A Quantitative Approach on Assume-Guarantee Contracts for Safety of Interconnected Systems*

Alina Eqtami, Antoine Girard

A Quantitative Approach on Assume-Guarantee Contracts for Safety of Interconnected Systems*

Alina Eqtami[1] and Antoine Girard[1]

***Abstract*— In this paper, the safety synthesis problem for a discrete-time system comprised by multiple interconnected systems is considered. Using compositional reasoning, a quantitative framework is applied to each of the subsystems. With this framework it has been possible to derive robust controlled invariant subsets for each of the subsystems with respect to the control invariant subsets of the other subsystems. These invariant subsets can be computed from a parameterized family of sets and they share a common safety controller. Contract-based design is utilized to built assume-guarantee contracts for all the subsystems, namely to assume that the other subsystems belong to their invariant sets and guarantee that the subsystem will belong to its invariant set. This circularity of the implications can be resolved by a fixed point algorithm which computes the parameters to guarantee that all the subsystems fulfill their contracts simultaneously. Then, the invariant set and the safety controller are given for the original system. To illustrate the effectiveness of the proposed approach, an application for the temperature regulation of adjacent rooms of a building is given as an example.**

I. INTRODUCTION

The concept of safety synthesis refers to the ability of the controller to maintain the state of the system in a specified set of safe states, [1]. Controlled invariant sets, have been widely used in the control literature for the solution to the safety problem, [2], [3], [4]. Based on this classical approach, the states of the system are qualitatively partitioned to either being safety-controllable or safety-uncontrollable. This depends, the former on that they belong to the maximal controlled-invariant subset of the safe set and the latter, that they don't. Therefore, this classic approach does not allow to compare states within the same category even though, intuitively, some states can be considered safer than others (i.e. those that are further from the unsafe set). It can then be anticipated that a quantitative approach that measures safety associated to the states of the system can be formulated.

In our previous work [5], a quantitative approach to safety control based on a functional fixed-point iteration was presented. This approach made it possible to compute a measure of safety which quantifies how far from the unsafe set (respectively, how close to the safe set) one can stay, starting from a given controllable (respectively, uncontrollable) state. Furthermore, it was shown that the level sets of the fixed-point coincide with the maximal controlled invariant subsets of a parameterized family of sets and that one can synthesize a common safety controller for all the sets of the family. Other works using quantitative semantics of qualitative specifications formulated in temporal logic, have appeared in [6], [7], while others are using model predictive control as in [8], [9].

Verifying invariance properties in a centralized manner is limited to systems with moderate size. The full set of states for larger systems is usually too big to design a controller. For this reason, flourishing ongoing research has emerged the recent years upon investigating decentralized approaches for invariance on larger dynamical systems. A line of research is focusing on investigating numerical methods to compute compositionally invariants [10], [11], [12], [13], while others are using formal methods and symbolic techniques [14], [15].

Another decentralized approach is contract-based design which can be used to verify the invariance properties of complex systems consisting of interconnected subsystems. This approach can establish correct behavior of the composed system, provided each subsystem satisfies its safety specification (guarantee) while assuming that the others satisfy theirs (assumption). Therefore, assume-guarantee contracts are assigned to all subsystems and if they all satisfy their own contract it is possible to reason for the global invariance property of the original system, [16], [17]. Assume-guarantee contracts for compositional reasoning have been previously used by means of small-gain theorems [18], [19]. The assume-guarantee framework is always sound whenever there is no circularity of implications. If there is circularity, then the problem is usually resolved assuming that at least one subsystem satisfies a contract independently of the others. In the present work the circularity on the implications exists, but we do not need to make any such (hard) assumptions on the subsystems' contracts.

In the current work, we consider the safety problem for a complex finite system comprised by multiple interconnected subsystems. The controller synthesis is not performed on the full state space whereas the contract-based framework is used to establish safety on the respective subsystems. We are using a quantitative approach for the design of the controllers of the subsystems, similar to our previous work [5]. This approach provides characterization of the controlled invariant subsets of a parameterized family of sets. Compositional reasoning is then used to define the safety on the complex system. It's thereon apparent that there exists circularity on assume-guarantee contracts of the subsystems, which makes

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

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

the problem hard to solve. However, using the proposed quantitative approach, this problem is circumvented since it is possible to compute the specific parameters, on the parameterized safe sets, that guarantee the fulfillment of all contracts simultaneously.

