Maximal Safe Set Computation for Idle Speed Control of an Automotive Engine

Andrea Balluchi[1], Luca Benvenuti[1,2], Maria D. Di Benedetto[2], Guido M. Miconi[1], Ugo Pozzi[1], Tiziano Villa[1], Howard Wong-Toi[3], and Alberto L. Sangiovanni–Vincentelli[1,4]

[1] PARADES, Via di S.Pantaleo, 66, 00186 Roma, Italy.
{alberto, balluchi, lucab, miconi, pozzi}@parades.rm.cnr.it
[2] Dip. di Ingegneria Elettrica, Università di L'Aquila, Poggio di Roio, 67040 L'Aquila, Italy, dibenede@giannutri.caspur.it
[3] Cadence Berkeley Labs, 2001 Addison St., Third Floor, Berkeley, CA 94704, USA. howard@cadence.com
[4] Dept. of Electrical Engineering and Computer Sciences, University of California at Berkeley, CA 94720, USA. alberto@eecs.berkeley.edu

Abstract. The specification for the idle control problem for automotive engines is to maintain the crankshaft speed within a given range in the presence of load changes. A new cycle-detailed hybrid model of the engine that captures well the interactions between the discrete phenomena of torque generation and spark ignition, and the continuous evolution of the power-train and air dynamics, is proposed. The idle control problem is formalized as a safety specification problem on the hybrid system. The Tomlin-Lygeros-Sastry procedure [12] is applied to compute the maximal controlled invariant set that satisfies the safety specification.

1 Introduction

The synthesis of a control strategy for an internal combustion engine in the idle regime is one of the most challenging problems in engine control. The objective is to maintain the engine speed as close as possible to the value that minimizes fuel consumption, while preventing the engine from turning off when a sudden load variation occurs. Load variations come from two sources: (1) from devices powered by the engine, such as the air conditioning system and the steering wheel servo-mechanism, or (2) from the driver changing the inertial load when operating the clutch pedal. A survey on different engine models and control design methodologies for the idle control is given in [8]. Both time–domain (e.g. [5]) and crank–angle domain (e.g. [13]) average–value models have been proposed in the literature. Several control design techniques have been applied to the idle control problem, such as multivariable control [10], ℓ_1 control [5], H_∞ control [6], μ-synthesis [7], sliding mode control [9] and LQ-based optimization [1].

In this paper, the idle control problem is specified as the one of keeping the crankshaft speed within a specified range, robustly with respect to load changes. The adoption of a hybrid formalism allows us to describe the cyclic behavior of the engine, thus capturing the effect of each spark ignition on the generated torque, the interaction between the discrete torque generation and the continuous power-train and air dynamics, and the discrete changes in the power-train. The torque that is generated by each cylinder and applied to the engine crankshaft can be assumed to be a function of the spark ignition time, and of the air-fuel mixture mass loaded in the cylinder during the intake phase. Since the air-to-fuel ratio is assumed to be constant (at the stoichiometric value), then the mixture mass is controlled by the throttle plate position and is subject to the dynamics of the cylinder filling due to the intake manifold. Hence, the available controls for the idle problem are: the spark ignition time and the position of the throttle valve, which regulates the air inflow[1]. The problem of maintaining the crankshaft speed within a given range is formalized as a safety specification for the hybrid closed-loop system. A *safety specification* is a state-invariance property, specifying a set of good states within which the closed-loop system must remain. A systematic procedure for computing the maximal safe set has been recently proposed by Tomlin, Lygeros, and Sastry [12]. This set consists of all the hybrid states for which there exists a hybrid control strategy (the maximal controller) that maintains the state in the set of good states forever, in spite of any discrete and continuous disturbance. The procedure is not guaranteed to terminate in a finite number of steps.

By applying this procedure to the hybrid model of the engine, the maximal safe set for the idle control is determined. We also obtain as a by-product the entire set of possible controllers that satisfy the constraints. We are free to choose among them the ones that optimize some criteria of choice. Moreover, considering the amount of load torque as a parameter, we can determine the maximum value for which a non empty maximal safe set (and, hence, at least one controller that satisfies the constraints) exists[2]. For parameters corresponding to commercial cars, the procedure has terminated in a few steps (typically six).

To summarize our main contribution, the use of a hybrid framework, where discrete and continuous signals are modeled in a separate but integrated manner, is a definite advantage over other approaches since it allows us to solve exactly the control problem while other approaches, where the system is approximated by either continuous [11], or discrete sampled [13] representations, obtain approximate solutions. The paper is organized as follows: in Section 2, a description of the engine in the idle region of operation is offered and its hybrid features are exposed. In Section 3, a *hybrid automaton model of the engine for*

[1] The effect of a spark command on the torque generation is more visible than the one of a throttle plate command, since air inflow is subject to both the manifold dynamics and the delay due to the mix compression. Hence, sudden loads can be much better compensated with spark ignition than with air inflow, while air inflow can be used to control the engine in steady state. For simplicity, we do not consider the throttle valve actuation dynamics.

