In: Proc. of the 36th Midwest Symposium on Circuits and Systems
August 16-18, 1993, Detroit, MI, USA, pp. 332–335.

Improving Characteristics of Discrete Event Controllers with Hybrid Controllability of Events[1]

Petr Kozák[2]
Systems Control Group, Dept. of Electrical Engineering,
University of Toronto, Toronto, Ontario, M5S 1A4 Canada

Abstract

Hybrid controllability describes delayed response of plant to control actions dependent on current i/o trajectory. The minimally restrictive controller for a plant with hybrid controllability solving a time extension of supervisory control problem is sensitive with respect to inaccuracies of hybrid plant parameters. The paper presents a controller which is more restrictive but works properly in presence of small deviations of hybrid parameters.

I. Introduction

The control system of a plant (e.g. manufacturing line) can be divided into two parts (with fuzzy boundary); continuous variable controllers and logical (discrete event) controllers. It is not always possible to consider the tasks of controllers from these two groups independent one from another. On the other hand, the methods for design of controllers within one group are not usually suited to deal also with problems from another group. This is one of motivations for development of "hybrid" models and design methods for "hybrid" controllers. The present paper discusses a control problem with discrete event specifications for a discrete event plant with certain hybrid component describing delayed response to control actions (i.e. to inputs).

Untimed discrete event models describe typically, e.g. [1], system dynamics in terms of logical (non-numerical) description of i/o trajectories and/or state trajectories. Timed discrete models can describe additionally time dependent characteristics of output trajectories (often infimal and/or maximal delays between two subsequent output discrete events) or communication delays, e.g [2, 3, 4]. A response of the plant to an input event is usually straightforward, e.g. immediate acceptance of disablement (or enablement) of an event [1, 3]. Difference between causal and strongly causal supervisors are discussed in [2]. A control problem for a plant with delayed response to control actions caused by communication delays is solved in [4]. These communication delays are independent of i/o trajectory.

The delayed response to control actions of certain plants depend in a natural way also on the state (i/o trajectory) of the plant (see the example below). A controller for such a plant designed using a model not describing the delayed response could realize too restrictive closed-loop behaviour or even this behaviour would not satisfy the control problem specifications. The following example describes briefly such a plant.

Example I.1: Consider a main road leading up to a hill with two side-roads **R1** and **R2**, Fig. 1. The roads **R1** and **R2** are only one way roads. A vehicle can be in one of seven states:

UD – on the upper part of hill moving downwards,
LD – on the lower part of hill moving downwards,
LU – on the lower part of hill moving upwards,
UU – on the upper part of hill moving upwards,
S1 – on side-road **R1**,
S2 – on side-road **R2**,
I – not on the three roads.

An automata (untimed) model of this system is on Fig. 2. There are six position sensors on the main road (located at 1,3, 5 for each direction giving signals labeled by **s**, **b**, **o**) and two position sensors on each of side roads (at the ends of roads signaling labels **a**).

[1]The work was partially supported by Bell Canada research contract No. 3–254–188–10 (Univ. of Toronto), and by the grants ČSAV #27502 and ČAV #27558.

[2]The author is on leave from Czech Academy of Sciences, Institute of Information Theory and Automation, Pod vodárenskou věží 4, 182 08 Prague 8, Czech Republic, E-mail: kozak@cspgas11.bitnet

The transition labels have the following interpretation:

o – entering the main road through place 5,

b – entering the main road through place 1,

s – other transitions on the main road,

a – any transition on any side road.

Vehicles are controlled such that they can be asked not to go straight on the main road but to turn off, i.e. it can be disabled to go straight. This could be formulated such that **s** is the only one controllable event [1].

If a vehicle **V2** (Fig. 1) going downwards the main road is disabled to go straight later than at point 4 then it is possible that the vehicle turns to **R1** or does not turn at all even if it is asked before it pass road **R2**. This is caused by inertia of vehicle, quality of brake and of road surface etc. A solution can be either to install one more sensor at the place 4 to indicate the time moment when the disablement should be generated or to consider also time information in the plant model. The distance between 4 and the junction with **R2** corresponds (for a given vehicle) to the quality of controllability of **s**. This quality is state dependent, e.g. for this case it suffices to disable **s** for a vehicle **V1** going upwards not later than 3. But if **s** is disabled at e.g. 2 the vehicle takes road **R1** instead of **R2**.

To control properly the vehicle, it is sufficient to know the speed of the vehicle and distance from the junction. However, information of this kind is not always available to a controller. The controller can only estimate it using parameters of the plant (e.g. maximal speed and weight of vehicle, minimal deceleration, distances between sensors and junctions) and time moments of discrete event occurrences. ■

Hybrid controllability of discrete events [5] can model the delayed response to control actions presented in the previous example in a simplified way (approximating [worst case] deceleration and acceleration by constants). The plant is modelled with time set equal to nonnegative reals and with known infimal delays between two subsequent output discrete events. The minimally restrictive controller for the plant and a problem, which can be viewed as a time extension of problem in [1], is given in [5]. The hybrid controllability is suggested [5] as a tradeoff between simplicity and tractability.

The plant with hybrid controllability [5] is completely observable, i.e. a controller can compute a current state of plant on the basis of i/o trajectory. However, this requires that all parameters of the plant are known accurately. Any inaccuracy can cause that controller does not know the current state of the plant which is necessary for calculation of control actions. The present paper describes a controller which is in certain sense less sensitive (more robust with respect) to small inaccuracies in hybrid plant parameters. The controller is not minimally restrictive.

Robustness of discrete event controllers with respect to untimed (and nonnumerical) parameters is discussed in [6].