The structure of this paper is as follows. In Section II, we introduce the class of transition systems considered through the paper. Section III is devoted on the safety objectives for interconnected systems, as well as introducing the concept of assume-guarantee contracts as a compositional method. In Section IV, first, we provide a brief overview of the proposed quantitative approach introduced in [5] accordingly modified for the decentralized framework and then the main results of the paper are presented, i.e., the controller synthesis for each system and the compositional synthesis for the interconnected system, as well as the characterization of the invariant set. Finally, in Section V, we show the effectiveness of the proposed approach by applying it to a temperature regulation problem of adjacent rooms.

II. Problem Formulation

In this section, firstly, we are going to address the problem under consideration and secondly we are going to introduce basic concepts and tools that are utilized for its proposed solution throughout the paper.

A. Interconnected systems

We consider a discrete-time dynamical system of the form:

$$\begin{aligned} x_1^+ &= f_1(x_1, x_2, \ldots, x_N, u_1) \\ x_2^+ &= f_2(x_2, x_1, \ldots, x_N, u_2) \\ &\vdots \\ x_N^+ &= f_N(x_N, x_1, \ldots, x_{N-1}, u_N) \end{aligned} \tag{1}$$

with $N \in \mathbb{N}$. For notational simplicity we are going to write the individual equations for system i from Eqs. (1), as follows:

$$x_i^+ = f_i(x_i, x_{-i}, u_i), \qquad i \in \{1, 2, \ldots, N\} \tag{2}$$

where index $-i$ denotes all the states that are not x_i. By x_i we denote the states of the system with $x_i \in X_i \subseteq \mathbb{R}^{n_i}$ and by u_i we denote the control inputs with $u_i \in U_i \subseteq \mathbb{R}^{m_i}$. Notice now, that system (1) is a composition of N interconnected systems and that the terms x_{-i} in (2) is the effect of all the other systems on system i.

The control objective of this paper consists of the states of system (1) meeting a safety specification. This specification comprises maintaining the states x_i with $i \in \{1, 2, \ldots, N\}$, inside a set $X_{S_i} \subseteq X_i$, where X_{S_i} is considered to be the corresponding safe set of system i. The formal definition for this safety specification will be given in the following subsection, however, before continuing it is of essence to briefly discuss how these kind of problems are usually treated.

The safety problem for system (1) is more often than not, a difficult problem to solve in a centralized way, since the full set of states $X_1 \times \cdots \times X_N$ is too large to design a controller. An approach is to design a local controller for the safety problem of each system i, treating the effect of x_{-i} from (2), as a bounded disturbance. The composition of the interconnected system is then resolved, using the assume-guarantee reasoning that is going to be presented later.

B. Transition systems

A transition system can be defined as follows:

Definition 2.1: A *transition system* $\mathscr{T}$ is a tuple

$$\mathscr{T} = (X, U, \Delta) \tag{3}$$

consisting of a set of states X; a set of inputs U and a transition relation $\Delta \subseteq X \times U \times X$.

For system (1), there is $X = X_1 \times \cdots \times X_N$ and $U = U_1 \times \cdots \times U_N$. The transition relation Δ signifies that a state x^+ can be reached initiating from x under the control input u. Furthermore, the set of enabled inputs at state x is denoted by $\mathrm{enab}_\Delta(x) = \{u \in U |\ \Delta(x,u) \neq \emptyset\}$. If $\mathrm{enab}_\Delta(x) = \emptyset$, then x is said to be a blocking state and the set of non-blocking states is denoted nbs_Δ.

As we discussed earlier, system (1) will be decomposed to N subsystems such as (2), each one of them having its own transition relation. Each subsystem can be modeled by a transition system that is affected by disturbances. This transition system is of the following form:

Definition 2.2: A *transition system with disturbances* $\mathscr{T}_i$ is a quadruple

$$\mathscr{T}_i = (X_i, W_i, U_i, \Delta_i) \tag{4}$$

where X_i is the set of states; W_i is the product space of the state sets of all $-i$, i.e., $W_i := \Pi_{j \neq i} X_j$, U_i is the set of inputs and Δ_i is the transition relation $\Delta_i \subseteq X_i \times W_i \times U_i \times X_i$, describing the dynamics of (2).