[2] Butts *et al.* [5] solve a sort of dual problem: given a bounded torque load accessible to measurement, synthesize a robust ℓ_1 controller for a discrete–time model of the engine that minimizes the excursion of the crankshaft speed for the system initially at rest.

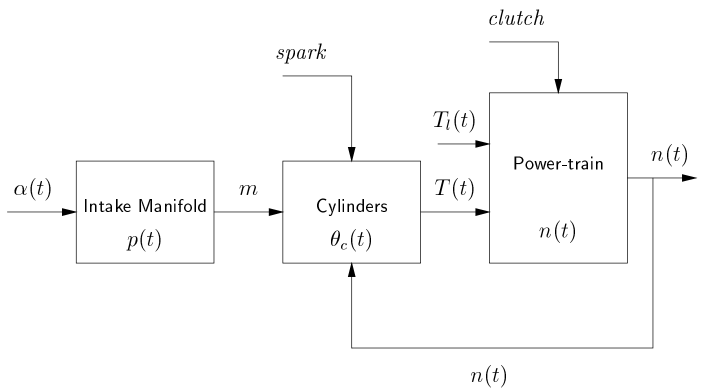


Fig. 1. The engine blocks and their communication topology.

the idle regime of operation is proposed for the *first* time. In Section 4, a general procedure for the calculation of the maximal controller is reviewed. In Section 5, the procedure is specialized to the idle control problem and some experimental results are described.

2 Description of the System

The overall system is composed of three main interacting blocks, namely the intake manifold, the cylinders and the power-train, as depicted in Figure 1. The manifold pressure p depends on the throttle valve angle α and determines the mass of air-fuel mixture m loaded by the cylinders. The torque T generated by the cylinders depends on both the mass m and the spark ignition time. Finally, the power-train dynamics and the crankshaft revolution speed n, controlled by the generated torque T, are subject to the sum of load torques T_l and the clutch position. In the sequel a detailed description of each block is reported.

Intake Manifold Dynamics. The mass of mix m entering a cylinder during the intake run is assumed to be proportional to the intake manifold pressure p at the end of the intake run. The pressure p is controlled by a throttle valve which changes the effective section of the intake manifold:

$$\dot{p}(t) \;=\; a_p p(t) + b_p \alpha(t) \; . \tag{1}$$

To prevent the choice of undesirable control laws that produce large excursions of the throttle valve, the throttle angle $\alpha(t)$ is constrained to belong to $[0, \alpha^{max}]$ with $\alpha^{max} = 20^0$.

Cylinders. In a 4–stroke combustion engine each cylinder cycles through the following four runs: intake (I), combustion (C), expansion (E) and exhaust (H).

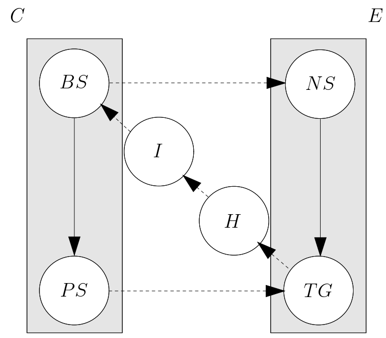


Fig. 2. Phases of a single cylinder: dashed lines denote transitions occurring when $\theta_c = 180$, solid lines denote transitions occuring when a spark ignition is given.

Ideally, spark ignition should occur exactly when the piston reaches the *top dead center* (TDC) configuration of the compression stroke. However, since combustion takes non-zero time to complete, it is convenient to produce a spark before the piston completes the compression stroke (*positive spark advance*), to achieve maximum fuel efficiency, i.e. the maximum torque generation. When a small value of torque is required, the spark can be ignited after the piston has completed the compression phase and is in the expansion stroke (*negative spark advance*).

Let θ_c denote the piston position, between two successive dead points, expressed in terms of the angle described by the crankshaft, obtained by the integration of the crankshaft velocity and by resetting θ_c to 0^0 when $\theta_c = 180^0$. The spark advance θ_s, defined as the angular distance from the TDC of the compression stroke, determines the crankshaft angular position at which the spark is given. It is positive for sparks given before the TDC ($\theta_s = 180^0 - \theta_c(t_s)$, where t_s is the ignition time), and negative otherwise ($\theta_s = -\theta_c(t_s)$). At the idle crankshaft speed, due to technological constraints, the feasible spark advances are $-15^0 \leq \theta_s \leq 20^0$. If the spark is ignited during the compression stroke, then C is split into two phases, namely BS (before spark) and PS (positive spark). Instead, if the spark is ignited during the expansion stroke, then E is split into two phases, namely NS (negative spark) and TG (torque generation). In the first case, the expansion stroke is represented by phase TG, while, in the second one, the compression stroke is represented by BS. The behavior of each piston is then characterized[3] by the six phases I, BS, PS, NS, TG and E, as shown in Figure 2.