The paper is organized as follows. Sections II and III formulate the model of plant and control problem, respectively. Minimally restrictive controller is given in Section IV. Section V presents a robust version of controller.

II. Plant Model

A. Preliminaries

This section summarizes notation used in the paper.

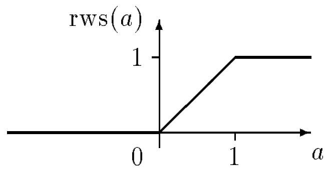
Real numbers are denoted by $\mathbb{R}$. Non-negative real numbers and natural numbers by $\mathbb{R}_0^+$ and $\mathbb{N}$, respectively. Intervals denoted e.g. by $[0,1]$ or $(0,1)$ are supposed to be real number intervals.

Set difference is denoted by $\setminus$.

Notation conventions: A word consisting of singleton sets, e.g. $\{a\}\{b\}$ is considered equal to ab if possible with respect to context. If $w = \epsilon$ is denoted by $w = e_1 e_2 \ldots e_n$ for some n then $n = 0$. It is supposed that $e_1 e_2 \ldots e_{n-1} = \epsilon$ if $n \leq 1$ for some $w = e_1 e_2 \ldots e_n$.

A ramp with saturation is mapping $\mathrm{rws} : \mathbb{R} \to [0,1]$ according to

$$\mathrm{rws}(a) = \begin{cases} 0 & \text{if } a < 0, \\ a & \text{if } 0 \leq a \leq 1, \\ 1 & \text{otherwise,} \end{cases}$$



for all $a \in \mathbb{R}$.

Restriction of a mapping f to a set A is denoted $f|_A$. Composition of mappings f and g is defined as $(f \circ g) : \mathrm{Dom}(g) \to \mathrm{Im}(f)$.

For an arbitrary set V masking m_V is a class mapping on the universal class such that it maps each set into its intersection with V. Example: $m_V \circ o$ denotes a mapping such that $\mathrm{Dom}(m_V \circ o) = \mathrm{Dom}(o)$ and for all $t \in \mathrm{Dom}(o)$ we have $(m_V \circ o)(t) = o(t) \cap V$.

Let $\mathcal{G}$ be a set of mappings such that the domain of each mapping $g \in \mathcal{G}$ is linearly ordered for some $\leq_g$. The set of prefixes of $\mathcal{G}$ is

$$\mathrm{pref}(\mathcal{G}) = \{ g|_A \mid g \in \mathcal{G} \ \wedge \ A \in \mathcal{I}_{(\mathrm{Dom}(g), \leq_g)} \ \} ,$$

where $\mathcal{I}_{(\mathrm{Dom}(g), \leq_g)}$ is the set of all $B \subseteq \mathrm{Dom}(g)$ (initial segments) such that for all $b \in B$ and $t \in \mathrm{Dom}(g)$ satisfying $t \leq_g b$ this holds $t \in B$.

The set of upper-bounded prefixes of $\mathcal{G}$ is

$$\mathrm{prefb}(\mathcal{G}) = \{ g|_A \mid g \in \mathcal{G} \wedge A \in \mathcal{I}_{(\mathrm{Dom}(g), \leq_g)} \wedge A \text{ is upper-bounded} \} .$$

The set of trajectories in $\mathcal{G}$ possible with respect to $f \in \mathrm{pref}(\mathcal{G})$ is

$$\mathcal{O}_{\mathcal{G}}(f) = \{ g \in \mathcal{G} \mid f \in \mathrm{pref}(g) \ \}.$$

B. Subsystems of Plant

Let $p \in \mathbb{N}$ and I be set of natural numbers i such that $1 \leq i \leq p$. The plant consist of p parallelly interconnected subsystems with names I. Each subsystem $i \in I$ has the following parameters:

RW-System. $(\Sigma_i, L_i, \Sigma_{c,i})$ is a system of [1], where Σ_i is the set of output event labels, $L_i \subseteq \Sigma_i^*$ is the language describing uncontrolled output behaviour such that $\mathrm{pref}(L_i) = L_i$, and $\Sigma_{c,i} \subseteq \Sigma_i$ is the set of controllable events,

Input Event Labels. $U_i = \{ \mathbf{E}_\sigma \mid \sigma \in \Sigma_{c,i} \} \cup \{ \mathbf{D}_\sigma \mid \sigma \in \Sigma_{c,i} \}$. The symbols $\mathbf{D}_\sigma$ and $\mathbf{E}_\sigma$ represent labels of disablement and enablement of events labeled by σ.

Basic Set of Behaviours. $\mathcal{M}_i$ is the set of all mapping $f : \mathbb{R}_0^+ \to \mathcal{P}(U_i \cup \Sigma_i)$ such that $f(t) \neq \emptyset$ for only finite number of time moments $t \in \mathbb{R}_0^+$, i.e. it is the set of timed traces of finite length with elements in power set of $U_i \cup \Sigma_i$. The empty set models "empty" event.

Infimal Delays. $\varepsilon_i : \Sigma_i^* \times \Sigma_i^* \to \mathbb{R}_0^+$ such that $\varepsilon_i(w, w') = 0$ whenever $w' = \epsilon$. The value $\varepsilon_i(w, w')$ is interpreted as the infimal delay between w and the first event in w'.

Hybrid Controllability. For all $\sigma \in \Sigma_{c,i}$ hybrid controllability $C_\sigma : \Sigma_i^* \to (0, 1)$. The number $C_\sigma(w)$ is controllability of σ after executing w.