It should be noted, that for transition systems with disturbances, the set of enabled actions at a state x_i is given by:

$$\mathrm{enab}_{\Delta_i}(x_i) = \{u_i \in U_i |\ \forall x_{-i} \in X_{-i}, \Delta_i(x_i, x_{-i}, u_i) \neq \emptyset\}$$

III. Assume-Guarantee Contracts for Safety

A. Safety specifications

Let us, now, consider a transition system $\mathscr{T}_i$ as in (4) for each system i and $X_{S_i} \subseteq X_i$ to be the corresponding set of safe states. The safety problem for system i, consists in characterizing a subset of safe states $S_i \subseteq X_{S_i}$, such that when the system's state x_i is initially in S_i and assuming that the states x_{-i} belong to known safe sets S_{-i}, the state x_i can remain in S_i forever, under suitable control. Moreover, we need to synthesize a controller which makes it possible to restrict the behavior of the individual system so that its state remains inside the set S_i. The closely related notions of a (robust) controlled invariant subset as well as the corresponding safety controller are given next:

Definition 3.1: Let us consider transition system $\mathscr{T}_i$ and $X_{S_i} \subseteq X_i$ a set of safe states:

- $S_i \subseteq X_{S_i}$ is a (robust positively) controlled invariant subset of X_{S_i} with respect to set of disturbances S_{-i} if and only if for all $x_i \in S_i$ there exists $u_i \in \mathrm{enab}_{\Delta_i}(x_i)$ such that for all $x_{-i} \in S_{-i}$, $\Delta_i(x_i, x_{-i}, u_i) \subseteq S_i$.

- $S_i^\star \subseteq X_{S_i}$ is the maximal (robust positively) controlled invariant subset of X_{S_i} with respect to the set of disturbances S_{-i}, if and only if $S_i^\star$ is a controlled invariant subset of X_{S_i} and for all controlled invariant subsets $S_i \subseteq X_{S_i}$, we have $S_i \subseteq S_i^\star$.

Given a (robust positively) controlled invariant subset $S_i \subseteq X_{S_i}$, a safety controller maintains the state of the controlled transition system inside S_i:

Definition 3.2: Let us consider transition system $\mathscr{T}_i$ and $X_{S_i} \subseteq X_i$ a set of safe states, let $S_i \subseteq X_{S_i}$ be a robust controlled invariant subset of X_{S_i} with respect to the set of disturbances S_{-i}. The controller $C_i : X_i \to 2^{U_i}$ is a safety controller for the robust controlled invariant subset S_i if, $S_i \subseteq \mathrm{Dom}(C_i)$ and for all $x_i \in S_i$ and for all $u_i \in C_i(x_i)$, and all $x_{-i} \in S_{-i}$, we have $\Delta_i(x_i, x_{-i}, u_i) \subseteq S_i$.

B. Assume-Guarantee reasoning for the composition of subsystems

The main objective of this paper, is to solve the safety problem for the original system (1). In order to do so, we are going to utilize the assume-guarantee reasoning. Firstly, some preliminaries will be given on assume-guarantee contracts. Intuitively, using this method a correct behavior of a composed system can be derived if each subsystem satisfies its specification (guarantee), assuming that the other subsystems satisfy their specifications (assumption). In this paper, the subsystems need to fulfill their safety specifications, therefore, the assume-guarantee contract for safety for a subsystem i will be defined as:

Definition 3.3: Let a transition system of the form (4) and X_{S_i} be the safe set of system i. Furthermore, let $X_{S_{-i}}$ be the safe sets of the other subsystems $-i$. The contract for safety of system i will be denoted as $\mathscr{C}_i^s = (A_i, G_i)$, where:

- $A_i \subseteq X_{S_{-i}}$, are sets of assumptions;
- $G_i \subseteq X_{S_i}$, are sets of guarantees.

Each subsystem i, is assigned a $\mathscr{C}_i^s$ contract that specifies the invariance property that i-subsystem must fulfill, under assumptions about its environment, i.e. subsystems $-i$. Using the assume-guarantee reasoning for each subsystem i we can derive a conclusion on the invariance property of their composition, and therefore find the controlled invariant set for system (1):

Proposition 3.1: Let each subsystem i of (2) be assigned a contract $\mathscr{C}_i^s$, as it is defined in Definition (3.3). Assume that G_i is a robust controlled invariant subset, with respect to the set of disturbances A_i, i.e.,

$$\forall x_i \in G_i, \exists u_i \in \mathrm{enab}_{\Delta_i}(x_i) : \forall x_{-i} \in A_i, \Delta_i(x_i, x_{-i}, u_i) \subseteq G_i$$

and assume that $\Pi_{j \neq i} G_j \subseteq A_i$. Then, the set

$$G := G_1 \times G_2 \times \cdots \times G_N$$

is positively controlled invariant.