When considering a 4-stroke internal combustion engine with four cylinders, the kinematics of the engine is such that, at any time, each cylinder is in a different stroke of the cycle. Since we assume that all the cylinders behave in

[3] When the spark ignition is synchronous with the TDC, we assume the cylinder leads from BS to TG through the phase PS.

the same way, then we can cluster all quadruples of cylinders' phases in only three engine phases, because it does not matter which cylinder is in a certain phase. Then, according to the ignition constraints $\theta_c \in [160^0, 180^0]$, in PS, and $\theta_c \in [0^0, 15^0]$, in NS, there are only three valid cylinder configurations and the discrete behavior of the system can be described by introducing the following three modes $S = (I, BS, TG, H)$, $S_+ = (I, PS, TG, H)$, $S_- = (I, BS, NS, H)$.

The transitions between S, S_+ and S_- are characterized as follows. In phase S, the cylinder in expansion is generating a torque (TG), and the cylinder in compression has not yet received the spark command (BS). If a spark ignition occurs before the end of the compression run, then the cylinder that is still in compression enters phase PS, which corresponds to the transition from S to S_+. Otherwise, at the TDC, the expansion phase starts (NS) and the transition from S to S_- takes place. In phase S_+, the spark command has been given for the cylinder in compression (PS), while the cylinder in expansion is generating a torque (TG). At the TDC, the cylinder which was in compression starts the expansion run entering phase TG, which corresponds to the transition from S_+ to S. In phase S_-, the cylinder in expansion is waiting for the spark command (NS), and the cylinder in compression has not received the spark command yet (BS). It is worth noting that no torque is generated in this case. When the spark ignition is given, the cylinder which is still in the expansion run changes from NS to TG, and the transition from S_- to S takes place.

The evolution of the torque, generated by each piston during the expansion phase, depends on the thermodynamics of the air-fuel mixture combustion. To simplify the model, we represent by T the average value of the torque generated over the expansion phase. Such value is proportional to the air m loaded in the cylinder during the intake phase and to the ignition efficiency (increasing) function $\eta(\theta_s) \leq 1$.

Since there is a delay from the time the air mass m is trapped in the cylinder and the time the torque is generated, the amount of loaded air mass must be stored for each cylinder. To this end, we introduce two variables, m_C and m_E denoting, respectively, the mass of air trapped at the end of the intake run in the cylinder starting the compression run, and the mass of air trapped at the end of the compression run in the cylinder starting the expansion run. Hence, the torque T produced by each piston is expressed as

$$T = \begin{cases} G\,\eta(\theta_s)\,m_C & \text{for positive spark advance,} \\ G\,\eta(\theta_s)\,m_E & \text{for negative spark advance.} \end{cases} \tag{2}$$

The torque $T(t)$ generated by the engine is obtained by applying a zero order hold block to each cylinder output T, and summing all the piecewise constant contributions of the pistons.

Power-train Dynamics. When the clutch is pushed, under the action of the torque $T(t)$ generated by the engine, the crankshaft speed evolution is determined by the following mechanical equations

$$\dot{n}(t) = a_n n(t) + b_n(T(t) - T_l(t)) \quad (3)$$
$$\dot{\theta}_c(t) = k_c n(t) \quad (4)$$

where $a_n = -B/J$ and $b_n = 1/J$, with J and B denoting the inertial momentum and the viscous friction coefficient of the segment of the power-train from the crankshaft to the clutch, respectively. If θ_c is in degrees and n is in revolutions per minute, then $k_c = 6$. When the clutch is released, the coefficients a_n and b_n are replaced by $a_n^L = -B/(J + J')$ and $b_n^L = 1/(J + J')$, where J' denotes the inertial momentum of the primary drive-line.

Finally, the torque load T_l is assumed to belong to $[0, T_l^{\max}]$, where the value $T_l^{\max}$ is treated as a parameter for the control problem.