Parameters for Integration. Let for all $\sigma \in \Sigma_{c,i}$, $\Theta_\sigma \in [0, 1]$, $\bar{\kappa}_\sigma : \Sigma_i^* \to \mathbb{R}$, and $\kappa_\sigma : \Sigma_i^* \to \mathbb{R}$ be such that

$$\forall w \in \Sigma_i^*, \quad \bar{\kappa}_\sigma(w) < 0 < \kappa_\sigma(w) \quad .$$

The number Θ_σ is initial condition of an integrator related to σ.

Given any timed trace f, $s(f)$ denotes sequence of event labels ordered in the same way as they occur in f. $\mathrm{last}(f)$ denotes the time of occurrence of last discrete event in f, or if no event occurs in f then $\mathrm{last}(f) = 0$.

For all $i \in I$ the following three mappings are defined:

Delay Mapping. A delay mapping $E_i : \mathrm{pref}(\mathcal{M}_i) \times \mathbb{R}_0^+ \to \mathcal{P}(\Sigma_i)$ describing the set of output event labels that are enabled with respect to the infimal delays at time t after execution of f is defined for all $f \in \mathrm{pref}(\mathcal{M}_i)$ and $t \in \mathbb{R}_0^+$ according to

$$E_i(f, t) = \{ \sigma \in \Sigma_i \mid \varepsilon_i(s(m_{\Sigma_i} \circ f), \sigma) < t - \mathrm{last}(m_{\Sigma_i} \circ f) \ \} \quad .$$

Disablement Mapping. A disablement mapping $\eta_i : \mathrm{pref}(\mathcal{M}_i) \to \mathcal{P}(\Sigma_i)$ determining the set of disabled events is defined for all $f \in \mathrm{pref}(\mathcal{M}_i)$ according to

$$\eta_i(f) = \{ \sigma \in \Sigma_i \mid \mathbf{D}_\sigma \in f(\mathrm{last}(m_A \circ f)) \ \} \quad ,$$

where $A = \{ \mathbf{E}_\sigma, \mathbf{D}_\sigma \}$.

Level of Disablement. For all $\sigma \in \Sigma_{c,i}$, $D_\sigma : \mathrm{pref}(\mathcal{M}_i) \to [0, 1]$ such that for all $f \in \mathrm{pref}(\mathcal{M}_i)$,

$$D_\sigma(f) \ = \ K_{n+1} \quad ,$$

where n is the number of discrete events in f, $\tau_0 = 0$, $K_0 = \Theta_\sigma$, and for $1 \leq j \leq n + 1$,

$$\tau_j \ = \ \begin{cases} \sup \mathrm{Dom}(f) & \text{if } j = n+1, \\ \text{time of occurrence of} & \text{otherwise,} \\ j\text{-th event in } f & \end{cases}$$

$$K_j \ = \ \begin{cases} \mathrm{rws}(K_{j-1} + (\tau_j - \tau_{j-1}) \cdot \kappa_\sigma(x)) & \text{if } \sigma \in \eta_i(g), \\ \mathrm{rws}(K_{j-1} + (\tau_j - \tau_{j-1}) \cdot \bar{\kappa}_\sigma(x)) & \text{otherwise,} \end{cases}$$

$g = f|_{[0, \tau_{j-1}]}$, $x = s(m_{\Sigma_i} \circ g)$ and $\cdot$ denotes multiplication of reals.

The behaviour of subsystem i is defined using an output law μ_i giving for each $f \in \mathrm{pref}(\mathcal{M}_i)$ and $t \in \mathrm{Dom}(f)$ a set of possible output event labels which can be generated after observing $f\,|_{[0,t)}$ at time moment t:

$$\begin{aligned}\mu_i(f,t) \;=\; & \{\emptyset\} \;\cup \\ & \{\{\sigma\} \mid \sigma \in \Sigma_i \wedge s(m_{\Sigma_i} \circ f\,|_{[0,t)})\sigma \in L_i \;\wedge\; \sigma \in E_i(f\,|_{[0,t)}, t) \\ & \wedge\, (\sigma \in \Sigma_i \setminus \Sigma_{c,i} \vee D_\sigma(f\,|_{[0,t)}) < C_\sigma(s(f\,|_{[0,t)}))\ )\ \}\ .\end{aligned}$$

The empty event can be always generated. The second line specifies that only events which are consistent with untimed model L_i and satisfying the infimal delay requirement may be generated. The third line states that if an event is generated than it is either uncontrollable or the current value of D_σ is smaller than the hybrid controllability of the event. The plant is depicted on Fig. 3.

C. Plant Definition

Let

$$\Sigma = \bigcup_{i\in I} \Sigma_i \quad , \quad U = \bigcup_{i \in I} U_i \quad ,$$

$$\begin{aligned}\mathcal{E} &= \mathcal{P}(\Sigma) \setminus \{\emptyset\}\ , \\ \mathcal{E}_c &= \{e \in \mathcal{E} \mid \exists i \in I,\ \Sigma_{c,i} \cap e \neq \emptyset\}\ , \\ L &= \{w \in \mathcal{E}^* \mid \forall i \in I,\ s(m_{\Sigma_i} \circ w) \in L_i\}\ ,\end{aligned}$$

and for all $i \in I$, $X_i = U_i \cup \Sigma_i$. Let $\mathcal{M}$ be the set of all timed traces with elements in $\mathcal{P}(U \cup \Sigma)$. Suppose that the sets Σ_i $(i \in I)$ are pairwise disjoint.