Proof: We need to prove that $G := G_1 \times G_2 \times \cdots \times G_N$ is positively controlled invariant for the transition system (3), thus we need to show that for all $(x_i, x_{-i}) \in G$, there exists $(u_i, u_{-i}) \in U_i \times U_{-i}$ such that the transition system $\Delta(x_i, x_{-i}, u_i, u_{-i}) \subseteq G$. This implication is straightforward noticing that, for $\mathscr{T}_i$ we obtain:

$$\forall x_i \in G_i, \exists u_i \in \mathrm{enab}_{\Delta_i}(x_i) : \forall x_{-i} \in G_{-i}, \Delta_i(x_i, x_{-i}, u_i) \subseteq G_i$$

since $G_{-i} \subseteq A_i$. Using this reasoning for all $i \in \{1, \ldots, N\}$ we can conclude that G is a positively invariant set. ■

Assume-guarantee contracts for compositional reasoning is always sound, provided there is no circularity between assumptions and guarantees. Circularity in a compositional framework is arguably the main difficulty in contract-based design. From Proposition 3.1, it can be deduced that there is in fact a cyclic dependence of the controlled invariant subsets G_i. Next, we proceed with the quantitative approach that aims to overcome this problem; to characterize the sets G_i and to design the safety controller.

IV. Quantitative approach to safety controller synthesis for interconnected systems

In this section we are going to present the quantitative approach for safety controller synthesis for each of the subsystems (2). This approach is called quantitative since not only does partition the states to safety controllable (i.e. $x_i \in S_i^\star$) and safety uncontrollable (i.e. $x_i \notin S_i^\star$), but it also measures the level of safety at a given state. This measure quantifies how far one can stay from the unsafe set, starting from that state, while, it also provides a measure that quantifies how close one can stay from the safe set, in case this state is safety uncontrollable. This approach is useful in the controller synthesis as well: for both controllable and uncontrollable states, it provides control inputs that would optimize the level of safety of the corresponding successors. The quantitative approach has been first presented in [5] in a centralized framework and is accordingly modified here for the decentralized case.

A. Controller synthesis for each of the systems

We introduce a cost function $h_i : X_i \to \mathbb{R}$, which is chosen to be the signed distance from the state x_i to the safe set X_{S_i}, i.e.

$$h_i(x_i) = d_s(x_i, X_{S_i}) \tag{5}$$

This cost function is chosen because it can quantify how safe or unsafe is a given state x_i. The distance function is given as:

$$d_s(x_i, X_{S_i}) = \begin{cases} \sup\{\gamma \geq 0 | B(x_i, \gamma) \cap X_{S_i} \neq \emptyset\} & \text{if} \quad x_i \notin X_{S_i} \\ -\sup\{\gamma \geq 0 | B(x_i, \gamma) \subseteq X_{S_i}\} & \text{if} \quad x_i \in X_{S_i} \end{cases}$$

where $B(x_i, \gamma)$ denotes the ball centered in x_i of radius γ. An interpretation of a positive value of $h_i(x_i)$ is that x_i lies outside the safe set: the larger $h_i(x_i)$, the further this state is from the safe set. Conversely, a negative value of $h_i(x_i)$ means that x_i lies inside the safe set. In this case the smaller value of $h_i(x_i)$, the further x_i is from the boundary of the safe set and thus, it is safer.

We are now ready to define the quantitative algorithm: First we define a sequence $\{V_i^k\}_{k \in \mathbb{N}}$ for each subsystem i, where $V_i^k : X_i \to \mathbb{R} \cup \{+\infty\}$. This is now defined iteratively as follows:

For $k=0$, and $x_i \in X_i$, we assume that: $V_i^0(x_i) := h_i(x_i)$.
For $k \in \mathbb{N}$ and $x_i \in X_i$, we define:

$$V_i^{k+1}(x_i) := \tag{6}$$
$$\begin{cases} \max\Big(h_i(x_i), \min\limits_{u_i \in \text{enab}_{\Delta_i}(x_i)} \max\limits_{\substack{x_i' \in \Delta_i(x_i,x_{-i},u_i) \\ x_{-i} \in A_i}} V_i^k(x_i')\Big) & \text{if } x \in \text{nbs}_{\Delta_i} \\ +\infty & \text{if } x_i \notin \text{nbs}_{\Delta_i} \end{cases}$$

The fixed-point is then obtained by:

$$V_i^\star(x_i) := \lim_{k \to +\infty} V_i^k(x) \tag{7}$$

If $\mathscr{T}_i$ is finite, then the limit is reached for a finite $k \in \mathbb{N}$.

