Formal Verification of Medical CPS: a Laser Incision Case Study

ANDRÉ A. GERALDES, University of Verona, Italy, and Istituto Italiano di Tecnologia, Italy
LUCA GERETTI, University of Verona, Italy
DAVIDE BRESOLIN, University of Padova, Italy
RICCARDO MURADORE and PAOLO FIORINI, University of Verona, Italy
LEONARDO S. MATTOS, Istituto Italiano di Tecnologia, Italy
TIZIANO VILLA, University of Verona, Italy

The use of robots in operating rooms improves safety and decreases patient recovery time and surgeon fatigue, but introduces new potential hazards that can lead to severe injury, or even the loss of human life. Thus, safety has been perceived as a crucial system property since the early days both by the industry, the medical community and the regulatory agents. In this paper we discuss the application of the mathematically rigorous technique known as Formal Verification to analyze the safety properties of a laser incision case study, and assess its safe and predictable operation. Like all formal methods approaches, our analysis has three distinct components: a method to create a model of the system, a language to specify the properties, and a strategy to prove rigorously that the behavior of the model fulfills the desired properties. The model of the system takes the form of a hybrid automaton consisting of a discrete control part that operates in a continuous environment. The safety constraints are formalized as reachability properties of the hybrid automaton model, while the verification strategy exploits the capabilities of the tool ARIADNE to address the verification problem and answer the related questions ranging from safety to efficiency and effectiveness.

CCS Concepts: •**Computing methodologies** → *Model verification and validation;* •**Computer systems organization** → *Heterogeneous (hybrid) systems; Robotics;*

Additional Key Words and Phrases: Formal Verification, Hybrid Systems, Surgical Robotics

ACM Reference Format:
André A. Geraldes, Luca Geretti, Davide Bresolin, Riccardo Muradore, Paolo Fiorini, Leonardo S. Mattos and Tiziano Villa. 2016. Formal Verification of Medical CPS: a Laser Incision Case Study. *ACM Trans. Cyber-Phys. Syst.* 0, 0, Article XXXX (2016), 29 pages.
DOI: 0000001.0000001

1. INTRODUCTION

First used medically in 1985, robots are now of common use in modern operating rooms for laparoscopy, neurosurgery, orthopedic surgery, emergency response, and various other medical disciplines [Beasley 2012]. In a short time the prototypes built in robotics laboratories turned into commercially available systems, with a new terminology witnessing this trend: robotic surgery, computer-integrated surgery, medical robotics, rehabilitation robotics, telerobotics, telesurgery, robotic assistive systems, robot-assisted laparoscopic surgery, etc. [Kazanzides et al. 2008; Taylor 2006; Berkelman et al. 2009]. The use of robots in operating rooms improves safety, accuracy, reproducibility, and decreases patient recovery time and surgeon fatigue [Cleary and Nguyen 2001; Marohn and Hanly 2004; Guglielmelli et al. 2009; Desai and Ayache

Author's addresses: A. A. Geraldes, L. Geretti, R. Muradore, P. Fiorini, and T. Villa, Department of Computer Science, University of Verona, Verona, Italy; D. Bresolin, Department of Mathematics, University of Padova, Padova, Italy; L. S. Mattos, Department of Advanced Robotics, Istituto Italiano di Tecnologia, Genova, Italy.

DOI: 0000001.0000001

2009], but introduces new potential hazards that can lead to severe injury, or even the loss of human life. Thus, safety has been perceived as a crucial system property since the early days [Taylor et al. 1991; Davies 1996; Fei et al. 2001]. Regulatory agencies such as the US Food and Drug Administration and the European Medicines Agency need effective means for assuring that medical devices are safe and reliable, and so require more rigorous design methodologies to provide this assurance.

In engineering practice, the analysis of a system is usually carried out via simulation, which allows the designers to explore one of the possible system executions at a time. As the scale and the complexity of medical robotic systems increase, it becomes more and more challenging to assure the safety of the system only by simulation and testing. The use of the mathematically rigorous technique known as *Formal Verification* (as part of *Formal Methods*) in the development of medical robots can help accomplish this [Jetley et al. 2006; Muradore et al. 2011; Kouskoulas et al. 2013; Bresolin et al. 2014]. The annotation "mathematically rigorous" means that the specifications are well-formed statements in a mathematical language, and "formal verification" denotes methods based on a rigorous deduction process that can be checked by a mechanical procedure. The value of formal verification is that it provides the means to explore all possible executions of the system and ensure proper functionality in all cases, or conversely to acquire information about potential fault cases. Nowadays, formal methods are standard practice in many ICT industries for the development of HW/SW systems, and are becoming a vital aspect in the design of safety-critical cyberphysical systems, including robotics and automation systems [Johnson 2007; Kress-Gazit 2011; Nuzzo et al. 2015]. In medical and health robotics, they can provide robust modeling, analysis, and verification tools, to allow optimal system integration by designing systems based on robotic technologies whose components work with each other in a predictable fashion [Matarić et al. 2013].

In this paper we discuss the analysis of safety properties of a laser incision case study, described in Fichera et al. [2015]. Rather than taking a testing or simulation approach, we apply formal verification to analyze the control algorithm of interest. This rigorous analysis ensures that the controller behaves correctly in all possible scenarios, rather than only for finitely many test cases, leading to a much stronger guarantee on the behavior of the system, and assuring its safe and predictable operation. The contributions of this work are the following:

(1) It highlights how a formal verification approach can be used to predict the behaviour of a robotic system. Using numerically conservative interval analysis with tools similar to ARIADNE [Benvenuti et al. 2014], which has been chosen in this paper, it is possible to provide guarantees on system properties. Conversely, simulation tools like SIMULINK®, however recognized by industry, are unable to replicate these results since they necessarily rely on a point-based exploration of the verification space, with uncontrolled numerical rounding.
(2) It performs a detailed analysis of the physical prototype, in order to produce a model of the system that can be analyzed by ARIADNE. Even if approximations are introduced in order to improve the numerical tractability of the system, the consistency of the verification results compared with the available experimental data validates the model analyzed by the tool.
(3) It helps the development and refinement of current methodologies and tools by identifying what needs to be improved to put formal methods into widespread use. For instance, referring to modeling and verification aspects, it is worth remarking that this case study prompted various improvements of ARIADNE to handle this challenging problem, with the effect of raising the bar for state-of-the-art nonlinear reachability analysis.

The paper is organized as follows. Section 2 provides a brief overview of the related work and tools that apply formal verification to medical robotics and other cyber-physical systems (CPS). Section 3 introduces the physics of the laser incision case-study, which is then modeled with a composition of hybrid automata in Section 4 and formally verified in Section 5. Section 6 concludes the paper.

2. RELATED WORK

In this paper we analyze medical robotic systems following the *Model-Based Design* paradigm, an approach that aims at detecting and correcting errors in the early stages of system design [Sangiovanni-Vincentelli 2007; Henzinger and Sifakis 2006; Nuzzo et al. 2015]. Originally applied in the area of embedded and control systems, model-based design has recently emerged as a means of improving the quality of the design process also in the medical device industry [Lee et al. 2012]. In this methodology, a designer first constructs a model of the system under design, and performs extensive analysis with respect to correctness requirements before generating the implementation from the model. Medical robotic systems, such as the laser incision system considered in this paper, consist of a collection of interacting hardware and software modules reacting to a continuously evolving environment. For this reason, one of the most appropriate mathematical models to represent medical systems is the one of *hybrid systems*, which combines discrete-event computational models with differential- and algebraic- equation models for continuous dynamical systems. In this way, hybrid systems can describe the behavior of both the "controller" (i.e., the medical robot) and the "plant" with continuously evolving physical activities on which the medical device operates (i.e., the patient body). Given that the interplay of continuous and discrete behaviors can model faithfully automotive, robotics, avionics, medical, and other safety-critical systems, formal verification of hybrid systems has been a vibrant research area for the past two decades, giving rise to a wide family of tools and formalisms [Alur 2011; Nuzzo et al. 2015].

A popular formalism to model hybrid systems is the one of *hybrid automata* [Alur et al. 1995; Henzinger 1996]. Intuitively, a hybrid automaton is a finite-state automaton enriched with a set of *continuous variables*. Each discrete state (called a *location* or *mode*) is annotated with constraints that specify the continuous evolution of the system, while transitions between locations are annotated with guards and resets that specify the discrete evolution. The safety verification problem for hybrid automata usually consists of checking whether every execution of the automaton starting from a given *initial set* of states stays within a given *safe set* of states. Hence, of particular importance in the analysis of a hybrid automaton is the computation of the *reachable set*, i.e., the set of all states that can be reached under the dynamical evolution starting from a given initial state set. The state of a hybrid automaton consists of a discrete location paired with a vector of continuous variables, therefore it has the cardinality of continuum. This makes the analysis computationally difficult: indeed, the reachable set of a hybrid automaton is not computable exactly, except for classes that severely restrict the dynamics of the continuous variables [Henzinger et al. 1998].

A relevant class for which reachability is computable exactly is the one of *timed automata* [Alur and Dill 1994], where all the continuous variables are clocks (they have derivative 1) that can only be reset to zero. Many verification problems can be solved exactly for this class, making it an interesting formalism for the verification of medical systems where the dynamics can be abstracted to an interleaving of (nondeterministic) delays and discrete events. Two recent works applied timed automata to some interesting medical case studies: an infusion pump [Kim et al. 2011] and an implantable pacemaker [Jee et al. 2010]. By exploiting the capabilities of two formal modeling and

analysis tools, UPPAAL [Behrmann et al. 2011] and TIMES [Amnell et al. 2004], the authors develop and verify the model of the system and generate code from it.

When the continuous dynamics of the system cannot be abstracted away, exact verification techniques cannot be applied anymore, and the key challenge is to develop suitable approximation techniques that can under- or over- approximate the evolution of the hybrid system. A popular strategy, put into practical use by the tool PHAVER [Frehse 2008], is to use polyhedral representations to over-approximate the state space of affine linear dynamics. Operations on polyhedra have a complexity that is exponential in the number of dimensions (that is, in the number of continuous variables), and thus scalability is limited: systems with more than 10 continuous variables are usually out of the capabilities of tools using polyhedral representations. A significant body of work has been aimed at replacing polyhedra with alternative representations. For system with linear dynamics, support functions (given a closed convex set S its support function describes the signed distances of supporting hyperplanes of S from the origin) has so far proved to be the most scalable approach, leading to the tool SPACEEX, which was able to analyze, for instance, a complex 28-dimensional helicopter control system [Frehse et al. 2011]. When moving to systems with non-linear dynamics, more complex representation techniques are needed. The tool HSOLVER [Ratschan and She 2007] uses constraint propagation and abstraction-refinement techniques to approximate the non-linear system by a finite-state discrete model that is refined until an answer to the verification problem is found, or the maximum number of refinement steps is reached. Discretization is performed also by the tool HYCOMP, a model checker for hybrid systems based on Satisfiability Modulo Theories (SMT), which takes as input networks of hybrid automata specified using the HyDI symbolic language. HYCOMP relies on the encoding of the network into an infinite-state transition system, which can be analyzed using SMT-based verification techniques; it features specialized encodings of the automata network and can discretize various kinds of dynamics [Cimatti et al. 2015]. An alternative approach, which does not rely on abstractions, is to approximate the continuous evolution of the system by using Taylor sets or models (they over-approximate continuous and $k+1$ times differentiable functions by their Taylor polynomials of degree up to k bloated by an interval representing the remainder [Chen et al. 2012]). Two examples of tools using Taylor-based representations are FLOW* [Chen et al. 2013] and ARIADNE [Benvenuti et al. 2014]. Deductive verification, where a designer interacts with a mechanized theorem prover to generate proofs of correctness of systems, is an alternative approach that does not need to compute approximations of the reachable set. The tool KEYMAERA X [Fulton et al. 2015] applies deductive verification to analyze nonlinear hybrid systems symbolically by combining deductive, real algebraic, and computer algebraic prover technologies; it is particularly suitable for verifying parametric hybrid systems.

All the above tools have been proved to be robust enough to analyze relevant industrial case-studies. Some of them have also been applied to medical robotics systems. In particular, KEYMAERA X has been used to prove safety of a control algorithm designed to provide directional force feedback for a surgical robot [Kouskoulas et al. 2013], while ARIADNE has been used to study how the choice of the control parameters and the measurement error affect the safety of a puncturing task [Muradore et al. 2011; Bresolin et al. 2015].