The output law $\mu_o : \mathrm{pref}(\mathcal{M}) \rightarrow \mathcal{P}(\mathcal{E})$ is defined as parallel composition of laws μ_i $(i \in I)$ according to

$$\mu_o(f,t) = \{e_1 \cup e_2 \cup \ldots \cup e_p \mid \forall i \in I,\ e_i \in \mu_i(m_{X_i} \circ f, t)\}\ ,$$

for all $f \in \mathrm{pref}(\mathcal{M})$ and $t \in \mathrm{Dom}(f)$.

The behaviour of plant is modelled by

$$\mathcal{G} = \{f \in \mathcal{M} \mid \forall t \in \mathrm{I\!R}_0^+,\ m_\Sigma \circ f(t) \in \mu_o(f,t)\ \}\ .$$

Example II.1: Consider the plant of Example I.1. The plant has one subsystem with $p = 1$, $\Sigma_1 = \{\mathbf{a}, \mathbf{b}, \mathbf{o}, \mathbf{s}\}$, and $\Sigma_{c,1} = \{\mathbf{s}\}$.

Define $\kappa_{\mathbf{s}}(w) = 0.1$ and $\bar{\kappa}_{\mathbf{s}}(w) = -0.2$ for all $w \in \Sigma_1^*$ recognized by states **UD** or **LD**. Define $\kappa_{\mathbf{s}}(w) = 0.2$ and $\bar{\kappa}_{\mathbf{s}}(w) = -0.1$ for all $w \in \Sigma_1^*$ recognized by states **UU** or **LU**. This reflects the fact that acceleration is easier than deceleration if the vehicle goes downwards and vice versa if it goes upwards. Let $\kappa_{\mathbf{s}}(w) = |\bar{\kappa}_{\mathbf{s}}(w)| = 0.15$ for all other w. Let

$$\varepsilon_1(w, \mathbf{s}) = \begin{cases} 3 & \text{for } w \text{ recognized by } \mathbf{UD} \text{ and } \mathbf{LD}, \\ 4 & \text{otherwise.}\end{cases}$$

The infimal delays are smaller if the vehicle goes downwards than if it goes in the opposite direction. Let the hybrid controllability of $\mathbf{s}$ is $C_{\mathbf{s}}(w) = 0.2$ for all w.

In order to avoid occurrence of $\mathbf{s}$ at state **UD**, it is necessary to have $D_{\mathbf{s}} \geq 0.2$ if the plant is in **UD** longer than 3 units. This can be achieved e.g. by disabling $\mathbf{s}$ by time 1 after entering **UD**. The increase of $D_{\mathbf{s}}$ is guaranteed to be up to 0.2 (regarding saturation at level 1) in this case. If the vehicle goes upwards, it suffices e.g. to disable $\mathbf{s}$ by 3 units after entering **UU** to guarantee that $\mathbf{s}$ does not occur at **UU**. ■

III. Control Problem

A. Formulation

Let $\emptyset \neq L_a \subseteq L_g \subseteq L_m \subseteq L$. Find a strongly controllable behaviour $\mathcal{Z}$ of the plant such that the following three constraints are satisfied

$$s(m_\Sigma \circ \mathcal{Z}) \cap L_m \;\subseteq\; L_g\ , \tag{1}$$

$$\forall f \in \mathrm{prefb}(\mathcal{Z}), \exists v \in \Pi_{\mathcal{Z}}(f),\quad v \;\in\; L_m\ , \tag{2}$$

$$L_a \;\subseteq\; \Pi_{\mathcal{Z}}(\Lambda_\emptyset) \cap L_m\ , \tag{3}$$

where $\Lambda_\emptyset$ is a mapping with domain equal to $\emptyset$ and for all $f \in \text{prefb}(\mathcal{Z})$ a set $\Pi_{\mathcal{Z}}(f)$ is defined according to

$$\begin{aligned}\Pi_{\mathcal{Z}}(f) \quad = \quad & \{v \in \mathcal{E}^* \mid \forall g \in \text{prefb}(\mathcal{O}_{\mathcal{Z}}(f)) \setminus \text{pref}(f), \\ & s(m_\Sigma \circ g) \in \text{pref}(v) \Rightarrow v \in s(m_\Sigma \circ \mathcal{O}_{\mathcal{Z}}(g))\ \}\ .\end{aligned}$$

The problem is solved in [5] with an additional requirement that $s(m_\Sigma \circ \mathcal{Z}) \cap L_m = K$ is (parallelly feasible boundary) PF-boundary if for all $v, w \in \mathcal{E}^+$ the following conditions

(*i*) $v \notin \text{pref}(K)$,

(*ii*) $e_1 e_2 \ldots e_{n-1} \in \text{pref}(K)$,

(*iii*) $\forall i \in I,\ s(m_{\Sigma_i} \circ v) = s(m_{\Sigma_i} \circ w)$,

together imply that

(*iv*) $w \notin \text{pref}(K)$,

where $v = e_1 e_2 \ldots e_n$ for some n and $e_k \in \mathcal{E}$ $(1 \leq k \leq n)$.

B. Necessary Conditions

The following notation is required. For all $i \in I$, $\sigma \in \Sigma_{c,i}$, $v \in \Sigma_i^*$, and $w \in \Sigma_i^*$,

$$F_\sigma(v, w) = \sum_{j=1}^{n} \kappa_\sigma(v e_1 e_2 \ldots e_j) \cdot \varepsilon_i(v e_1 e_2 \ldots e_j, e_{j+1})$$

where $w = e_1 e_2 \ldots e_n$ for some n, for all $e_k \in \Sigma_i$ $(1 \leq k \leq n)$, and $e_{n+1} = \sigma$.

The value $F_\sigma(v, w)$ represents the increase of D_σ along the untimed output trajectory $w\sigma$ guaranteed by the infimal delays supposing that v was previously executed and σ is disabled.