The quantitative algorithm can also be used to design the local safety controllers, as follows:

Theorem 4.1: Let $\mathscr{T}_i$ be finite, then for all $a \in \mathbb{R}$ $S_i^a = \{x_i \in X_i \mid V_i^\star(x_i) \leq a\}$ is the maximal robust controlled invariant subset of the set $X_i^a = \{x_i \in X_i \mid h_i(x_i) \leq a\}$, with respect to A_i. Let us consider the controller $C_i^\star$ defined by:

$$C_i^\star(x_i) = \begin{cases} \emptyset & \text{if } x_i \notin \text{nbs}_{\Delta_i} \\ \arg \min\limits_{u_i \in \text{enab}_{\Delta_i}(x_i)} \max\limits_{\substack{x_i' \in \Delta_i(x_i,x_{-i},u_i) \\ x_{-i} \in A_i}} V_i^\star(x_i') & \text{if } x_i \in \text{nbs}_{\Delta_i} \end{cases} \tag{8}$$

Then, for all $a \in \mathbb{R}$, $C_i^\star$ is a safety controller for the robust controlled invariant subset S_i^a, with respect to A_i.
The proof of this theorem is similar to the proof of Theorem 7 in [5]. Theorem 4.1 yields that the quantitative approach allows to compute the maximal controlled invariant subsets of a parameterized family of safe sets and allows the design of a common safety controller $C_i^\star$ given by (8) for the whole family of maximal controlled invariant subsets.

B. Compositional synthesis for interconnected systems

It can be seen from (8), that $C_i^\star$ chooses inputs that will minimize the (worst-case) value of V_i^* at the next state. It can then be obtained that applying controller $C_i^\star$, the function $V_i^\star$ is non-increasing along the trajectories of the controlled system. In order to make a connection to the classical control theory, $V_i^\star$ can be seen to act as a (weak) robust Lyapunov function with respect to the external effect x_{-i}, with $x_{-i} \in A_i$. The value $V_i^\star(x_i)$, then, provides a measure of the level of safety of x_i, since along trajectories of the controlled system, starting from state x_i, the value of $V_i^\star(\cdot)$ and thus of $h_i(\cdot)$ would remain smaller than or equal to $V_i^\star(x_i)$. Expanding this realization on the measure of safety, we are now going to parameterize the safe set. Assume the following form of specifications span the N states of (1):

$$A_i := \{x_{-i} \in X_{-i} \mid d_s(x_j, X_{S_j}) \leq \delta_j, \forall j \neq i\} \tag{9}$$

For every subsystem i, we are going to employ the quantitative algorithm as described previously. Applying the quantitative algorithm on the transition system $\mathscr{T}_i$, with transition relation $x_i' \in \Delta_i(x_i, x_{-i}, u_i)$ with $x_{-i} \in A_i$, we can derive the value function $V_i^\star$ which will now depend on the parameter δ_{-i}. This procedure is described below in Algorithm 1. The smallest value of $V_i^\star$ will then provide us with the smallest non-empty robust controlled invariant set, according to Theorem 4.1 and the respective parameters are denoted by $\eta_i(\delta_{-i})$.

Algorithm 1: Design of value function $V_i^\star$

Data: $\mathscr{T}_i$, A_i, G_i
Result: Function $\eta_i(\delta_{-i})$
for $i = 1, \ldots, N$ **do**
  Find $V_i^\star(x_i)$ from (7), for $x_i' \in \Delta_i(x_i, x_{-i}, u_i)$, with $x_{-i} \in A_i$ given by (9);
  $\eta_i(\delta_{-i}) := \min_{x_i} V_i^\star(x_i)$
end

Corollary 1: Let the safety contract $\mathscr{C}_i^s$ for subsystem $\mathscr{T}_i$, with A_i be taken from (9). Then, the set $G_i := \{x_i \in X_i \mid V_i^\star(x_i) \leq \eta_i(\delta_{-i})\}$ is a controlled invariant set for $\mathscr{T}_i$.

Proof: From Theorem 4.1 taking $a \equiv \eta_i(\delta_{-i})$ results to $G_i := \{x_i \in X_i \mid V_i^\star(x_i) \leq \eta_i(\delta_{-i})\}$ being a robust controlled invariant subset of the set $X_i^{\eta_i(\delta_{-i})} = \{x_i \in X_i \mid d_s(x_i, X_{S_i}) \leq \eta_i(\delta_{-i})\}$, with respect to A_i. ∎

Built upon these results, we are now able to obtain a characterization on the invariant set of the original transition system (3).

Theorem 4.2: Let $\mathscr{T}_i$ from (4), with guarantee set of the form $G_i := \{x_i \in X_i \mid V_i^\star(x_i) \leq \eta_i(\delta_{-i})\}$. If

$$\eta_i(\delta_{-i}) \leq \delta_i \quad \forall i = \{1, \ldots, N\} \tag{10}$$

then $G = G_1 \times \cdots \times G_N$ is a positive invariant set for $\mathscr{T}$ from (3).