3. A LASER INCISION CASE STUDY

Today many surgical interventions use lasers as a precision tool, due to their ability of performing fine ablation or cutting procedures, even at the microscopic scale [Mattos et al. 2011]. One such example is phonomicrosurgery, in which the laser is used as a scalpel for excising tumorous tissue in the larynx. Due to the precision of laser

incisions, surgeons can preserve more healthy tissue, which is of utmost importance for the quality of the surgery, since it reduces the recovery time and has a significant impact on patient's voice.

When biological tissue is irradiated by laser, different types of interaction may happen, depending on the power density and the duration of the laser pulse [Niemz 2007]. In phonomicrosurgery, CO_2 laser is typically used in long pulses or continuous wave mode, causing a thermal interaction with soft tissue. During the irradiation, the laser energy is absorbed by the tissue, raising its temperature and causing the water molecules to evaporate. This leads to micro explosions that result in tissue removal. This process is called *ablation by vaporization* [Fichera et al. 2015].

Vaporization is not the only thermal effect caused by CO_2 laser. At lower temperatures tissue may already suffer some reversible (e.g. hyperthermia) or irreversible (e.g. coagulation and necrosis) changes. However if the irradiation persists long enough, the temperature of the tissue surpasses $100\,^{\circ}C$, leading to *carbonization* of adjacent tissue. This phenomenon may be recognized by blackening of the tissue and it should be avoided as it extends the thermal damage to healthy tissue, increasing the patient healing time and decreasing the quality of the surgery [Fichera 2016].

In order to avoid carbonization, laser incisions are usually performed by rapidly steering the laser spot over the tissue surface, in such a way that the ablation at each point of the tissue occurs over repeated passes. This steering motion can be achieved by a scanning unit, usually composed of a motorized mirror with two degrees of freedom. Commercial robotic scanners like *AcuBlade* and *HiScan Surgical* are capable of repeatedly steering the laser spot over a predefined path (such as a straight line or a circular path). The use of such a robotic scanner increases the uniformity between passes, allowing the surgeon to concentrate only on reorienting the scan line and controlling the duration of the exposure, in order to achieve the desired depth of cut. Moreover, if the laser activation command is also integrated with the robotic scanner, the system is able to perform incisions completely autonomously.

Even though the surgeon must remain in control of the procedure, the possibility of performing elementary incisions autonomously is advantageous, as it increases the precision of the cut, while reducing the mental workload of the surgeon. Using an autonomous laser scanner, the surgeon could specify the desired shape and depth of the incision, while the system calculates the optimal scanning velocity and exposure time, based on the model of the tissue ablation and the parameters of the system.

In this work, we are interested in characterizing the autonomous incision of a straight line trajectory, using a robotic laser scanner. More specifically, we want to model the experimental setup used in Fichera et al. [2015], to allow validating the results of the formal verification with experimental data. Consequently, we need to model the robotic laser scanner and the laser-tissue interaction.

3.1. Robotic laser scanner

The experimental setup used in Fichera et al. [2015] is represented in Fig. 1. It is composed of a laser source (not shown), a delivery arm, a robotic scanner, and a microscope. The laser scanner consists of a motorized mirror, which reflects the laser beam coming from the delivery arm towards the target surface. The scanner is directly attached to the microscope, so that the target area is at the center of the microscope, providing good visualization of the ablation procedure.

The motorized mirror is a Fast Steering Mirror (FSM), S-334 from PI GmbH, with two orthogonal axes of rotation, θ_x and θ_y, often called tip and tilt degrees of freedom. Actuating the axes θ_x and θ_y allows changing the Cartesian position (x, y) of the laser spot over the target surface. Considering that the target surface does not move with respect to the scanner, the relationship between the motion of a single rotation axis θ_x

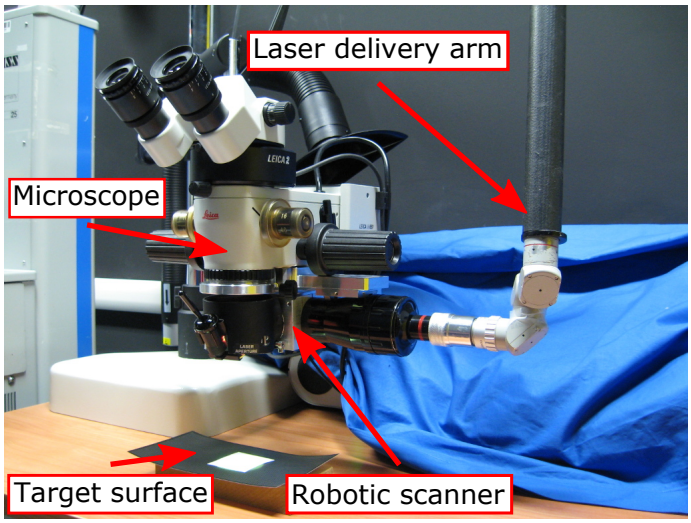


Fig. 1. Laser ablation setup with robotic laser scanner, used in [Fichera et al. 2015]

of the mirror and the displacement of the laser spot in the x direction is

$$x(t) = H \tan(2\theta_x(t)) \tag{1}$$

where H is the distance between the scanner and the target surface. Since the angular amplitude of the mirror is very small (less than $50\,mrad$), the paraxial approximation may be used, which gives

$$x(t) = 2H\theta_x(t). \tag{2}$$

Therefore the linear dynamics of the laser spot is defined by the angular dynamics of the mirror.

Each axis of the mirror is controlled by a differential piezo drive, which consists of two linear piezoelectric actuators controlled by complementary voltages. When the control voltage changes, one piezo expands and the other contracts, causing the mirror to tilt around its central point. Besides that, each piezo actuator is equipped with a strain gauge sensor, which allows controlling the motion of the mirror in closed loop. Since piezo actuators are very fast and do not show overshoot, their dynamics is typically modeled as a first-order transfer function with a very small time constant.

In order to ablate a straight line trajectory, only the axis of the mirror along the trajectory needs to be controlled. For that, a triangular wave is used as reference $x_{ref}(t)$, in order to keep the speed constant along the trajectory. This scenario may only lead to overshoots at the points where the speed of the mirror needs to be reversed, so the tracking accuracy of the system depends on the tilting frequency. In Fichera et al. [2015], the maximum frequency was 33 Hz, while the resonant frequency of the mirror is 700 Hz. Since the mirror is operated far below its resonant frequency, we can approximate the transfer function of the scanner and the controller as a constant value in our working conditions (i.e., infinite bandwidth), without impacting on the accuracy of the model.

3.2. Temperature Dynamics

To model the temperature dynamics of soft tissue under laser irradiation, we start assuming a fixed laser beam to make the analysis easier. Considering the surface of the tissue flat and the laser beam normally incident, we can define a cylindrical coordinate

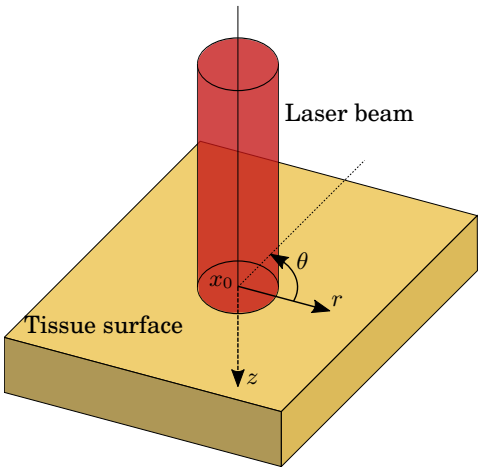


Fig. 2. Cylindrical coordinate system used to map the tissue surface

system $\{r, \theta, z\}$ on the surface of the tissue, centered at the position of the laser spot, as shown in Fig. 2. Due to radial symmetry of the laser beam, the θ coordinate can be omitted from the equations. In such case, the temperature gradient $\dot{T}$ of the tissue can be modeled as a superposition of two phenomena [Niemz 2007]:

(1) the heat deposition due to laser absorption S (W/m^3), and
(2) the heat diffusion $\triangle T$ over the tissue volume described by a second-order partial differential equation.

We end up with the following equation

$$\dot{T}(r, z, t) = \frac{1}{\rho c} S(r, z, t) + \kappa \triangle T(r, z, t), \tag{3}$$

where t is the time, ρ is the tissue density, c is the specific heat capacity, κ is the temperature conductivity and $\triangle$ is the Laplace operator. The solution of this equation is complex and is usually evaluated numerically, however an analytical solution can be obtained under certain assumptions.

Considering a Gaussian beam perfectly focused at the tissue surface, the heat deposition inside the tissue is described by Niemz [2007] as:

$$S(r, z, t) = \alpha I(r, z, t) = \alpha I_0 e^{-\left(\frac{2r^2}{\omega^2} + \alpha z\right)} e^{-\left(\frac{8t^2}{\tau^2}\right)}, \tag{4}$$

where I_0 is the beam intensity incident on the surface of the tissue, ω is the beam waist, α is the coefficient of absorption and τ is the duration of the laser pulse. If we further assume that the intensity of the laser beam is constant during the laser pulse, the time dependency of S can be dropped. For any given point (r, z) the heat increase due to laser absorption becomes constant. In particular, for the point $(r, z) = (0, 0)$, the heat increase is given by

$$S(0, 0) = \alpha I_0. \tag{5}$$

If we look only at the homogeneous part of Equation 3, which models the heat diffusion after the laser source is switched off, we obtain

$$\dot{T}(r, z, t) = \kappa \left(\frac{\partial^2}{\partial r^2} + \frac{1}{r} \frac{\partial}{\partial r} + \frac{\partial^2}{\partial z^2} \right) T(r, z, t), \tag{6}$$

which has the general solution

$$T(r,z,t) = T_0 + \frac{\chi_0}{(4\pi\kappa t)^{3/2}} e^{-\left(\frac{r^2+z^2}{4\kappa t}\right)}, \tag{7}$$

where T_0 is the temperature of the tissue before laser irradiation and χ_0 is an integration constant. This allows us to model the temperature decrease at any given point (r,z) of the tissue. For the point $(0,0)$, it can be seen that the temperature decreases according to a $t^{-3/2}$ law

$$T(0,0,t) = T_0 + \frac{\chi_0}{(4\pi\kappa)^{3/2}} t^{-3/2}. \tag{8}$$

The differential form of the Equation 8 is

$$\dot{T}(0,0,t) = -\frac{3}{2}\left(T(0,0,t) - T_0\right) t^{-1}, \tag{9}$$

which can be seen as an approximation of the heat conduction equation for the point $(0,0)$. Inserting Equations 5 and 9 into 3 yields the following differential equation:

$$\dot{T}(t) = \frac{\alpha I_0}{\rho c} - \frac{3}{2}\left(T(t) - T_0\right) t^{-1}. \tag{10}$$

If the laser source steers the laser spot over the tissue surface, the heat deposition is no longer constant. In particular, if the laser spot moves along a straight line trajectory, passing over the point x_0, the heat deposition at x_0 is given by

$$S(t) = \alpha I_0 e^{-\left(\frac{2(x(t)-x_0)^2}{\omega^2}\right)}, \tag{11}$$

where $x(t) - x_0$ is the distance between the center of the laser spot and the particular point x_0 under analysis. Incorporating this behavior in Equation 10 provides the complete temperature dynamics for a scanning laser

$$\dot{T}(t) = \frac{\alpha I_0}{\rho c} e^{-\left(\frac{2(x(t)-x_0)^2}{\omega^2}\right)} - \frac{3}{2}\left(T(t) - T_0\right) t^{-1}. \tag{12}$$

3.3. Ablation dynamics

When the temperature of a point x_0 at the surface of the tissue reaches $100\,^{\circ}C$, the tissue stops heating and vaporization starts. In this case, the rate of tissue ablation is given by

$$\dot{m} = \frac{1}{Q_{vap}} \dot{Q}, \tag{13}$$

where $\dot{m}$ is the evaporation rate of water inside the tissue, $\dot{Q}$ is the temporal change of heat in the volume of tissue being vaporized and the Q_{vap} is the enthalpy of vaporization of the water. As stated in the temperature dynamics, the heat variation is the difference between the laser absorption and the heat diffusion, however, since the temperature of the tissue remains constant during the entire vaporization process, it is correct to assume that the energy previously used for heating the tissue causes the vaporization. Therefore, according to a basic law of thermodynamics

$$\dot{Q} = m_h c \dot{T}, \tag{14}$$

where $\dot{T}$ is the temperature increase rate, given by Eq. 12, and m_h is the mass of the tissue undergoing such temperature variation.