Let $\emptyset \neq \mathcal{Z} \subseteq \mathcal{G}$ and $\emptyset \neq K \subseteq L_m$ be a PF-boundary such that $s(m_\Sigma \circ \mathcal{Z}) \cap L_m = K$. Define $\beta : \text{pref}(K) \to \mathcal{P}(\mathcal{E})$ such that for all $v \in \text{pref}(K)$ we have

$$\begin{aligned}\beta(v) \quad = \quad & \{e \in \mathcal{E} \mid ve \in L\ \wedge\ \forall w \in \mathcal{E}^+,\ [(5) \wedge (6)]\ \Rightarrow \\ & \exists i \in I, \exists j \in \mathbb{N}, 1 \leq j \leq n, \exists a \in e_j \cap \Sigma_{c,i},\ [a \notin e \vee (7)]\ \}\ ,\end{aligned} \tag{4}$$

where $w = e_1 e_2 \ldots e_n$ for some n, $e_k \in \mathcal{E}$ $(1 \leq k \leq n)$, $w' = e_1 e_2 \ldots e_{j-1}$, $w'' = s(m_{\Sigma_i} \circ v)s(m_{\Sigma_i} \circ w')$, and

$$vw\ \in\ L \setminus \text{pref}(K) \tag{5}$$

$$v e_1 e_2 \ldots e_{n-1} \in \text{pref}(K) \tag{6}$$

$$C_a(w'') - F_a(s(m_{\Sigma_i} \circ v), s(m_{\Sigma_i} \circ w'))\ <\ C_a(v) \tag{7}$$

The following theorem [5] summarizes necessary properties of K.

Theorem III.1: If $\mathcal{Z}$ is a solution then the following conditions are satisfied:

(*i*) $K \subseteq L_g$, $\text{pref}(K) \cap L_m = K$, and K is a controllable language with respect to $\mathcal{S}^{RW} = (\mathcal{E}, L, \mathcal{E}_c)$,

(*ii*) $\forall v \in \text{pref}(K)$, $\forall e \in \mathcal{E}$, $\forall w \in \mathcal{E}^*$,
$[ve \in \text{pref}(K) \wedge \forall i \in I, s(m_{\Sigma_i} \circ w) = s(m_{\Sigma_i} \circ e)\ ] \Rightarrow vw \in \text{pref}(K)$.

(*iii*) $\forall v \in \text{pref}(K)$, $\exists w \in \mathcal{E}^*$, $vw \in K\ \wedge\ \forall j \in \mathbb{N}, 1 \leq j \leq n,\ e_j \in \beta(vw')$,

(*iv*) $\forall w \in L_a$, $\forall j \in \mathbb{N}, 1 \leq j \leq n,\ e_j \in \beta(w')$,

(*v*) $\forall w \in L \setminus \text{pref}(K)$, $w \neq \epsilon$,

$$\begin{aligned}& e_1 e_2 \ldots e_{n-1} \in \text{pref}(K)\ \Rightarrow \\ & \quad [\exists i \in I, \exists j \in \mathbb{N}, 1 \leq j \leq n, \exists \sigma \in e_j \cap \Sigma_{c,i}, \\ & \quad \Theta_\sigma + \kappa_\sigma(\epsilon) \cdot \varepsilon_i(\epsilon, w''\sigma) + F_\sigma(\epsilon, w'') \geq C_\sigma(w'')]\ \ ,\end{aligned}$$

where $w = e_1 e_2 \ldots e_n$ for some n, $e_k \in \mathcal{E}$ $(1 \leq k \leq n)$, $w' = e_1 e_2 \ldots e_{j-1}$, and $w'' = s(m_{\Sigma_i} \circ w')$. ■

IV. Minimally Restrictive Controller

Suppose that K satisfies the conditions of Theorem III.1. Let for an arbitrary real number a the value $\text{pos}(a)$ is equal to a if $a > 0$ otherwise $\text{pos}(a) = 0$.

Define for all $i \in I$, $\sigma \in \Sigma_{c,i}$, $f \in \text{pref}(\mathcal{M}_i)$, $w \in \Sigma_i^*$

$$Z_\sigma(f, w) = D_\sigma(f) + \kappa_\sigma(v) \cdot d + F_\sigma(v, w)\ \ , \tag{8}$$

where $v = s(m_{\Sigma_i} \circ f)$ and

$$d = \mathrm{pos}(\mathrm{last}(m_{\Sigma_i} \circ f) + \varepsilon_i(v, w\sigma) - \sup \mathrm{Dom}(f)) \quad .$$

The value $Z_\sigma(f, w)$ represents a minimal value of D_σ guaranteed after execution f along the untimed output trajectory $w\sigma$ supposing that σ is disabled.

The minimally restrictive controller is defined [5] using a control law $\mu_c : \mathcal{G} \times \mathrm{I\!R}_0^+ \to \mathcal{P}(\mathcal{P}(U)) \setminus \{\emptyset\}$ determining control actions after i/o trajectory $m_\Sigma \circ f|_{[0,t)}$ at time t for all $f \in \mathcal{G}$ and $t \in \mathrm{I\!R}_0^+$, with

$$\begin{aligned} \mu_c(f,t) \quad = \quad & \{x \in \mathcal{P}(U) \mid \forall w \in \mathcal{E}^+,\ [\,(5) \wedge (6)\,] \ \Rightarrow \\ & \exists i \in I, \exists j \in \mathrm{I\!N}, 1 \le j \le n, \exists \sigma \in \Sigma_{c,i},\ [\,(10) \vee (11)\,]\,\}\ , \end{aligned} \tag{9}$$