Proof: From Corollary 1, it can be obtained that the sets $G_i = \{x_i \in X_i \mid V_i^\star(x_i) \leq \eta_i(\delta_{-i})\}$ are controlled invariant sets of subsystems $\mathscr{T}_i$. We need now to prove that $\Pi_{j \neq i} G_j \subseteq A_i$, which is true when $\eta_i(\delta_{-i}) \leq \delta_i$ for all $i = \{1, \ldots, N\}$ because $G_i \subseteq \{x_i \in X_i \mid d_s(x_i, X_i) \leq \eta_i(\delta_{-i})\}$. Hence, from Proposition 3.1 we conclude that $G = G_1 \times \cdots \times G_N$ is a positive invariant set for $\mathscr{T}$. ∎

C. Characterization of the compositional invariant set

The circular dependence on the sets G_i that was described earlier for the compositional framework, has now been shifted on the parameters δ_i. Therefore, the objective is to find parameters $\delta_i^\star$ such that the corresponding sets G_i that will be characterized through the quantitative procedure (for these parameters), all be control invariant. Specifically, according to Theorem 4.2, parameters $\delta_i^\star$ should satisfy (10). In fact, they can be computed by another fixed-point iteration, as it is described in Algorithm 2.

D. Compositional abstraction based synthesis using the quantitative approach

Let system (1) be decomposed into N subsystems (2) with local specifications as we have already discussed. Making use of symbolic abstractions (i.e. discrete abstractions) on the subsystems we can compute local controllers, assuming that the other subsystems meet their own specifications. These abstractions can be obtained in several ways (computing

Algorithm 2: Parameters $\delta_i^\star$

Data: δ_i, $\eta_i(\delta_{-i})$
Result: $\delta_i^\star$
initialization: $k=0$, $\delta_i^0=\delta_i^{\min}$, $\delta_{-i}^0=\delta_{-i}^{\min}$;
while $\delta_i^k \neq \delta_i^{k-1}$ *and* $\delta_i^k \leq 0$ **do**
  for $i=1,\ldots,N$ **do**
    Find $\eta_i(\delta_{-i}^k)$ from Algorithm 1;
    $\delta_i^{k+1}=\eta_i(\delta_{-i}^k)$
  end
  $k=k+1$;
  if $\delta_i^k=\delta_i^{k-1}$ **then**
    return δ_i^k
  end
  else $\exists i$ such that $\delta_i^k>0$
    "No valid decomposition"
  end
end

reachable sets, state quantization etc.) and in addition finiteness of the abstraction guarantees that the limit (7) is reached in a finite number of steps k. The concrete subsystem as well as the corresponding abstraction should be governed by some required formal behavioral relationship between them. In particular assume $\mathscr{T}_i^c$ to be the transition system of the concrete system and $\mathscr{T}_i^a$ to be the transition system of the abstraction. Then it is required that $\mathscr{T}_i^c$ to be either approximately alternatingly simulated or approximately alternatingly bisimilar to $\mathscr{T}_i^a$. The definitions of these relations can be found in [20]. In our prior work in [5] has been proven that provided the transition systems, concrete and abstraction, lead these relations, applying the quantitative approach on the abstraction results to a parameterized family of controlled invariant subsets for the concrete system.

V. Numerical Results

In this section we consider a simple example for illustration purposes: a temperature regulation problem for two rooms which belong to a building and share a wall, is going to be considered. Each of the rooms is equipped with a respective heater. The two subsystems are interconnected since the temperature of one is affecting the other and vice versa. The problem at hand is to regulate the temperature of each room around a desired nominal value. Using the quantitative approach we are going to synthesize a controller that keeps the temperature of each room in a set around their nominal values, which will also be characterized. Notice, that the same control scheme can be applied for a number of rooms n greater than two, without significant difficulty. The model that we are going to employ for the temperature regulation is the following:

$$\begin{aligned} T_1^+ &= T_1+\alpha(T_2-T_1)+\beta(T_e-T_1)+\gamma(T_h-T_1)u_1 \\ T_2^+ &= T_2+\alpha(T_1-T_2)+\beta(T_e-T_2)+\gamma(T_h-T_2)u_2 \end{aligned} \tag{11}$$

where T_1, T_2 are the temperatures of the first and second room, respectively. The outside temperature is considered to be constant, at $T_e=-1^\circ C$, while $T_h=50^\circ C$ is the heater temperature. Each room $i=\{1,2\}$, has a control input that lies in $u_i\in[0,1]$. The conduction factors are given by $\alpha=0.45$, $\beta=0.045$ and $\gamma=0.09$.