Considering that the shape of the ablation crater can be well approximated by a 2D Gaussian [Fichera et al. 2015], the mass of the ablated region can be obtained by

$$m_h = 2\pi\sigma^2 z\rho_w, \tag{15}$$

where z is the depth of ablation, σ^2 is the variance of the Gaussian and ρ_w is the density of the water at $100\,^\circ C$. If we assume the variance of the Gaussian to be constant, the depth of cut increases linearly with the mass of evaporated water. Therefore inserting Eq. 14 and the derivative of Eq. 15 into Eq. 13 gives

$$\dot{z} = \frac{m_h c}{2\pi\sigma^2\rho_w Q_{vap}}\dot{T}. \tag{16}$$

This expression allows us to describe the ablation dynamics as a function of the temperature dynamics. Unfortunately, the proportionally constant cannot be physically obtained, since determining the variance of the ablation crater is not trivial, as it depends on many parameters of the laser beam. Also the mass m_h does not have a clear definition, as it corresponds to a volume of tissue that is completely heated when the vaporization starts. Therefore, we decided to use a different approach and to define this proportionality constant as a general parameter k_{cut}.

$$\dot{z}(t) = k_{cut}\dot{T}(t). \tag{17}$$

Then we obtained k_{cut} by using linear least squares fitting with the experimental data of Fichera et al. [2015].

The process of ablation continues until $\dot{T}(t)$ becomes negative or until all water molecules on the irradiated portion of the tissue have evaporated, in which case the temperature starts rising above $100\,^\circ C$, causing tissue carbonization. This condition can be modeled by defining a maximum depth z_{thr} that can be ablated in a single pass of the laser spot. There is little information in the literature about the ideal value for z_{thr}, since the start condition of the carbonization is usually not identified. We decided to use z_{thr} as three times the optical penetration of the laser beam, because this corresponds to the region in which 95% of the photons are absorbed. For a CO_2 laser, we have $z_{thr} = 30\,\mu m$.

4. MODELING WITH HYBRID AUTOMATA

We model the laser incision task by using the well known formalism of hybrid automata [Alur et al. 1995]. Intuitively, a hybrid automaton is a "finite-state automaton" with continuous variables that evolve according to dynamics specified at each discrete node.

Definition 4.1. A *hybrid automaton* is a tuple $\mathcal{A} = \langle \mathrm{Loc}, \mathrm{Edg}, X, \mathrm{Inv}, \mathrm{Dyn}, \mathrm{Eve}, \mathrm{Act}, \mathrm{Res}\rangle$ such that:

(1) $\langle \mathrm{Loc}, \mathrm{Edg}\rangle$ is a finite directed graph; the vertices, Loc, are called *locations* or *control modes*, and the directed edges, Edg, are called *discrete transitions* or *control switches*;
(2) X is a finite set of *continuous variables* representing the continuous state space of the system;
(3) each location $\ell \in \mathrm{Loc}$ is labeled by the *invariant condition* $\mathrm{Inv}[\ell]$ on X and the *dynamic law* $\mathrm{Dyn}\,[\ell]$ on $X \times X \times \mathbb{R}^{\geq 0}$ such that if $\mathrm{Inv}[\ell](\mathbf{x})$ is true then $\mathrm{Dyn}\,[\ell](\mathbf{x}, \mathbf{x}, 0)$ is true;
(4) each edge $e \in \mathrm{Edg}$ is labeled by an *event name* $\mathrm{Eve}\,[e]$, the *activation condition* $\mathrm{Act}\,[e]$ on X and the *reset relation* $\mathrm{Res}\,[e]$ on $X \times X$.

Table I. List of variables, where x_0 is the observation point.

Name	Description
x	Position of the center of the laser beam
v_x	Speed of the laser beam
T	Temperature at x_0
q	Exposure of x_0 to the laser beam (dimensionless)
z	Accumulated ablation depth at x_0 for the whole ablation procedure
z_i	Instantaneous ablation depth at x_0 related to half of a scan period

Table II. List of constants and parameters.

Name	Value	Description
L	$4.6\,mm$	Length of the line for the laser trajectory
V	$[4.94,\ 920]\,cm/s$	Modulus of the speed of the laser spot
R	$250\,\mu m$	Radius of the laser spot
x_0	$[0,\ 2.3]\,mm$	Observation point along the trajectory
T_0	$37\ ^\circ C$	Skin temperature
T_{evap}	$100\ ^\circ C$	Evaporation temperature
λ	$6825.5643\ s^{-1}$	Decay coefficient
μ	$6.03796 \cdot 10^5\ ^\circ C s^{-1}$	Exposure-to-temperature coefficient
k_{cut}	$1.78833087 \cdot 10^{-8}\ m/^\circ C$	Temperature-to-ablation coefficient
z_{thr}	$30\,\mu m$	Carbonization threshold for ablation

Table III. List of automata, where the related Figure number is shown along with the input/output (I/O) variables and input/output (I/O) events.

Name	Fig	I Var.	O Var.	I Events	O Events
Laser trajectory	3		x,v_x		*switch_left*, *switch_right*
Superficial exposure	4	x,v_x	q		*comes*, *leaves*
Superficial temperature	5	q	T	*stop_evaporating*	*start_evaporating*
Ablation depth	6	q	z, z_i	*start_evaporating*	*stop_evaporating*, *carbonize*

A *state* of a hybrid automaton $\mathcal{A}$ is a pair $\langle \ell, \mathbf{x} \rangle$, where $\ell \in \mathrm{Loc}$ is a location and $\mathbf{x}$ is an assignment of values to the continuous variables in X. A state $\langle \ell, \mathbf{x} \rangle$ is said to be *admissible* if $\mathrm{Inv}[\ell](\mathbf{x})$ holds.

The evolution of a hybrid automaton alternates *continuous* and *discrete* steps. In a continuous step, the location does not change, while the continuous variables change following the continuous dynamics $\mathrm{Dyn}\,[\ell]$ of the location. A discrete evolution step consists of the activation of a discrete transition $e \in \mathrm{Edg}$ that can change both the current location and the value of the state variables, in accordance with the reset function $\mathrm{Res}\,[e]$ associated to the transition. The interleaving of continuous and discrete evolutions is decided by the invariant $\mathrm{Inv}[\ell]$ of the location, which must be true for the continuous evolution to keep on going, and by the guard predicate $\mathrm{Act}\,[e]$, which must be true for a discrete transition e to be activated. Formally, a *trajectory* ξ of a hybrid automaton can be defined as a (finite or infinite) sequence $(\xi_i)_{i \geq 0}$ of continuous functions $\xi_i : [t_i, t_{i+1}] \to \mathrm{Loc} \times X$ such that $\mathrm{Dyn}[\ell](\xi_i(s), \xi_i(t), t-s)$ holds for all $t_i \leq s \leq t \leq t_{i+1}$, and both $\mathrm{Act}\,[e](\xi_i(t_{i+1}))$ and $\mathrm{Res}\,[e](\xi_i(t_{i+1}), \xi_{i+i}(t_{i+1}))$ hold for some $e \in \mathrm{Edg}$.

Multiple automata are able to communicate in the following way: if an edge e_1 in automaton $\mathcal{A}_1$ and an edge e_2 in automaton $\mathcal{A}_2$ have the same event name, they *synchronize* over that label. The requirement for synchronization is that only one automaton triggers the transition associated with its edge, i.e., only one automaton defines a corresponding activation condition. Another condition for the definition of a *composition* of automata is that only one automaton can define the dynamics of a given continuous variable.

The system to be modeled is composed by four automata, each related to the dynamics of a specific variable (or two variables closely coupled). The list of variables is

provided in Table I, while Table II collects all the constants used in the four automata. In particular, x_0 and V are considered *parameters*: constants for which an interval of independent values is explored in our analysis, in order to identify some properties of the resulting system.

Finally, Table III lists the automata with the related variables and events. Specifically, such table defines an *output variable* for an automaton as a variable whose dynamics is defined by the automaton. Conversely, an *input variable* is not defined by the automaton while still present in its definition. In a similar way, an *input event* for an automaton is an event which is not associated to a transition guard, meaning that the automaton relies on another automaton with a transition guard that triggers the event (for which the event would be an *output event*). This notation has been used in this table to make explicit the dependencies between automata, without the introduction of additional notation in the rest of the paper.

For any automaton, if invariants are not specified, they are assumed to be the complement of the guard activation conditions; in other words, the trajectory is allowed to remain in the location unless a transition is active.

Before describing each automaton in detail, we can summarize the behavior of the system as follows: the laser beam performs its trajectory, at a certain point reaching the observation point x_0. This situation translates into an increase of the exposure q, which causes the temperature T to start rising. When the temperature reaches 100 degrees, ablation starts, increasing z_i and consequently z. After the laser beam crosses x_0, the exposure reduces and ultimately the temperature starts decreasing: this stops the ablation and z_i returns to zero, while T returns to T_0.

Some modeling choices have been tailored to the tool that we used for verification: the C++ library ARIADNE. This library allows to describe automata with non-linear behavior, while computing conservative over-approximations of the reachability of the system. This later property is important in order to provide sound conclusions from the computed results, but at the same time makes the verification numerically more challenging. This implies that some simplifications of the dynamics were required, as explained in the first four Subsections, each one dedicated to a specific automaton. Subsec. 4.5 instead shows a concrete example of evolution obtained using ARIADNE and comments on the critical aspects of the adopted system model. Finally, Subsec. 4.6 discusses the improvements to the tool that were required by this specific class of problem.

4.1. Automaton for laser trajectory

The automaton that models the trajectory of the laser, shown in Fig. 3, requires one location only: such location is called *scanning*, where we set the dynamics for the node position x and its speed v_x. While the expression for the derivative of x is straightforward, a remark on the derivative of v_x is useful: we have modeled a constant value of the speed, which only changes sign due to resets (shown in Fig. 3 using the $\Rightarrow$ symbol). This is because we neglect the effect of acceleration and deceleration on the borders. Therefore the laser beam just scans in one direction or the opposite, with a constant speed modulus. The spatial domain for x is $[0, L]$, where $L = 4.6\,mm$. The scanning period P_{scan} is defined as the time required to perform a laser pass on both directions, i.e.,

$$P_{scan} = \frac{2\,L}{V}. \tag{18}$$

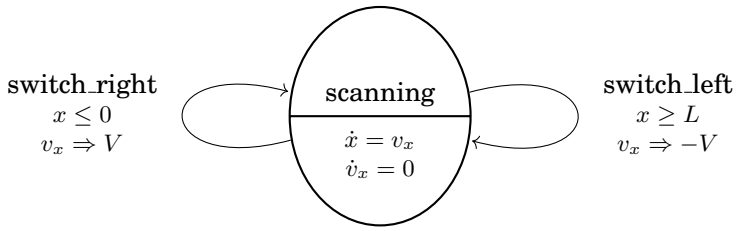


Fig. 3. The automaton for the laser beam position x and speed v_x.

4.2. Automaton for superficial exposure

The automaton for the superficial exposure q, shown in Fig. 4, is an auxiliary automaton which provides a measure of the incidence of the laser over the observed point x_0. The value of q ranges between 0.0 and 1.0, with a maximum when the laser is centered on x_0, and a minimum as soon as the distance is greater or equal to the laser beam radius $R = 250\,\mu m$. Therefore, two locations are present: the *far* one, where $||x - x_0|| \geq R$, and the *close* one, where $||x - x_0|| \leq R$. While q doesn't change in the *far* location, its expression in the *close* location needs some explanation.

From Eq. 11, we approximate

$$S(0,0,t) = \alpha I_0 e^{-\left(\frac{2(x(t)-x_0)^2}{\omega^2}\right)} \tag{19}$$

with

$$S(0,0,t) = \begin{cases} \frac{\alpha I_0}{2}\left(cos\left(\frac{\pi(x(t)-x_0)^2}{R^2}\right)+1\right) & , \text{ if } x(t)^2 \leq R^2 \\ 0 & , \text{ if } x(t)^2 > R^2 \end{cases} . \tag{20}$$

This implies that the spatial effect of the exposure to the laser beam is modeled as a raised cosine function:

$$q = \frac{1}{2} + \frac{1}{2}\cos\left[\pi\left(\frac{x - x_0}{R}\right)^2\right]. \tag{21}$$

In general, when dealing with a distance we use the squared expression because the norm function has numerical issues around zero: the norm function requires a square root, whose domain may partially fall into the negatives when overapproximations are involved. However, one could argue that since in this particular problem the distance is unidimensional, we are able to restore the original formulation by removing the square operator. While this is definitely correct, we kept the squared expression for numerical purposes: by squaring the expression, we also square the error. If the quantity is strictly lesser than one, as it is the case with q, such squaring is able to reduce the overapproximation error of some orders of magnitude. This choice is ultimately related to the current capabilities of the ARIADNE library and should not be considered a general guideline for handling this class of systems.

