In *IEEE Conference on Decision and Control and European Control Conference*, pages 520–525, Orlando, USA, 2011.

[7] J. Cámara, A. Girard, and G. Gössler. Synthesis of switching controllers using approximately bisimilar multiscale abstractions. In *Hybrid Systems: Computation and Control*, pages 191–200, 2011.

[8] C. Cassandras and S. Lafortune. *Introduction to discrete event systems*. Springer, second edition, 2007.

[9] A. Girard and G.J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, 2007.

[10] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, 2010.

[11] J. Lygeros, K.H. Johansson, S.N. Simic, J. Zhang, and S.S. Sastry. Dynamical properties of hybrid automata. *IEEE Transactions on Automatic Control*, 48(1):2–17, 2003.

[12] S. Mouelhi, A. Girard, and G. Gössler. CoSyMA: a tool for controller synthesis using multi-scale abstractions. In *Hybrid Systems: Computation and Control*, pages 83–88, 2013.

[13] G. Pola, A. Borri, and M.D. Di Benedetto. Integrated design of symbolic controllers for nonlinear systems. *IEEE Transactions on Automatic Control*, 57(2):534–539, 2012.

[14] G. Pola, A. Girard, and P. Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, 2008.

[15] G. Pola, P. Pepe, M.D. Di Benedetto, and P. Tabuada. Symbolic models for nonlinear time-delay systems using approximate bisimulations. *Systems and Control Letters*, 59(6):365–373, 2010.

[16] G. Pola and P. Tabuada. Symbolic models for nonlinear control systems: alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2):719–733, 2009.

[17] P.J. Ramadge and W.M. Wonham. Supervisory control of a class of discrete event processes. *SIAM Journal on Control and Optimization*, 25(1):206–230, 1987.

[18] P. Tabuada. *Verification and control of hybrid systems - a symbolic approach*. Springer, 2009.

[19] Y. Tazaki and J.I. Imura. Discrete-state abstractions of nonlinear systems using multi-resolution quantizer. In *Hybrid Systems: Computation and Control*, volume 5469 of *LNCS*, pages 351–365. Springer, 2009.

[20] Y. Tazaki and J.I. Imura. Discrete abstractions of nonlinear systems based on error propagation analysis. *IEEE Transactions on Automatic Control*, 57(3):550–564, 2012.

[21] M. Velasco, J. Fuertes, and P. Marti. The self triggered task model for real-time control systems. In *24th IEEE Real-Time Systems Symposium*, pages 67–70, 2003.

[22] M. Zamani and A. Abate. Symbolic control of stochastic switched systems via finite abstractions. In *Quantitative Evaluation of Systems*, volume 8054 of *LNCS*, pages 305–321, 2013.

[23] J. Zhang, K.H. Johansson, J. Lygeros, and S. Sastry. Zeno hybrid systems. *International Journal of Robust and Nonlinear Control*, 11(5):435–451, 2001.

PLACE PHOTO HERE

Antoine Girard received the Diplôme d'Ingénieur from the Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble, the M.S. degree in applied mathematics from the Université Joseph Fourier, Grenoble, France, both in 2001 and the Ph.D. degree in applied mathematics from the Institut National Polytechnique de Grenoble, France, in September 2004. From October 2004 to December 2005, he was a postdoctoral researcher at the Department of Electrical and Systems Engineering of the University of Pennsylvania, Philadelphia and from January to August 2006, he was a postdoctoral researcher at the Verimag laboratory, Grenoble, France. Since September 2006, he has been an Associate Professor at the Université Joseph Fourier, Grenoble, France.

His research interests deal with analysis and control of hybrid systems with an emphasis on computational approaches, approximation, abstraction and applications to cyber-physical systems. He is also interested in multi-agent and distributed parameter systems.

Antoine Girard received the George S. Axelby Outstanding Paper Award from the IEEE Control Systems Society in 2009 and the Bronze Medal of CNRS in 2014. In 2015, he was a co-chair of the International Conference on Hybrid Systems: Computation and Control (HSCC'15). He is also serving on the editorial board of the IEEE Transactions on Automatic Control and Nonlinear Analysis: Hybrid Systems.

PLACE PHOTO HERE

Gregor Gössler received his engineering diploma (Dipl.-Inform.) in computer science from Karlsruhe University, the Diplôme d'Ingénieur from the Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble, and the M.S. degree in computer science from Grenoble University, France, all in 1998, and the Ph.D. degree in computer science from Grenoble University in 2001. In 2001/2002 he was a postdoctoral researcher at the EECS department of the University of California at Berkeley, before joining INRIA, France in 2002.

His main research interests are in the fields of formal methods for embedded and safety-critical systems, component-based design, and techniques ensuring correctness by construction.

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.