where $w = e_1 e_2 \ldots e_n$ for some n, $e_k \in \mathcal{E}$ $(1 \le k \le n)$, $v = s(m_\Sigma \circ f|_{[0,t)})$, $w' = e_1 e_2 \ldots e_{j-1}$, $w'' = s(m_{\Sigma_i} \circ v) s(m_{\Sigma_i} \circ w')$, and

$$Z_\sigma(m_{V_i} \circ f|_{[0,t)}, s(m_{\Sigma_i} \circ w')) > C_\sigma(w'') \tag{10}$$

$$Z_\sigma(m_{V_i} \circ f|_{[0,t)}, s(m_{\Sigma_i} \circ w')) = C_\sigma(w'') \Rightarrow \sigma \in \eta_i(m_{V_i} \circ u) \tag{11}$$

and $u \in \mathrm{pref}(m_U \circ \mathcal{G})$ such that

$$\mathrm{Dom}(u) = [0, t] \quad \wedge \quad u|_{[0,t)} = m_U \circ f|_{[0,t)} \quad \wedge \quad u(t) = x \quad .$$

The minimally restrictive solution is defined [5] as

$$\mathcal{Z} = \{f \in \mathcal{G} \mid \forall t \in \mathrm{I\!R}_0^+,\ m_U \circ f(t) \in \mu_c(f,t)\ \} \quad . \tag{12}$$

According to μ_c, the controller can enable certain event σ for a limited time if D_σ is sufficiently high. It must disable it again if certain lower level is reached. The controller must know the value of D_σ for evaluation of Z_σ. Frequent enablements and disablements, and inaccurately known parameters κ_σ and $\bar{\kappa}_\sigma$ can cause deviation of the computed value from the actual value. The events observed on the output of plant do not enable to check the actual value of D_σ. But if the integrator for D_σ is saturated then it is much more accurate to determine the value of D_σ. Thus a robust strategy can be formulated in this way.

V. Robust Controller

For all $f \in \mathcal{G}$ and $t \in \mathrm{I\!R}_0^+$

$$\begin{aligned} \mu_{\mathrm{r}}(f,t) \quad = \quad & \{x \in \mu_o(f,t) \mid \forall i \in I, \forall \sigma \in \Sigma_{c,i}, \\ & \big[\sigma \in \eta_i(f|_{[0,t)}) \wedge (t - \tau) \cdot \kappa_\sigma(s(m_{\Sigma_i} \circ f|_{[0,\tau]})) < 1\big] \Rightarrow A \cap x = \emptyset\ \}, \end{aligned}$$

where $\tau = \mathrm{last}(m_A \circ f)$ and $A = \{\mathbf{E}_\sigma, \mathbf{D}_\sigma\}$.

This controller must disable a event σ at least for the time interval during which the integrator would integrate 1 according to known parameters. This enable to reach (with high probability) the saturation and then it is possible to set the value of D_σ calculated by the controller to 1.

In the following, it is checked that

$$\mathcal{Z}_{\mathrm{r}} = \{f \in \mathcal{G} \mid \forall t \in \mathrm{I\!R}_0^+,\ m_U \circ f(t) \in \mu_{\mathrm{r}}(f,t)\ \}$$

is a solution. It can be shown using [7] that $\mathcal{Z}_{\mathrm{r}}$ is a strongly controllable behaviour. The robust control law μ_{r} is more restrictive than μ_c, because for all $f \in \mathcal{G}$ and $t \in \mathrm{I\!R}_0^+$, $\mu_{\mathrm{r}}(f,t) \subseteq \mu_c(f,t)$. Therefore also $\mathcal{Z}_{\mathrm{r}} \subseteq \mathcal{Z}$. To prove that $\mathcal{Z}_{\mathrm{r}}$ is a solution, the following two lemmas are required. Interpretation of lemmas is such that events given by mapping β are not blocked.

Lemma V.1: For all $f \in \mathrm{prefb}(\mathcal{G})$ and $e \in \beta(v)$ such that

$$\forall t \in \mathrm{Dom}(f),\ m_U \circ f(t) \in \mu_{\mathrm{r}}(f,t) \tag{13}$$

this holds $ve \in s(m_\Sigma \circ \mathcal{O}_{\mathcal{Z}_{\mathrm{r}}}(f))$, where $v = s(m_\Sigma \circ f)$.

Proof. (A.) Fix f and e such that (13) is true. Let $h \in \mathcal{O}_{\mathcal{G}}(f)$ such that $h(t) = \emptyset$ for all $t \in (\mathrm{I\!R}_0^+ \setminus \mathrm{Dom}(f))$.

1. If $\max \mathrm{Dom}(f)$ does not exist then define $\varrho = \sup \mathrm{Dom}(f)$.
2. If $\max \mathrm{Dom}(f)$ exists then define

$$\begin{aligned} X = \{ & t \in \mathrm{I\!R}_0^+ \setminus \mathrm{Dom}(f) \mid \\ & \exists w \in \mathcal{E}^+, \exists i \in I, \exists j \in \mathrm{I\!N}, 1 \le j \le n_i, \exists \sigma \in e_j \cap \Sigma_{c,i}, \\ & (\,(5) \wedge (6)\,)\ \wedge\ Z_\sigma(m_{V_i} \circ h|_{[0,t)}, s(m_{\Sigma_i} \circ w'))\ =\ C_\sigma(v)\ \} \end{aligned}$$

where $w = e_1 e_2 \dots e_n$ for some n, $e_k \in \mathcal{E}$ $(1 \le k \le n)$, and $w' = e_1 e_2 \dots e_{j-1}$. If $X \neq \emptyset$ then define $\max \mathrm{Dom}(f) < \varrho < \inf X$ else define $\max \mathrm{Dom}(f) < \varrho$.