In order to use q later inside the expressions for $\dot{T}$, $\dot{z}$ and $\dot{z}_i$, it is necessary that we provide the expression for $\dot{q}$. Differentiating the raised cosine, we consequently obtain $\dot{q} = -\frac{v_x \pi}{R^2}(x - x_0)\sin\left[\pi\left(\frac{x-x_0}{R}\right)^2\right]$. This expression implies that x and v_x are both input variables for the dynamics of q.

Finally, it is interesting to comment on the impact of using an alternative formulation for Eq. 21. As already discussed, we chose to use the square of the norm of the distance since the square root operator is not numerically robust when the argument

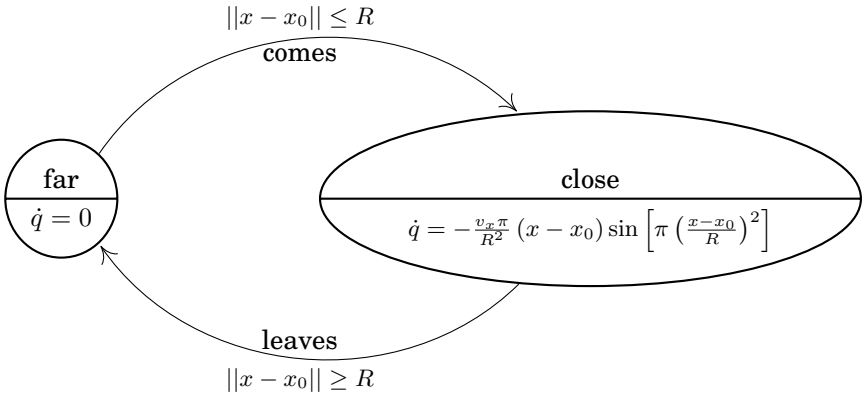


Fig. 4. The automaton for the superficial exposure q to the laser beam.

is close to zero and overapproximations are present. Since the reachable set includes such zero condition, it was necessary to fix the model accordingly.

4.3. Automaton for superficial temperature

The automaton for the behavior of the superficial temperature T is shown in Fig. 5. It includes two locations: *varying* and *evaporating*. The first location takes into account the positive variation due to laser incidence and the negative one due to cooling to the surface temperature T_0.

In regards to the negative term, we approximate Eq. 8 with

$$T(0,0,t) = T_0 + (T_f - T_0)\, e^{-\lambda t} \tag{22}$$

where T_f is the maximum temperature that the tissue achieves during the irradiation, typically $100\,^\circ C$. Consequently we approximate the term

$$-\frac{3}{2}\,(T(t) - T_0)\, t^{-1} \tag{23}$$

from Eq. 12 with

$$-\lambda\,(T(t) - T_0)\,. \tag{24}$$

The two contributions are characterized by the constants $\mu = 6.03796 \cdot 10^5\,^\circ C\, s^{-1}$ and $\lambda = 6825.5643\, s^{-1}$. The second location instead is such that the temperature is locked to $T_{evap} = 100\,^\circ C$. The transition to the *evaporating* location is regulated by the $T \geq T_{evap}$ condition, while the transition to the *varying* location is regulated by an input event *stop_evaporating* fired by the automaton in Fig. 6.

The approximation of Eq. 24 is motivated by the fact that accounting for the t^{-1} factor would have required an additional variable, with added complexity from the numerical viewpoint. In fact, the cooling effect does not have a significant impact to the dynamics when there is laser incidence, since it is dominated by the heating effect. When no incidence is present, we will show in Fig. 8 that the temperature transient on a given x_0 is completed a long time before x_0 is again exposed to the laser spot. In other words, the exact dynamics of cooling is not very relevant. Consequently, we deemed this simplification a reasonable compromise between accuracy and numerical complexity.

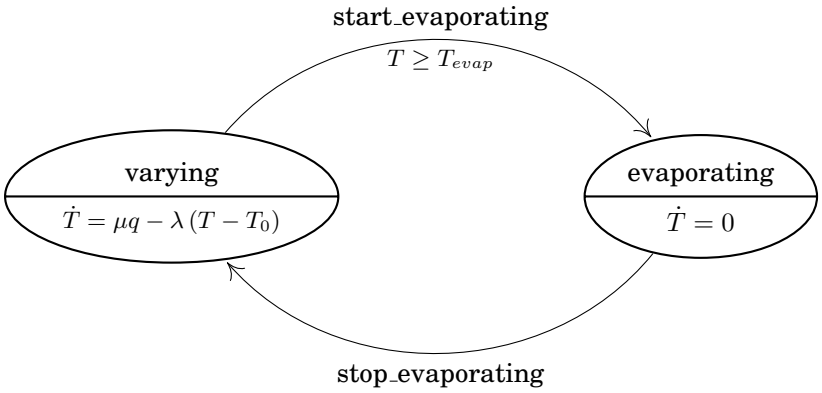


Fig. 5. The automaton for the superficial temperature T of the tissue on the chosen point.

4.4. Automaton for ablation depth

The automaton for the ablation depth regulates the dynamics of the accumulated depth z and its instantaneous value z_i. While the role of z is clear, z_i requires more explanation. Its value ideally represents the ablation-per-pass, under the assumption that a large ablation-per-pass triggers carbonization of the tissue. We work under the assumption that z_i should become zero when the pass has been completed: this may be modeled trivially if x_0 is far from the edge, since the laser crosses x_0, and one can identify well-defined beginning and end of the pass. However, the behavior becomes more complicated when x_0 is close to the edge of the linear trajectory: the laser beam will pass on x_0 twice in a rapid succession, compared to the case when x_0 is far from the edge. The temperature (and consequently the vaporization of the tissue and the resulting ablation) on the second pass will be influenced by the first pass, therefore there is no clear identification of the end of the first pass. In particular, if x_0 is very close to the edge, evaporation does not stop between the two consecutive passes and z_i continues to grow; let $x_{0,d}$ be the point where this situation starts occurring. If z_i were reset to zero as soon as evaporation stops, there would be a discontinuous behavior of z_i around $x_{0,d}$. Consequently, to account for that situation, the value of z_i needs to decay over time instead of being reset to zero in a discontinuous way. Hence the *idle* location where no ablation occurs, i.e. z does not vary, has an exponential decay for z_i to provide a continuous evolution towards zero. The *ablating* location instead has the same dynamics as T, but with a proportional constant $k_{cut} = 1.78833087 \cdot 10^{-8}\ m/°C$; please note that, since the temperature during evaporation is locked to T_{evap}, we substitute such value in the expression. In practice, we lock the temperature to $100\,°C$ and the energy that would otherwise increase the temperature is instead translated into ablation by means of evaporation. The transition between *idle* and *ablating* is triggered by the *start_evaporating* event produced by the superficial temperature automaton. On the other hand, the opposite transition happens as soon as $\dot{z} = 0$, i.e., there is no additional ablation; it is worth remarking that we must have $\dot{z} \geq 0$ at all times: a negative derivative would not be physically correct. This condition also means that $\dot{T} = 0$, therefore from now on the temperature will decrease. If the value of z_i is greater than a given threshold $z_{thr} = 30\,\mu m$, then carbonization occurs and we reach the *carbonization* location. We are not interested in the dynamics of such location, hence we provide an invariant set to *false* at all times, in order to stop evolution.

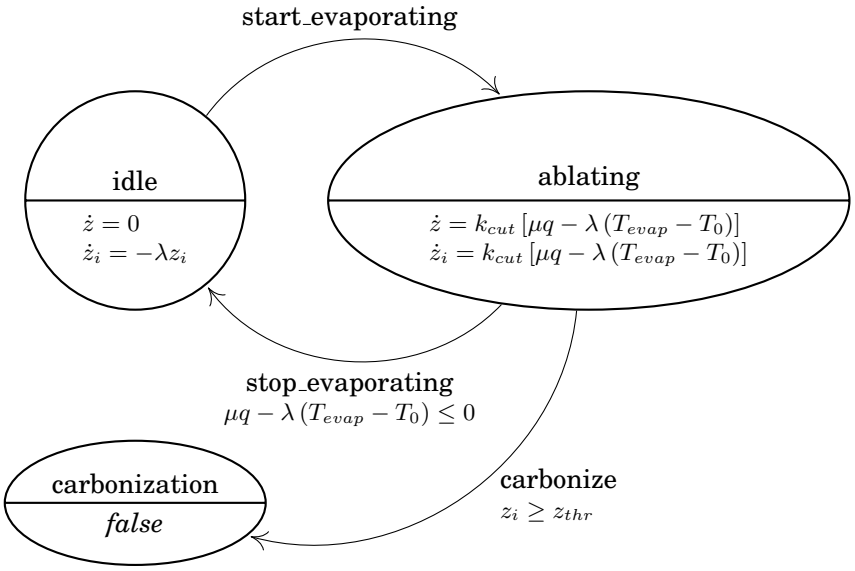


Fig. 6. The automaton for the accumulated ablation depth z and its instantaneous value z_i.

4.5. System evolution

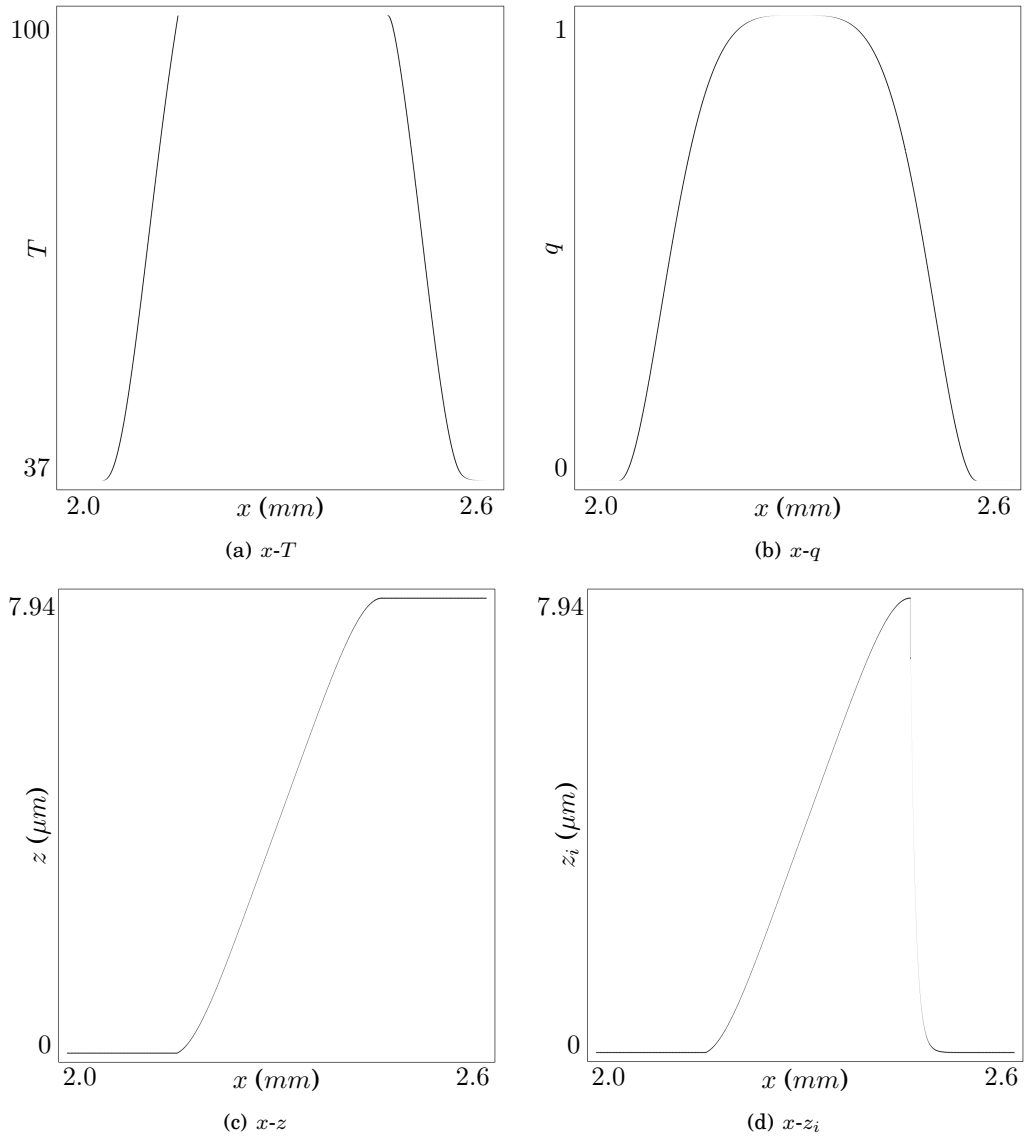
In this Subsection we provide an example of reached sets as computed by ARIADNE using the described models of hybrid automata and comment on the critical issues regarding the evolution of the system. In particular, we chose an initial set of $x = 0\,mm$, $v_x = V = 9.2\,cm/s$, $T = 37\,°C$, $q = 0$, $z = 0\,\mu m$, $z_i = 0\,\mu m$, meaning that a scan period $P_{scan} = \frac{2 \times L}{V} = 100\,ms$ is enforced. The initial locations are:

— *far*, for the superficial exposure automaton of Fig. 4;
— *varying*, for the superficial temperature of Fig. 5;
— *idle*, for the ablation depth of Fig. 6.