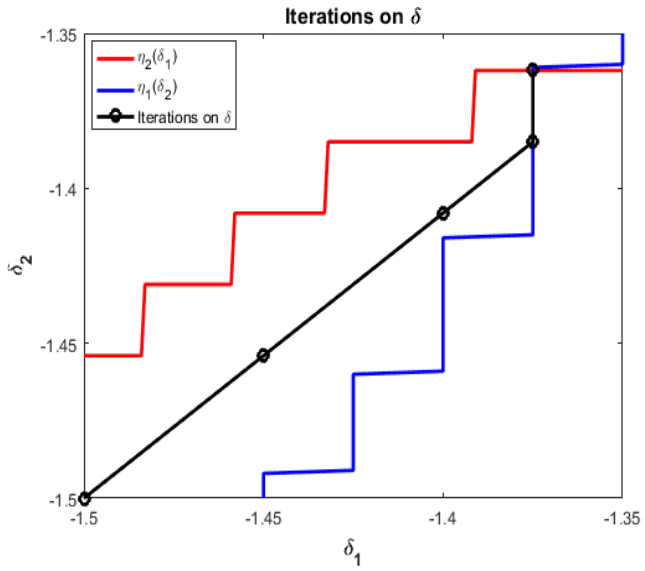

Fig. 1. (a) Sequence of values $\eta_1(\delta_2)$ and $\eta_2(\delta_1)$ for system (11). Red and blue solid lines represent $\eta_1(\delta_2)$ and $\eta_2(\delta_1)$, respectively. The black solid line depicts the iteration of the parameters δ_1 versus parameter δ_2, until they reach their fixed point $\delta_1^\star=-1.3750$ and $\delta_2^\star=-1.3620$.

Each rooms' temperature lie in a state set X_i, for $i=1,2$. The first room's temperature lies in $X_1=[10,35]^\top$ while for the second room there is $X_2=[10,33]^\top$. Moreover, the corresponding safe sets are $X_{S_1}=[22,25]^\top$ and $X_{S_2}=[20,23]^\top$, respectively. The discrete-time dynamics of (11) can be decomposed and be represented as two finite transition subsystems $\mathscr{T}_1$ and $\mathscr{T}_2$. Two symbolic models were built following the approach described in [14]. The symbolic model for each room was built assuming that the temperature of the other is not exactly known, but lying to its safe set, which introduced non-determinism to the symbolic models. Furthermore, the state sets were uniformly partitioned by n_{x_i} intervals per component, with $n_{x_1}=n_{x_2}=1000$, while the control set $U=[0,1]^2$ was uniformly discretized into $u_{modes}=21$ for all the components.

The proposed algorithm (2) was then performed for the two transition systems $\mathscr{T}_1$ and $\mathscr{T}_2$, assuming initial value for the parameters $\delta_1^0=-1.5$ and $\delta_2^0=-1.5$. The number of iterations of the algorithm (2) were finite and specifically $k=5$, as it can be seen in Fig.1.The fixed point $\delta_1^\star,\delta_2^\star$ was obtained with $\delta_1^\star=-1.3750$ and $\delta_2^\star=-1.3620$. Hence, we conclude that the set $S=S_1\times S_2$ is a controlled invariant set, with $S_1=[22-\delta_1^\star,25+\delta_1^\star]^\top=[23.3750,23.6250]^\top$ and $S_2=[20-\delta_2^\star,23+\delta_2^\star]^\top=[21.3620,21.6380]^\top$.

Assuming initial temperatures $T_1^0=23.4^\circ C$ and $T_2^0=21.4^\circ C$ for the two rooms, Fig.2 illustrates the trajectory of the room's temperatures while applying the controllers. It can be witnessed that both temperatures remain inside the safe set S which is illustrated by the dashed lines.

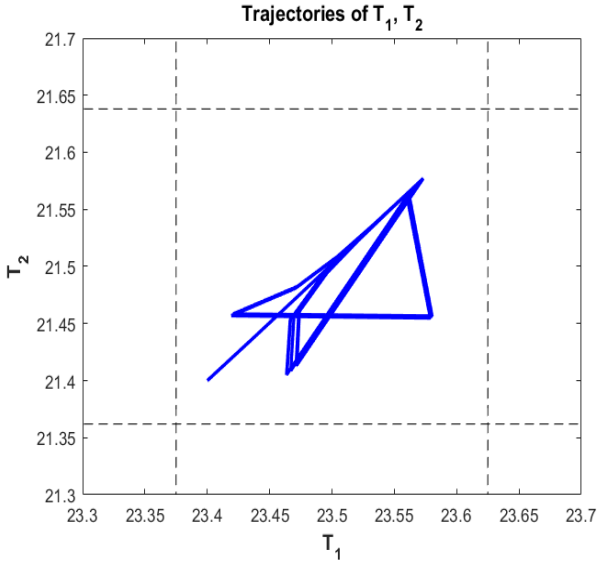

Fig. 2. The blue line depicts a trajectory of the two temperatures of the two rooms, initiating at $T^0_{1,2} = [23.4, 21.4]^\circ C$. The black dashed lines represent the safe set.