Let $g \in \mathcal{O}_{\mathcal{G}}(h|_{[0,\varrho)})$ such $g(\varrho) = \{\mathbf{D}_a \mid i \in I \wedge a \in \Sigma_{c,i}\}$ and $g(t) = \emptyset$ for all $t \in (\varrho, \infty)$.

According to our construction of g and to the definitions of μ_o and μ_{r} we have for all $t \in \mathbb{R}_0^+ \setminus \mathrm{Dom}(f)$ that $m_U \circ g(t) \in \mu_{\mathrm{r}}(g, t)$. It implies using (12) that $g \in \mathcal{Z}_{\mathrm{r}}$. Thus $f \in \mathrm{pref}(\mathcal{Z}_{\mathrm{r}})$.

(B.) Thanks to definition of μ_o there is a $\varrho' \in (\varrho, \infty)$ such that for all $\sigma \in \Sigma$, D_σ is saturated, i.e. $D_\sigma(g|_{[0,\varrho)}) = 1$. Definition of β implies using the fact $e \in \beta(v)$ that for all $\sigma \in e$ exists some $M_\sigma < C_\sigma(v)$ the value of D_σ must be kept above in order to avoid generating a word not in $\mathrm{pref}(K)$. For all $\sigma \in e$ define $\Delta_\sigma = (1 - M_\sigma)/\bar{\kappa}_\sigma(v)$. Define $\varrho'' > \varrho'$ such that for all $\sigma \in e$, $\varrho'' - \Delta_\sigma > \varrho'$.

Construct $g' \in \mathcal{O}_{\mathcal{G}}(g|_{[0,\varrho']})$ such that $g'(t) = \emptyset$ $(t \in (\varrho', \infty))$ if it is not stated otherwise. Let for all $\sigma \in e$, $g'(\varrho'' - \Delta_\sigma) = \{\mathbf{E}_\sigma\}$ and $g(\varrho'') = \{\mathbf{D}_a \mid i \in I \wedge a \in \Sigma_{c,i}\}$. We have for all $\sigma \in e$, $D_\sigma(g'|_{[0,\varrho'']}) = M_\sigma$ therefore according to definition of μ_o there is $\varrho' \le \tau \le \varrho''$ such that $e \in \mu_o(g', \tau)$. The event e can occur, i.e. there is $g'' \in \mathcal{O}_{\mathcal{G}}(g'|_{[0,\tau)})$ such that $m_\Sigma \circ g''(\tau) = e$ and thanks to our construction for all $t \in [0, \tau]$, $m_U \circ g''(t) \in \mu_{\mathrm{r}}(g'', t)$. Using part A. of the proof setting $g''|_{[0,\tau]}$ for f we get $g''|_{[0,\tau]} \in \mathrm{pref}(\mathcal{Z}_{\mathrm{r}})$ and therefore $ve \in s(m_\Sigma \circ \mathcal{O}_{\mathcal{Z}_{\mathrm{r}}}(f))$. ■

Lemma V.2: For all $f \in \mathrm{prefb}(\mathcal{G})$ and $w \in \mathcal{E}^+$ such that

(i) $\forall t \in \mathrm{Dom}(f),\ m_U \circ f(t) \in \mu_{\mathrm{r}}(f, t)$,

(ii) $\forall j \in \mathbb{N}, 1 \le j \le m,\ e_j \in \beta(v e_1 e_2 \dots e_{j-1})$

this holds $vw \in s(m_\Sigma \circ \mathcal{O}_{\mathcal{Z}_{\mathrm{r}}}(f))$, where $w = e_1 e_2 \dots e_m$ for some m, and $v = s(m_\Sigma \circ f)$.

Proof. Using the previous lemma by finite induction on the length of w. ■

Theorem V.1: If K satisfies the conditions (i) – (v) of Theorem III.1 then $\mathcal{Z}_{\mathrm{r}}$ is a solution.

Proof. Condition (1) is satisfied because $\mathcal{Z}_{\mathrm{r}} \subseteq \mathcal{Z}$. Satisfaction of conditions (2) and (3) is implied using Lemma V.2 by (iii) and (iv) of Theorem III.1. ■

VI. Conclusion

The paper suggests a robust strategy for control of systems with hybrid controllability. The interpretation of integrator outputs can be different for different plants, e.g. velocity, distance, time, temperature. It enables to model in a simplified way "inertia" present often in real-world plants. The paper presents an attempt to find a balance between modelling power and tractability of problems.

Future research will be aimed to investigation of other hybrid components of discrete event plants and to issues related to observability and identification of parameters.

References

[1] P.J. Ramadge and W.M. Wonham, "Supervisory control of a class of discrete event processes", *SIAM J. Control Optim.*, vol. 25, pp. 206–230, Jan. 1987.

[2] P. Kozák, "Supervisory control of discrete event processes: A real-time extension", Technical Report # 1692, Czechoslovak Academy of Sciences, Prague, 1991, revised 1992.

[3] B.A. Brandin and W.M. Wonham, "Supervisory control of timed discrete-event systems", Technical Report # 9210, Control Science and Engineering, Dept. of El. Eng., Univ. of Toronto, Canada, 1992.

[4] P. Kozák, "Control of elementary discrete event systems: Synthesis of controller with non-zero decision time", in *Proc. of 1st IFAC Symp. on Design Methods of Control Systems*, pp. 457–462, Zurich, Switzerland, Sep. 1991. Pergamon Press, Oxford.