In addition, we chose an observation point of $x_0 = 2.3\,mm$, namely the center of the trajectory. However, we want to compute the result of half a scan period, focusing on the pass in the forward direction only; consequently, we evolve the system for a maximum time of $P_{scan}/2 = 50\,ms$. In Fig. 7 the reached sets projected on T, q, z and z_i are shown as a function of x. In particular, the plots are centered on x_0 with a radius of $0.3\,mm$ for improved readability, since there would be no perceivable difference in the rest of the x interval.

The "missing lines" in Figs. 7(a)-7(b) are due to negligible line widths, which are in turn caused by a very low width of the set compared to the scale of the y axis. In particular, in the central part of Fig. 7(a), and at the extremes of Fig. 7(b), the trajectory is exactly constant (to $100\,°C$ and $0\,°C$, respectively), meaning that the width of the set in the y direction is zero.

Fig. 7(b) shows that the exposure rises when approaching x_0 from the left. The temperature reacts accordingly, until $T = 100\,°C$ is reached. At that point, T is locked while evaporation occurs; the z and z_i variables increase. After the laser is sufficiently far from x_0, the temperature drops and evaporation stops, along with the increase of z and z_i. While z maintains its value, z_i drops rapidly to reach zero again.



(a) x-T (b) x-q

(c) x-z (d) x-z_i

Fig. 7. An example of reached sets after evolution for half a laser pass, around $x_0 = 2.3\,mm$.

For completeness, the event trace for a full scan period, according to the given initial conditions, would be: *comes*, *start_evaporating*, *stop_evaporating*, *leaves*, *switch_left*, *comes*, *start_evaporating*, *stop_evaporating*, *leaves*, *switch_right*.

In the following we comment on the performance of the tool along with the most critical aspects regarding reachability computation for this problem.

First, we can state that the ARIADNE running time for evolution of the system for 1 scan period is around one minute on a high-end laptop computer. Such result represents an average, since it actually depends on the evolution time step: as the step is tuned to be inversely proportional to the evolution gradient in order to control the over-approximation error, the running time increases as P_{scan} decreases. More precisely, a

lower P_{scan} translates into a higher V and consequently a higher $\dot{q}$, the latter influencing $\dot{T}$, $\dot{z}$ and $\dot{z}_i$.

The most critical part of the evolution from the numerical viewpoint is associated with temperature variation. Consequently, overapproximation error has a significant tendency to increase when the temperature automaton of Fig. 5 is in the *varying* location, in particular when the exposure automaton of Fig. 4 is in the *close* location. The error however is reset to zero as soon as the temperature automaton reaches the *evaporating* location, hence it does not accumulate indefinitely during the evolution.

Another problem is associated with the condition for the end of evaporation. In practice, there is a Zeno effect after the *stop_evaporating* event in Fig. 6 is produced, by which the system would be allowed to jump from the *idle* to the *ablating* locations indefinitely in zero time. This problem is intrinsic to the provided models and we were unable to rewrite the system to avoid it without also modifying the behavior in terms of continuous reachability. ARIADNE is designed to mitigate such issues numerically by evaluating second order derivatives of the dynamics for guard crossing, but still these situations turn out to be critical in terms of overapproximation error.

One could argue that the guards in 4 introduce the same issue and that we should have modelled the guard for either the *comes* or *leaves* transition using strict inequality. First, the numerical framework of ARIADNE works on the assumption that testing for equality is undecidable in general, hence strict inequality is not allowed. Second, this case is easier to handle numerically when the second order derivatives are considered. As a result, spurious transitions are never triggered in this particular case.

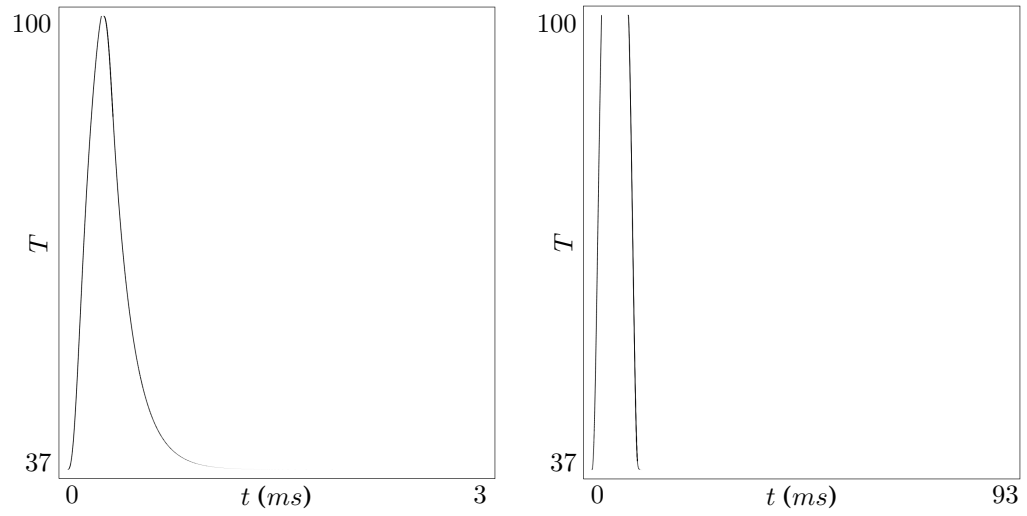
4.6. Improvements to ARIADNE

The numerical analysis of the described model required the introduction of some improvements to ARIADNE. More specifically, it was necessary to address two main problems:

(1) Handle the growing approximation error when the trajectory converges to a fixed value for some variables;
(2) Fix the implementation of guard evaluation for "spheric" guards.

The first problem arises from the numerical rounding error becoming dominant over time in respect of the set width on a given dimension. Such problem is relevant in the case study of this paper, as shown for example in Fig. 7(a) where it can be seen that T is bound to converge to either $100\,°C$ or $37\,°C$ during half a laser pass. The issue of controlling the rounding error was addressed by using a simple *reconditioning* scheme where the set is overapproximated by its bounding box (and consequently simplified) as soon as the dynamics becomes *contractive*. This approach, while apparently coarse, works well with trajectories with radii approaching zero: while the simplification of the set has negligible impact on the representation quality and on the overapproximation error, it allows for the error itself to shrink over time and also it improves the efficiency of the procedure.

The second problem was related to the fact that ARIADNE, prior to this case study, worked under the assumption that a guard does not "fold" over itself, but it is more akin to a barrier which is intersected only once by a crossing set. This is definitely not the case for the guard related to the distance to x_0 in Fig. 4: if the integration step of the evolution procedure is large enough, the evolution set is able to enter and leave the activation set of the guard in one step. This event resulted in an incorrect handling of the transition, which was identified as *inactive*. Such situation of missing a "spheric" guard represents a corner case, since the integration step would usually be sufficiently



(a) $6\,ms$ (b) $186\,ms$

Fig. 8. Evolution of temperature for half a pass period, for $P_{scan} = 6\,ms$ (a) and $P_{scan} = 186\,ms$ (b).

small to avoid the issue. Still, our formal verification approach mandates to capture all behaviors regardless of numerical aspects. Consequently we fixed the implementation to detect this particular situation and handle the transition correctly.

5. FORMAL VERIFICATION

The objective of this Section is to use ARIADNE to compute reachability in a numerically conservative way and use the obtained results to identify some properties of the modeled system.

First, a basic property that will be used throughout the remaining of this Section is the superposition of effects related to ablation passes. Fig. 7 showed that the transients for the T, z and z_i variables are practically confined to a small space interval compared to the line length L. However, those results were obtained for a specific $P_{scan} = 100$ ms. In Fig. 8 we provide the results for two values of the laser scan period, namely 6 ms and 186 ms, which will be shown in the following to be the bounds for the P_{scan} values that allow evaporation (at least 6 ms) while simultaneously avoiding carbonization (at most 186 ms). The initial set was $x = x_0 - R$ (i.e., the laser spot starts reaching x_0 from the left), $T = 37\ ^\circ C$, $q = 0$, $z = 0\,\mu$m, $z_i = 0\,\mu$m, with $v_x = 153.33$ cm/s in the $P_{scan} = 6$ ms case, and $v_x = 4.94$ cm/s in the $P_{scan} = 186$ ms case. The initial locations are *close* for the superficial exposure automaton, *varying* for the superficial temperature automaton and *idle* for the ablation depth automaton. The evolution time is equal to $P_{scan}/2$, which is the time required for the laser spot to reach again x_0. We clearly see that the temperature transient is completed by the time that half a pass is performed; more specifically, we obtained an (overapproximated) result of $37.000001\ ^\circ C$ in the first case, and a temperature difference $< 10^{-6}$ in the second case.

Since the modeled dynamics for T, z and z_i do not depend on z, each scan period (i.e., a full back and forth movement of the laser beam) results in an independent contribution to z. In other terms, we can perform formal verification for a single scan period in order to state properties of the ablation procedure for multiple periods.

In the following, we will identify the conditions under which we can provide a *safe*, *effective* and *efficient* ablation procedure. Safety in this context means to avoid car-

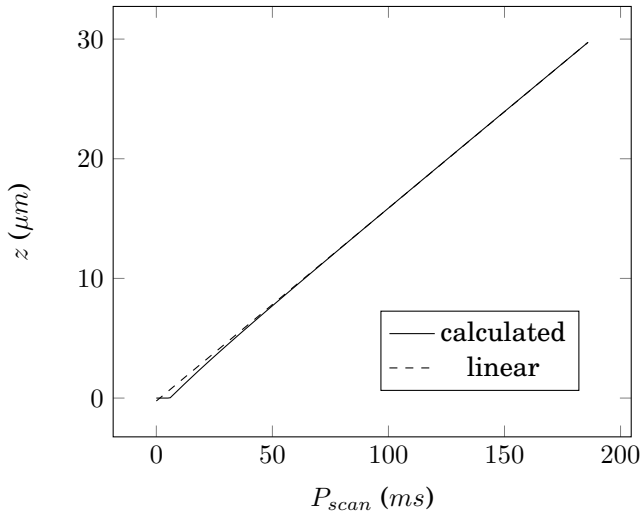


Fig. 9. Dependency of z for one scan period P_{scan}, compared to a linear approximation.

bonization for all points in the laser trajectory. Effectiveness relates to the quality of the ablation along the trajectory, i.e., to have a precise and homogeneous ablation depth. In particular, we want to reach a specified *target depth* D at the end of the incision procedure for all points in the trajectory. Finally, efficiency relates to the speed of the procedure in terms of the scanning period of the laser beam that can be used. The properties have been specified as conditions on the set of reachable states, and then verified by analyzing the evolution of the system computed by ARIADNE. Safety is formalized by defining a safe set of states and then checking if the reachable set is contained in it. Effectiveness and efficiency are reachability properties defined by related optimization measures on the continuous variables at the end of the ablation procedure. In all cases, the properties are checked for the entire range of parameter values, and the answer obtained by the tool is either a range of good values for the parameters (safety) or a value that maximizes/minimizes some performance measure (effectiveness and efficiency).

These measures are closely related to each other. In particular, restricting to a safe behavior provides a hard limit on the laser speed. For reasons of clarity of presentation, we will start by discussing the efficiency aspect, and then move to safety and effectiveness. A final Subsection will compare the data obtained with ARIADNE vs. the results shown in Fichera et al. [2015], collected using a real prototype of the system, to validate our analysis against the data measured on the physical system. In particular, the choice of D is provided by the aforementioned reference Fichera et al. [2015].

5.1. Efficiency

The efficiency objective is to minimize the time to reach a specified depth D. We call such time the *total incision time* P_{tot}.

Since we need to have an integer number of scan periods N, the relation $P_{tot} = N \times P_{scan}$ holds, where we remind here that P_{scan} comes from Eq. 18. Hence, efficiency can be formalized as the problem of finding the values of N and P_{scan} that minimize P_{tot} and guarantee that the depth z at the end of the ablation procedure is close to D.