VI. CONCLUSIONS

In this paper, we proposed a quantitative approach to safety controller synthesis for complex systems comprised by multiple interconnected subsystems. Using assume-guarantee contracts for each of the subsystems while applying the quantitative fixed point algorithm we were able to compute controlled invariant subsets of parameterized family of sets and synthesize the corresponding controllers. In order to argue for the safety specification of the original complex system since there is circularity between the implications of the subsystem's contracts, we proposed a way to compute the parameters on the parameterized invariant sets, that guarantee the simultaneous fulfillment of all the contracts. Thus, the compositional problem was resolved, providing the corresponding controller and the characterization of the invariant set. Finally, numerical results, showed the effectiveness of the approach.

In future work, we plan to extend our framework to deal with other high-level specifications beyond safety which is considered in this paper, such as reachability or more general properties specified by automata or temporal logic.

REFERENCES

[1] A. Girard, "Controller synthesis for safety and reachability via approximate bisimulation," *Automatica*, vol. 48, no. 5, pp. 947 – 953, 2012.

[2] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Springer, 2008.

[3] M. Rungger and P. Tabuada, "Computing robust controlled invariant sets of linear systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3665–3670, 2017.

[4] J. Lygeros, C. Tomlin, and S. Sastry, "Controllers for reachability specifications for hybrid systems," *Automatica*, vol. 35, no. 3, pp. 349 – 370, 1999.

[5] A. Eqtami and A. Girard, "Safety control, a quantitative approach," in *IFAC Conference on Analysis and Design of Hybrid Systems*, 2018, pp. 187–192.

[6] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theoretical Computer Science*, vol. 410, no. 42, pp. 4262–4291, 2009.

[7] A. Donzé and O. Maler, "Robust satisfaction of temporal logic over real-valued signals," in *International Conference on Formal Modeling and Analysis of Timed Systems*. Springer, 2010, pp. 92–106.

[8] V. Raman, A. Donzé, D. Sadigh, R. M. Murray, and S. A. Seshia, "Reactive synthesis from signal temporal logic specifications," in *International Conference on Hybrid Systems: Computation and Control*. ACM, 2015, pp. 239–248.

[9] S. Sadraddini and C. Belta, "Robust temporal logic model predictive control," in *Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2015, pp. 772–779.

[10] S. Raković, B. Kern, and R. Findeisen, "Practical set invariance for decentralized discrete-time systems," in *IEEE Conference on Decision and Control*, 2010, pp. 3283–3288.

[11] C. Conte, N. Voellmy, M. Zeilinger, M. Morari, and C. Jones, "Distributed synthesis and control of constrained linear systems," in *American Control Conference*, 2012, pp. 6017–6022.

[12] P. Nilsson and N. Ozay, "Synthesis of seperable controlled invariant sets for modular local control design," in *American Control Conference*, 2016, pp. 5656–5663.

[13] S. Coogan and M. Arcak, "A dissipativity approach to safety verification for interconnected systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1722–1727, 2015.

[14] P.-J. Meyer, A. Girard, and E. Witrant, "Safety control with performance guarantees of cooperative systems using compositional abstractions," in *Proceedings of the 5th IFAC Conference on Analysis and Design of Hyrbid Systems*, 2015, pp. 317–322.

[15] A. L. Coënt, L. Fribourg, N. Markey, F. D. Vuyst, and L. Chamoin, "Distributed synthesis of state-dependent switching control," in *International Workshop on Reachability Problems*, 2016, pp. 119–133.

[16] A. Saoud, A. Girard, and L. Fribourg, "On the composition of discrete and continuous-time assume-guarantee contracts for invariance," in *European Control Conference*, 2018.

[17] ——, "Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems," in *IEEE Conference on Decision and Control (CDC)*, 2018.

[18] E. Kim, M. Arcak, and S. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *International Conference on Hybrid Systems: Computation and Control*, 2017, pp. 207–216.

[19] E. Dallal and P. Tabuada, "On compositional symbolic controller synthesis inspired by small-gain theorems," in *54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 6133–6138.

[20] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer US, 2009.