[5] P. Kozák, "Control of real-time discrete event systems with hybrid controllability of events", *in Proc. of 32st IEEE Conf. Decision and Control*, San Antonio, TX, USA, Dec. 1993.

[6] F. Lin, "Robust and adaptive supervisory control of discrete event systems", *in Proc. of 1992 American Control Conf.*, pp. 2804–2808, Chicago, IL, USA, June 1992.

[7] P. Kozák, "A unifying framework for discrete event system control theory", in *Discrete Event Systems: Modeling and Control*, pp. 95–109. Birkhäuser Verlag, Basel, Switzerland, 1993.

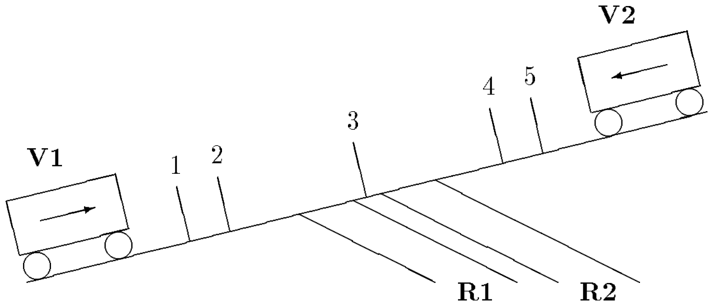


Figure 1: Example: vehicles on a hill road

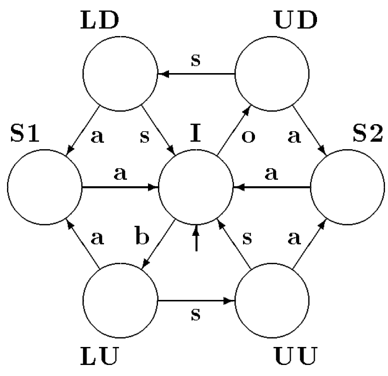


Figure 2: Example: Automata model of the plant

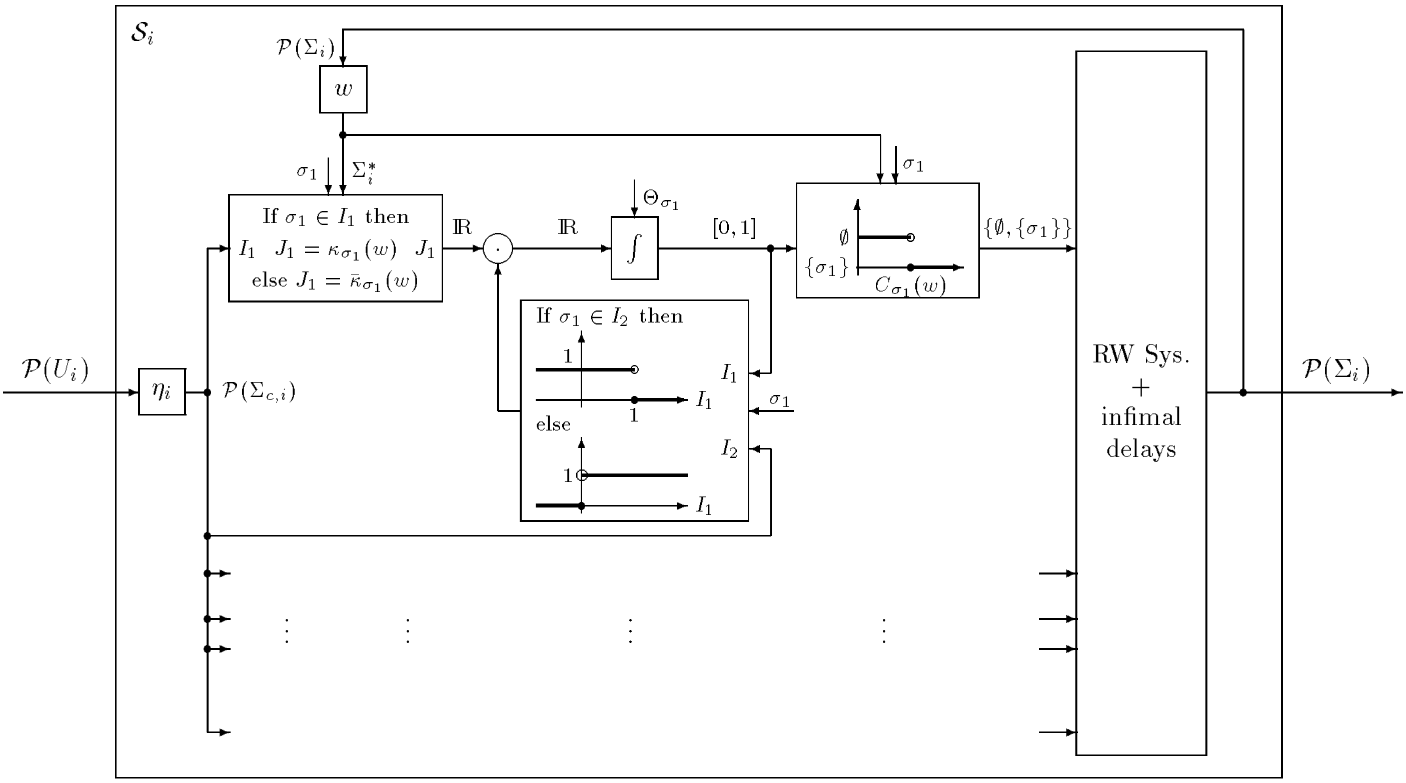


Figure 3: Model of the ith subsystem