The property is tested by analyzing how the depth z varies with respect to the scan period P_{scan}. We consider one single scan period ($N = 1$) and a range of P_{scan} from $1ms$

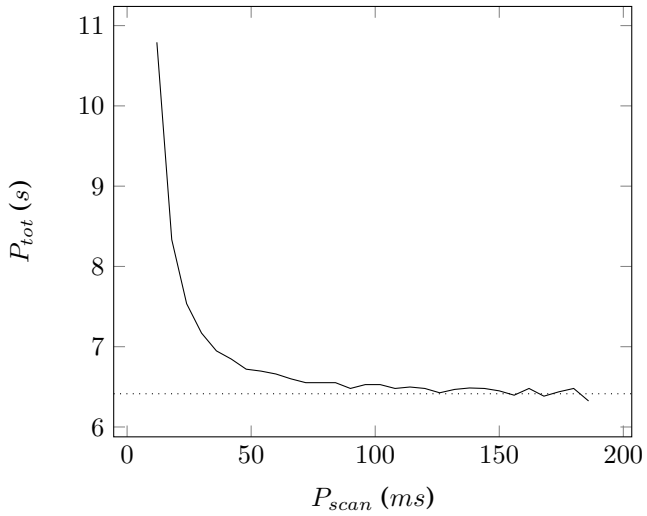


Fig. 10. Total incision time P_{tot} as a function of the scan period P_{scan}, where the dotted line identifies $P_{tot} = 6.4\,s$.

to $186ms$. Since, as we already observed, a single scan is sufficient to state properties of the entire ablation procedure, we do not loose generality by considering only $N = 1$. The range of P_{scan} has been obtained by the safety checking procedure, and it is formally guaranteed to avoid carbonization for all points in the laser trajectories. The initial values are $x = 0$, $T = 37\,^{\circ}C$, $q = 0$, $z = 0\,\mu$m, $z_i = 0\,\mu m$, with $v_x = 920\,cm/s$ in the $P_{scan} = 1\,ms$ case, and $v_x = 4.94\,cm/s$ in the $P_{scan} = 186\,ms$ case. The initial locations are *far* for the superficial exposure automaton, *varying* for the superficial temperature automaton and *idle* for the ablation depth automaton.

The results shown in Fig. 9 refer to a point of observation x_0 equal to $x_{mid} = 2.3\,mm$, i.e., the midpoint of the linear trajectory of the laser. We can see that the dependency is almost linear for high values of P_{scan}. This allows us to conclude that for high values of P_{scan}, we will obtain the same total incision time. It is also worth noting that the minimum value of P_{scan} that triggers vaporization is $P^m_{scan} = 6\,ms$ (using a granularity of $1\,ms$), for which we have a depth-per-pass of $29.7842\,nm$. This turns out to be exactly 3 orders of magnitude lower than the depth for the maximum scan period used, which reads $z = 29.7306\,\mu m$.

Fig. 10 shows the value of P_{tot} as a function of $P_{scan} > P^m_{scan}$, for $D = 1040\,\mu m$. Such target depth value, which will be used in the rest of this Section, stems from the results presented in Fichera et al. [2015]. To obtain the plot, for each value of P_{scan} the corresponding N has been calculated as the minimum number of passes *plus one* that yielded $z > D$, which means N is rounded downwards for safety reasons. The irregular behavior is due to the inaccuracy introduced by such rounding. We can see that P_{tot} decreases in average as P_{scan} increases, converging to a value of $\approx 6.4\,s$, identified by the dotted line in Fig. 10.

On the other hand, for $P_{scan} \to 0$, we have that $P_{tot} \to \infty$: if the laser moves too fast, then it is not able to raise the temperature to T_{evap} and consequently vaporization does not start, yielding no ablation at all. Compared to Fig. 9, we show the values from $12\,ms$ to $186\,ms$, since $P_{tot}|_{6\,ms} = 209.502\,s$ would have made the remaining data in the graph less readable.

Consequently, we can say that a high value of P_{scan} is desired in order to obtain an efficient procedure. Moreover, such behavior is independent of D: given the superposi-

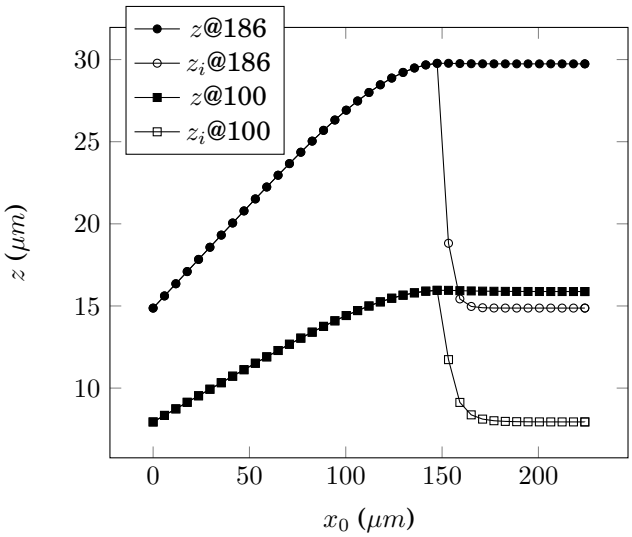


Fig. 11. Behavior of $z(x)$ and $z_i(x)$ according to the point of observation x_0, after one scan period at $P_{scan} = 186\,ms$ or $P_{scan} = 100\,ms$.

tion of effects for consecutive scannings discussed at the beginning of this Section, it is clear that if we chose $D' = 2\,D$ the curve would have $P'_{tot} \approx 2\,P_{tot}$ values, where the approximate equality stems from the rounding noise explained earlier.

5.2. Safety

The results of the previous Subsection did not give us information about the spatial distribution of z, since it was focused on the midpoint of the trajectory, where border effects are not present. To guarantee safety, instead, we need to avoid carbonization at any point along the trajectory. This property can be formalised by defining as *safe set* the set of states such that the automaton in Fig. 6 is in a location different from *carbonization*, and then finding the values of P_{scan} such that, for all possible observation points x_0, the approximation of reachable set computed by ARIADNE is contained in the safe set.

Thus, the formal verification of the safety property requires an iterative search over both the scan period P_{scan} and x_0. Before giving the details on how this search is performed, we concentrate on two specific values of P_{scan}, namely $186\,ms$ and $100\,ms$, and we perform a full scan while changing the observation point x_0. The initial values are $x = L$, $T = 37\ ^\circ C$, $q = 0$, $z = 0\,\mu m$, $z_i = 0\,\mu m$, with $v_x = -9.2\,cm/s$ in the $P_{scan} = 100\,ms$ case, and $v_x = -4.94\,cm/s$ in the $P_{scan} = 186\,ms$ case. The initial locations are *far* for the superficial exposure automaton, *varying* for the superficial temperature automaton and *idle* for the ablation depth automaton.

Fig. 11 shows the behavior of z and z_i in the $[0\,\mu m,\ 230\,\mu m]$ interval for x_0, which corresponds to the 5% of the range of the linear trajectory closer to the edge. As we can see, near the edge the values of z and z_i match, because z_i is not allowed to decrease: the region is always under significant incidence of the laser (i.e., q is close to 1). At the same time, however, the closer we are to the edge, the less ablation we obtain: this is because at the edge, the laser beam performs the exact equivalent of one pass in a scan period, while far enough from the edge the laser beam performs one pass for each direction, hence two passes per scan period. Between those two behaviors, the two passes "overlap" in an almost linear fashion. After reaching a maximum value, z_i

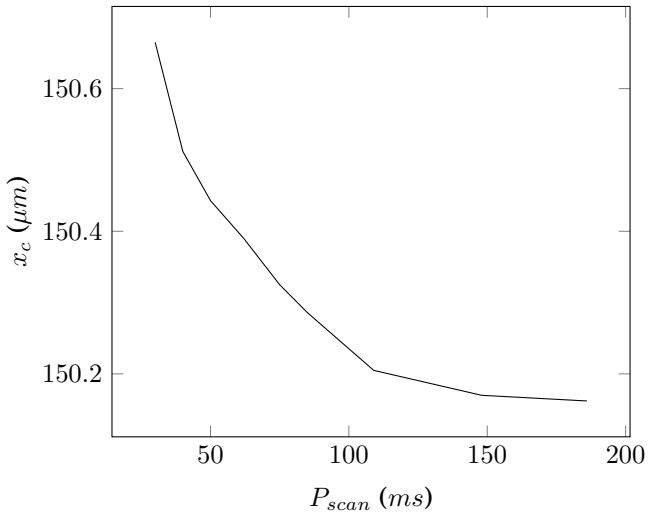


Fig. 12. Dependency of the critical point x_c over P_{scan}.

decreases (to half of z) rapidly with x_0, since far from the edge the value of z is the sum of the values of z_i due to the two separate passes.

It is interesting to note that the behavior of z is not monotonic over this interval of x: there exists a critical point x_c for which a maximum value of z is obtained. This value of z represents an *overshoot* compared to the value of z very far from the edge; it is also the maximum value attained by z_i before dropping to half of z. Such overshoot, however comparatively small, can be seen in Fig. 11 around $x_0 = 150\mu m$. We can calculate the overshoot as

$$\frac{z(x_c)}{z(x_{mid})} - 1 \tag{25}$$

where x_{mid} can be safely considered as lying far from the edge. The overshoot decreases as P_{scan} increases, for example from 0.91% at $P_{scan} = 100\,ms$ to a value of 0.47% at $P_{scan} = 186\,ms$. Smaller values of P_{scan} yield sensibly larger overshoots, providing us with the following conclusion: a very fast scan period introduces significant differences in the depth of incision. While the reduction of depth at the edge is reasonable, the overshoot should be kept as limited as possible, meaning that P_{scan} should be as high as possible.

The value of x_c is also a function of P_{scan}, as can be seen from Fig. 12: as P_{scan} increases, the critical point slightly moves towards the edge, converging to a value around $150.16\,\mu m$. Since the range of x_c values covers around 0.1% the laser beam radius R, the impact of this effect is very limited.

Anyway, the analysis of two specific values for P_{scan} is not sufficient to formally guarantee safety of the ablation procedure. Indeed, finding the maximum allowed scan period P^M_{scan} requires an iterative search over x: we start by choosing a reasonable interval for x and a sufficiently high value for P_{scan}, then we find the maximum of z_i over one scan period, while changing the value of x_0 within the interval to identify the corresponding x_c. If the maximum is below $z_{thr} = 30\,\mu m$, then no carbonization occurs and we can safely increase P_{scan}. The procedure stops when the scan period causes carbonization. Using a granularity of $1\,ms$, we found that $P_{scan} = 186\,ms$ is the maximum period which guarantees safety. This scan period was found at $x_c =$

$[150.166\,\mu m, 150.172\,\mu m]$, giving a depth of $z_i = 29.8867\,\mu m$. The corresponding value for z_i at the midpoint is $14.8717\,\mu m$, with z twice that value, i.e., $29.7434\,\mu m$.

It is important to underline that x_c is expressed as an interval due to the fact that we explore the x_0 space in a rigorous way. Such exploration is performed by splitting the $[0\,\mu m, 230\,\mu m]$ interval into sub-intervals, followed by analyzing the set of systems that result from using such sub-intervals as values for the x_0 parameter. Consequently, the identification of the critical point (and the corresponding P^M_{scan}) could not have been performed using a simulation tool, since a formally correct result in the absence of a numerically conservative interval calculus would have required an infinite accuracy.

5.3. Effectiveness

Effectiveness deals with the quality of the incision procedure. Ideally we want to obtain the same depth of incision for all points in the trajectory, which must be as close to D as possible. This is a *reachability property* on the model: the value of variable z (accumulated ablation depth at x_0) at the end of the scan passes should be equal to D for all observation points x_0. As shown in the previous Subsections, a homogeneous value of z for all x is not possible due to border effects. Hence, we will define a measure of the "closeness to D" of the ablation depth (Eq. (27)) and find the value of P_{scan} that maximises it. Also, we need $P_{scan} \geq 6\,ms$ in order to trigger evaporation. Finally, due to the restriction to an integer number of scan periods N, only discrete values of total incision depth can be achieved. In particular, we choose N such that $N + 1$ passes reach a depth of $D = 1040\,\mu m$ for the critical point in the trajectory. This is similar to the procedure used to obtain P_{tot} in Fig. 10, where we computed the results at the midpoint of the trajectory.

Let us focus on $P_{scan} = 186\,ms$ for now. We perform two evolutions for one pass period, choosing $x_0 = x_c$ in the first case, and $x_0 = x_{mid}$ in the second case. The initial values are $x = L$, $v_x = -4.94\,cm/s$, $T = 37\ ^\circ C$, $q = 0$, $z = 0\,\mu m$, $z_i = 0\,\mu m$. The initial locations are *far* for the superficial exposure automaton, *varying* for the superficial temperature automaton and *idle* for the ablation depth automaton.

For these conditions after a pass period we obtain $z(x_c) = 29.8867\,\mu m$ and $z(x_{mid}) = 29.7434\,\mu m$ respectively. Hence, we need a minimum of

$$N = \lfloor D/\left(z(x_c)\right)\rfloor = \lfloor 1040/\left(29.8867\right)\rfloor = \lfloor 34.7980\rfloor = 34 \tag{26}$$

periods before stopping the incision procedure. At the critical point, we have a total $z = N \times 29.8867\,\mu m = 1016.1478\,\mu m$, i.e., 97.7% of the ablation target; at the midpoint we have a total $z = N \times 29.7434\,\mu m = 1011.2756\,\mu m$, which is 97.2% of D. This fact suggests that the maximum allowed scan period is not necessarily the optimal period in terms of ablation.

In general, we define the ablation ratio

$$\rho_a = \frac{N\,z(x_{mid})}{D} = \left\lfloor \frac{D}{z(x_c)} \right\rfloor \frac{z(x_{mid})}{D} \tag{27}$$

as a measure of closeness to the target depth D. It holds that $\rho_a < 1$ by construction, but we desire a value as close to 1 as possible. Since N is a function of P_{scan}, we want to find the value of the scan period $P^{opt}_{scan} \leq P^M_{scan}$ such that ρ_a is maximized.

Figure 13 shows the behavior of ρ_a while varying P_{scan}. As we can see, the rounding of $\frac{D}{z(x_c)}$ to an integer N causes jaggedness. In particular, we obtain higher values of ρ_a when $\frac{D}{z(x_c)}$ is closer to an integer value (with respect to the rounding downwards operation). It holds that, for a sufficiently low P_{scan}, the overshoot (which increases as P_{scan} decreases) prevents ρ_a from reaching relatively high values. We searched sys-

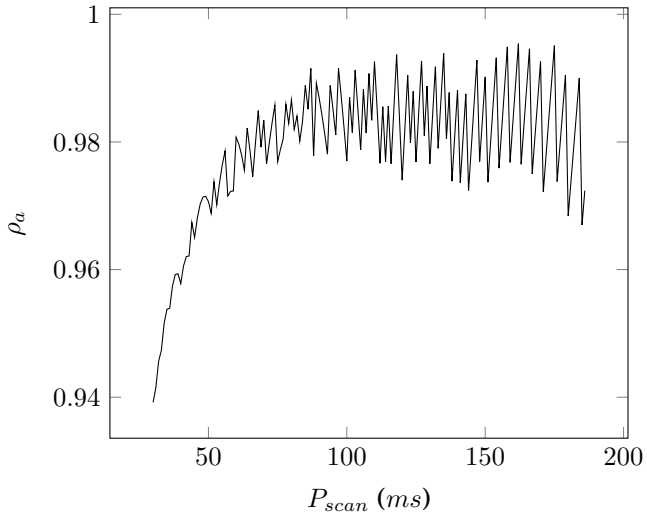


Fig. 13. Value of ρ_a as a function of P_{scan}.

Table IV. Experimental results obtained in Fichera et al. [2015]. For each scanning period (P_{scan}) and total incision time (P_{tot}), values indicate the mean (d), standard deviation (σ) and coefficient of variation (c_v) of the depth of cut measured at the center of the scan line.

P_{tot} (s)	P_{scan} (ms)	d (mm)	σ (mm)	c_v (%)
3	30	0.50	0.064	12.91
	50	0.63	0.037	5.90
	100	0.86	0.073	8.54
4	30	0.52	0.028	5.40
	50	0.77	0.056	7.32
	100	0.75	0.041	5.60
5	30	0.65	0.030	4.57
	50	0.69	0.045	6.69
	100	0.78	0.065	8.40
6	30	0.59	0.066	11.27
	50	0.72	0.081	11.27
	100	1.04	0.072	6.99

tematically all the values of P_{scan} from $186\,ms$ to $30\,ms$, finding a maximum ρ_a of 0.9951 at $P_{scan} = 175\,ms$.

5.4. Consistency

In order to prove the validity of the proposed model, it is important to verify the consistency of the obtained data with the data from the physical system. In Fichera et al. [2015], several incisions were performed while changing the scanning period P_{scan} and the total incision time P_{tot} and measuring the obtained depth of cut for points close to the center of the scan line. The values used for P_{scan} were $\{30,\ 50,\ 100\}$ ms and for P_{tot} were $\{3,\ 4,\ 5,\ 6\}$ s. For each of these 12 combinations, 9 repeated trials were performed, resulting in 108 incisions. Table IV shows the mean depth of cut for each combination $\{P_{tot},\ P_{scan}\}$, as well as the standard deviation and the coefficient of variation of the data.

Using ARIADNE, we calculated the expected depth of cut for these same experimental conditions. It is important to note that for all combinations $\{P_{tot},\ P_{scan}\}$ the cor-

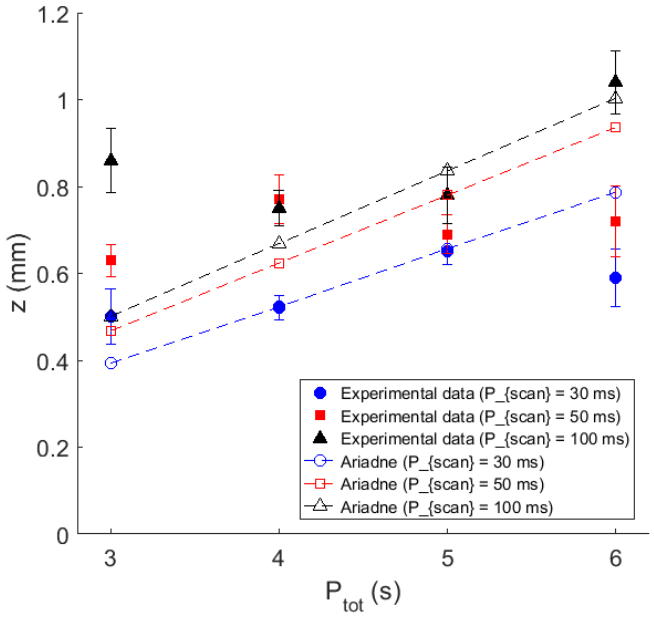


Fig. 14. Comparison between ARIADNE results and the experimental data from Fichera et al. [2015].

responding number of passes N is integer, except for the cases $\{4,\ 30\}$ and $\{5,\ 30\}$. To keep the number of passes integer, these combinations were adapted to $\{3.99,\ 30\}$ and $\{5.01,\ 30\}$ respectively. The comparison between ARIADNE's results and the experimental data is represented in Fig. 14. As we can see, the results obtained with ARIADNE are linear, because our model assumes that, keeping all parameters constant, the depth of cut per scanning period is always the same. We can also see that higher values of P_{scan} provide higher depths of cut, but this effect is less significant for high values of P_{scan}.

In the experimental data, it is also possible to see that the depth of cut grows with P_{scan}, however the relationship between z and P_{tot} is much less linear. This is due to the high variance of each experimental condition, which can be seen by the error bars shown in the graph. Computing the distance between ARIADNE's predicted depth of cut and the experimental results, we obtain a normalized mean square error of 5.04%. Considering that most experimental conditions present a coefficient of variation higher than 5%, we can affirm that the discrepancy between the obtained results is within the variance range of the experimental data, therefore ARIADNE's results are consistent with those of the real system.

It is also important to understand why the experimental data presents higher variance than the model implemented in ARIADNE. This is because of many simplifications that had to be done in the modeling of the physical system. First of all, the power of the laser was assumed to be constant, even though the power of a commercial laser system may fluctuate over time. Next, we assumed the laser spot to be perfectly focused at the tissue surface, regardless of the current value of z. In a real scenario, the focal length of the optical system is kept constant, which means that when z increases, the laser spot starts getting out of focus, which reduces the energy density on the point under analysis, while deforming the shape of the ablation crater. Additionally we assumed the laser beam to be always orthogonal to the tissue surface, due to the paraxial approxi-

mation, and the intensity profile of the laser beam to be perfectly Gaussian, ignoring any kind of electromagnetic interference and mechanical misalignments.

The mathematical representation of the tissue also included some simplifications. First, the tissue was assumed to be completely uniform. Even though the experiments in Fichera et al. [2015] are performed in Agar-based gel, which is more uniform than real biological tissue, complete uniformity is hard to be obtained. Afterward, the properties of the tissue, such as the density and the coefficient of absorption, were considered constant during the entire ablation procedure, even though these parameters may change with the temperature. Second, the interaction between the laser and the tissue was considered to be completely absorbent, ignoring scattering of photons. Finally, the tissue surface was assumed to be infinite, so that the heat diffusion equation does not need to account for any border effects. Considering all these facts, the proposed model does not account for all the complexity of a real laser ablation procedure. Nevertheless, since the obtained results are still consistent with the experimental data, it is then possible to affirm that such simplifications have little impact on the usefulness of the model.

6. CONCLUSIONS AND FUTURE WORK

In this paper we discussed the application of formal methods to medical robotic systems. To demonstrate the value of formal modeling and verification, we analyzed the model of a robotic laser scanner to identify the conditions under which it can provide a safe, effective and efficient ablation procedure. To prove that the ablation procedure respects the desired properties, we modeled the system by using hybrid automata. Then we exploited the reachability analysis capabilities of the tool ARIADNE to investigate how the values of significant parameters (the scan period and the number of scan periods) affect safety, effectiveness and efficiency of the ablation procedure. A comparison of our verification results with the experimental data from Fichera et al. [2015] shows that the proposed model and methodology is consistent with a physical prototype of the system.

In this paper, formal verification has been focused on varying one specific parameter, namely x_0, while in general a multi-parameter exploration would be desirable. For example, the P_{scan} parameter has been analyzed with a granularity of $1\,ms$ instead of finding the boundary values in the continuous space. Still, we deemed this simplification reasonable since a hardware implementation of the scanner would ultimately be limited to discretized values anyway. Two additional elements of complexity are the use of intervals for constants and a non-empty initial set, meaning that we analyze a family of behaviors of the system. The first one would have been a feasible extension of the model, however it would have required an additional analysis of the physical prototype to identify ranges for constants. The second addition instead would have been of little consequence: we have exact knowledge of the initial conditions for z, z_i and q, while an inaccuracy on the value of T is rapidly absorbed by the temperature dynamics; finally, an initial indetermination in the x position is not particularly useful if the variable evolves by scanning all its range anyway. As a final comment, we did not introduce non-determinism due to non-urgent guards since no correspondence in the physical system was recognized.

In general, the inclusion of any interval-based extension to the model is not trivially handled in the non-linear case from the numerical point of view. Consequently, we chose to limit the interval analysis in order to allow numerical convergence under a reasonable verification time budget. Overall, this work represents an improvement over the state-of-the-art, increasing the complexity of the system under analysis while providing rigorous guarantees on the obtained results.

Summarizing, automated verification of medical robotic systems remains a computationally intractable problem where scalability remains a challenge. The use of ARIADNE for this case study allowed to identify key issues and stimulate improvements to the tool itself. Compared to the capabilities of the tool when used in Bresolin et al. [2015] and earlier works, we introduced an effective way to handle overapproximation errors when dealing with exponential convergence of the dynamics. Such method relies on reconditioning of the set, for which we can either limit the rounding error or even absorb it by under a contractive dynamics. This improvement curbs the growth of non-determinism due to overapproximations, and so it lets analyze a system of higher differential order; nevertheless, there is still room to improve the control of the approximation error. For example, when calculating reachability it is important to account for variables whose domains have very different orders of magnitude (like T and z, for example). In those cases, in fact, it would be desirable to have a comparable standard deviation of the error among the variables, which is a non-trivial issue when such variables are tightly coupled. Finally, a significant enhancement would be the implementation of *differential inclusions*: the ability to handle inputs whose dynamics is unknown, and are defined with their range of values. This feature would model noise, and so expand the validity of a given model and of its verification results.

The level of commitment from the industry remains limited to exploratory projects in collaboration with the academia. A challenge is to integrate verification tools and techniques in the design flow and in the certification process to ease the industrial adoption. We advocate that a systematic model-based analysis and design paradigm is the best approach for handling the inherent complexity of medical robotic systems. Reachability analysis of hybrid automata may play a role in such a paradigm as such technique allows to verify properties and components when the continuous dynamics has to be analyzed in a very accurate way. Moreover, implementing compositional verification techniques and assume-guarantee reasoning would allow the designer to integrate ARIADNE with other tools that use more traditional methods, and may be a key enhancement to tackle the complexity of medical robotic systems and to facilitate the adoption of formal verification by industry.

REFERENCES

Rajeev Alur. 2011. Formal Verification of Hybrid Systems. In *Proceedings of the Ninth ACM International Conference on Embedded Software (EMSOFT'11)*. ACM, Taipei, Taiwan, 273–278. DOI:http://dx.doi.org/10.1145/2038642.2038685

R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P. h. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. 1995. The Algorithmic Analysis of Hybrid Systems. *Theoretical Computer Science* 138 (1995), 3–34.

Rajeev Alur and David L. Dill. 1994. A Theory of Timed Automata. *Theor. Comput. Sci.* 126, 2 (1994), 183–235. DOI:http://dx.doi.org/10.1016/0304-3975(94)90010-8

Tobias Amnell, Elena Fersman, Leonid Mokrushin, Paul Pettersson, and Wang Yi. 2004. TIMES: A Tool for Schedulability Analysis and Code Generation of Real-Time Systems. In *Proceedings of the 1st International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS 2003)*. Springer, Marseille, France, 60–72. DOI:http://dx.doi.org/10.1007/978-3-540-40903-8_6

Ryan A. Beasley. 2012. Medical Robots: Current Systems and Research Directions. *Journal of Robotics* 2012, Article 401613 (2012), 14 pages. DOI:http://dx.doi.org/10.1155/2012/401613

Gerd Behrmann, Alexandre David, Kim Guldstrand Larsen, Paul Pettersson, and Wang Yi. 2011. Developing UPPAAL over 15 years. *Softw., Pract. Exper.* 41, 2 (2011), 133–142. DOI:http://dx.doi.org/10.1002/spe.1006

Luca Benvenuti, Davide Bresolin, Pieter Collins, Alberto Ferrari, Luca Geretti, and Tiziano Villa. 2014. Assume-guarantee verification of nonlinear hybrid systems with ARIADNE. *Int. J. Robust. Nonlinear Control* 24, 4 (2014), 699–724. DOI:http://dx.doi.org/10.1002/rnc.2914

P. Berkelman and others. 2009. A Compact Modular Teleoperated Robotic System for Laparoscopic Surgery. *The International Journal of Robotics Research* 28, 9 (2009), 1198.

Davide Bresolin, Luca Geretti, Riccardo Muradore, Paolo Fiorini, and Tiziano Villa. 2014. Verification of Robotic Surgery Tasks by Reachability Analysis: A Comparison of Tools. In *Digital System Design (DSD), 2014 17th Euromicro Conference on*. IEEE, 659–662.

Davide Bresolin, Luca Geretti, Riccardo Muradore, Paolo Fiorini, and Tiziano Villa. 2015. Formal verification of robotic surgery tasks by reachability analysis. *Microprocessors and Microsystems* 39, 8 (2015), 836–842. DOI:http://dx.doi.org/10.1016/j.micpro.2015.10.006

Xin Chen, Erika Abraham, and Sriram Sankaranarayanan. 2012. Taylor Model Flowpipe Construction for Non-linear Hybrid Systems. In *Proceedings of the 2012 IEEE 33rd Real-Time Systems Symposium*. IEEE Computer Society, Washington, DC, USA, 183–192. DOI:http://dx.doi.org/10.1109/RTSS.2012.70

Xin Chen, Erika Ábrahám, and Sriram Sankaranarayanan. 2013. Flow*: An Analyzer for Non-linear Hybrid Systems. In *Proceedings of the 25th International Conference on Computer Aided Verification (CAV 2013) (LNCS)*, Vol. 8044. Springer, Saint Petersburg, Russia, 258–263. DOI:http://dx.doi.org/10.1007/978-3-642-39799-8_18

Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. 2015. HyComp: An SMT-Based Model Checker for Hybrid Systems. In *Proceedings of the 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015) (LNCS)*, Vol. 9035. Springer, London, UK, 52–67. DOI:http://dx.doi.org/10.1007/978-3-662-46681-0_4

Kevin Cleary and Charles Nguyen. 2001. State of the art in surgical robotics: Clinical applications and technology challenges. *Computer Aided Surgery* 6, 6 (2001), 312–328.

Brian L. Davies. 1996. *A discussion of safety issues for medical robots*. MIT Press, Cambridge, MA, 287–296.

J.P. Desai and N. Ayache. 2009. Editorial Special Issue on Medical Robotics. *The International Journal of Robotics Research* 28, 9 (September 2009), 1099–1100. DOI:http://dx.doi.org/10.1177/0278364909338986

Baowei Fei, Wan Sing Ng, Sunita Chauhan, and Chee Keong Kwoh. 2001. The safety issues of medical robotics. *Reliability Engineering & System Safety* 73, 2 (2001), 183 – 192. DOI:http://dx.doi.org/10.1016/S0951-8320(01)00037-0

Loris Fichera. 2016. *Cognitive Supervision for Robot-Assisted Minimally Invasive Laser Surgery* (1st ed.). Springer International Publishing, Switzerland.

Loris Fichera, Diego Pardo, Placido Illiano, Jesus Ortiz, Darwin G Caldwell, and Leonardo S Mattos. 2015. Online estimation of laser incision depth for transoral microsurgery: approach and preliminary evaluation. *The International Journal of Medical Robotics and Computer Assisted Surgery* 12, 1 (March 2015), 53–61. DOI:http://dx.doi.org/10.1002/rcs.1656

G. Frehse. 2008. PHAVer: algorithmic verification of hybrid systems past HyTech. *International Journal on Software Tools for Technology Transfer (STTT)* 10 (2008), 263–279. Issue 3. DOI:http://dx.doi.org/10.1007/s10009-007-0062-x

G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. 2011. SpaceEx: Scalable Verification of Hybrid Systems. In *Proc. 23rd International Conference on Computer Aided Verification (CAV 2011) (LNCS)*, Vol. 6806. Springer, Snowbird, UT, USA, 379–395. DOI:http://dx.doi.org/10.1007/978-3-642-22110-1_30

N. Fulton, S. Mitsch, J.D. Quesel, M. Völp, and A. Platzer. 2015. KeYmaera X: An aXiomatic tactical theorem prover for hybrid systems. In *Proceedings of the International Conference on Automated Deduction, CADE'15, Berlin, Germany*, Vol. 9195. Springer, 527–538.

E. Guglielmelli, M. J. Johnson, and T. Shibata. 2009. Guest Editorial Special Issue on Rehabilitation Robotics. *Robotics, IEEE Transactions on* 25, 3 (June 2009), 477 –480.

T.A. Henzinger. 1996. The theory of hybrid automata. In *Proceedings of the 11th IEEE Symposium on Logic in Computer Science (LICS '96)*. IEEE Computer Society, New Brunswick, New Jersey, USA, 278–292.

T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. 1998. What's Decidable about Hybrid Automata? *J. Comput. System Sci.* 57, 1 (1998), 94 – 124. DOI:http://dx.doi.org/10.1006/jcss.1998.1581

Thomas A. Henzinger and Joseph Sifakis. 2006. The Embedded Systems Design Challenge. In *14th International Symposium on Formal Methods (FM 2006) (LNCS)*, Vol. 4085. Springer, Hamilton, Canada, 1–15. DOI:http://dx.doi.org/10.1007/11813040_1

Eunkyoung Jee, Shaohui Wang, Jeong-Ki Kim, Jaewoo Lee, Oleg Sokolsky, and Insup Lee. 2010. A Safety-Assured Development Approach for Real-Time Software. In *Proceedings of the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2010)*. IEEE, Macau, China, 133–142. DOI:http://dx.doi.org/10.1109/RTCSA.2010.42

R. Jetley, S. Purushothaman Iyer, and P. Jones. 2006. A formal methods approach to medical device review. *Computer* 39, 4 (April 2006), 61–67. DOI:http://dx.doi.org/10.1109/MC.2006.113

Timothy L. Johnson. 2007. Improving automation software dependability: A role for formal methods? *Control Engineering Practice* 15, 11 (2007), 1403–1415. DOI:http://dx.doi.org/10.1016/j.conengprac.2006.07.005

P. Kazanzides, G. Fichtinger, G.D. Hager, A.M. Okamura, L.L. Whitcomb, and R.H. Taylor. 2008. Surgical and interventional robotics-core concepts, technology, and design. *Robotics & Automation Magazine, IEEE* 15, 2 (2008), 122–130.

BaekGyu Kim, Anaheed Ayoub, Oleg Sokolsky, Insup Lee, Paul L. Jones, Yi Zhang, and Raoul Praful Jetley. 2011. Safety-assured development of the GPCA infusion pump software. In *Proceedings of the 11th International Conference on Embedded Software (EMSOFT 2011)*. ACM, Taipei, Taiwan, 155–164. DOI:http://dx.doi.org/10.1145/2038642.2038667

Yanni Kouskoulas, David Renshaw, André Platzer, and Peter Kazanzides. 2013. Certifying the Safe Design of a Virtual Fixture Control Algorithm for a Surgical Robot. In *Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control (HSCC '13)*. ACM, Philadelphia, Pennsylvania, USA, 263–272. DOI:http://dx.doi.org/10.1145/2461328.2461369

H. Kress-Gazit. 2011. Robot challenges: Toward development of verification and synthesis techniques [from the Guest Editors]. *Robotics Automation Magazine, IEEE* 18, 3 (Sept 2011), 22–23. DOI:http://dx.doi.org/10.1109/MRA.2011.942486

I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. K. Venkatasubramanian. 2012. Challenges and Research Directions in Medical Cyber–Physical Systems. *Proc. IEEE* 100, 1 (Jan 2012), 75–90. DOI:http://dx.doi.org/10.1109/JPROC.2011.2165270

Col Michael R Marohn and Capt Eric J Hanly. 2004. Twenty-first century surgery using twenty-first century technology: surgical robotics. *Current Surgery* 61, 5 (2004), 466–473.

Maja Matarić, Allison M. Okamura, and Henrik I. Christensen. 2013. Roadmap for Medical and Healthcare Robotics. In *A Roadmap for U.S. Robotics–From Internet to Robotics* (2013 ed.). Georgia Institute of Technology, Atlanta, GA, Chapter 2, 27–62.

L. S. Mattos, G. Dagnino, G. Becattini, M. Dellepiane, and D. G. Caldwell. 2011. A virtual scalpel system for computer-assisted laser microsurgery. In *2011 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, San Francisco, CA, 1359–1365. DOI:http://dx.doi.org/10.1109/IROS.2011.6094574

R. Muradore, D. Bresolin, L. Geretti, P. Fiorini, and T. Villa. 2011. Robotic Surgery: Formal Verification of Plans. *Robotics & Automation Magazine, IEEE* 18, 3 (2011), 24–32.

Markolf H Niemz. 2007. *Laser-tissue interactions. Fundamentals and Applications*. Springer, Berlin.

Pierluigi Nuzzo, Alberto L. Sangiovanni-Vincentelli, Davide Bresolin, Luca Geretti, and Tiziano Villa. 2015. A Platform-Based Design Methodology With Contracts and Related Tools for the Design of Cyber-Physical Systems. *Proc. IEEE* 103, 11 (2015), 2104–2132. DOI:http://dx.doi.org/10.1109/JPROC.2015.2453253

S. Ratschan and Z. She. 2007. Safety Verification of Hybrid Systems by Constraint Propagation Based Abstraction Refinement. *ACM Transactions in Embedded Computing Systems* 6, 1, Article 8 (2007), 23 pages.

A. Sangiovanni-Vincentelli. 2007. Quo Vadis, SLD? Reasoning About the Trends and Challenges of System Level Design. *Proc. IEEE* 95, 3 (2007), 467–506.

R.H. Taylor. 2006. A Perspective on Medical Robotics. *Proc. IEEE* 94, 9 (Sept. 2006), 1652 –1664.

R. H. Taylor, H. A. Paul, P. Kazanzides, B. D. Mittelstadt, W. Hanson, J. Zuhars, B. Williamson, B. Musits, E. Glassman, and W. L. Bargar. 1991. Taming the bull: safety in a precise surgical robot. In *Fifth International Conference on Advanced Robotics (ICAR)*, Vol. 1. IEEE, Pisa, Italy, 865–870. DOI:http://dx.doi.org/10.1109/ICAR.1991.240565

Received ; revised ; accepted