3 Hybrid Model of the Engine

We model the mixed discrete-continuous dynamics of the engine as a hybrid automaton. We consider a particular class of hybrid automata characterized by a set of discrete *locations* (also called *modes*) corresponding to the FSM states, a set of continuous variables and a set of piecewise-constant variables. The controller and the environment act on the system with two kinds of inputs: the continuous inputs affect the continuous dynamics; the discrete inputs determine the discrete mode transitions, the resetting of continuous variables and the setting of symbolic constants. This modeling formalism combines the features of [2] with elements of the hybrid dynamics of [12]. The formal definition and the behavior of this hybrid automaton is analogous to the one described in [4], with the separation between continuous variables and piecewise-constant variables explicitly introduced here. The hybrid model of the 4-stroke 4-cylinder internal combustion engine has six modes S_-, S, S_+, S_-^L, S^L, and S_+^L, derived from the three modes S_-, S, and S_+ of the four cylinders and the two discrete positions of the clutch, which can be either closed or open. Figure 3 shows the resulting hybrid automaton. Hence, we can formally write the engine hybrid automaton as a tuple $H = (\{Q, X, \Xi\}, \{\Sigma_c, U\}, \{M_c^{disc}, M_c^{cts}\}, \{\Sigma_e, D\}, \{M_e^{disc}, M_e^{cts}\}, \{f, \delta\})$, where:

- the **state space** is composed of the finite set of *modes* or *locations* Q, which consists of $S_-, S, S_+, S_-^L, S^L, S_+^L$, the space of *continuous variables* $X = \{(p, n, \theta_c) \mid (p, n, \theta_c) \in \mathbb{R}^3\}$, and the space of *piecewise-constant variables* $\Xi = \{(T, m_C, m_E, \theta_s) \mid (T, m_C, m_E, \theta_s) \in \mathbb{R}^4\}$. An element (q, x, ξ) in the space $Q \times X \times \Xi$ is called a *configuration*;
- the **control inputs** $\alpha(t)$ and σ_c can be described by means of the domain of continuous input values $U = [0, \alpha^{max}]$, the finite domain of *discrete control events* $\Sigma_c = \{spark\}$ with $\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$ being the set of *discrete control moves* and the special ϵ move being the *silent* move, the *discrete controller feasible move function* $M_c^{disc} : Q \times X \times \Xi \to 2^{\Sigma_c^\epsilon} \setminus \{\}$ described as follows[4]:

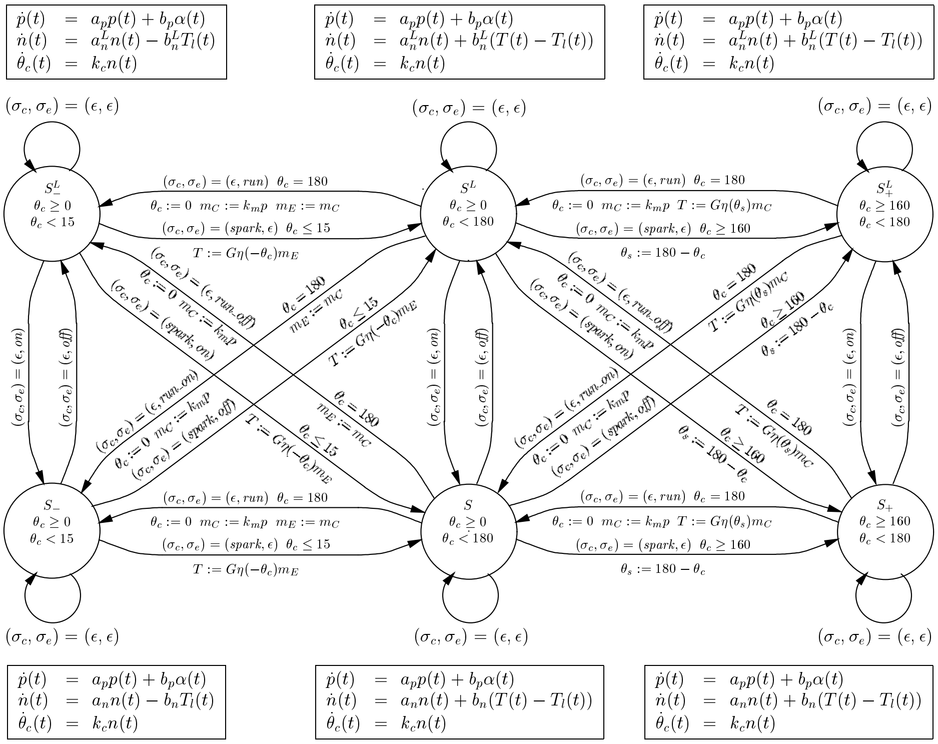


Fig. 3. Hybrid model for the engine running at minimum.

$$
\begin{array}{ll}
M_c^{disc}(S_+, \theta_c \leq 180^0) = \{\epsilon\} & M_c^{disc}(S_+^L, \theta_c \leq 180^0) = \{\epsilon\} \\
M_c^{disc}(S_-, \theta_c < 15^0) = \{\epsilon, spark\} & M_c^{disc}(S_-^L, \theta_c < 15^0) = \{\epsilon, spark\} \\
M_c^{disc}(S_-, \theta_c = 15^0) = \{spark\} & M_c^{disc}(S_-^L, \theta_c = 15^0) = \{spark\} \\
M_c^{disc}(S, \theta_c < 160^0) = \{\epsilon\} & M_c^{disc}(S^L, \theta_c < 160^0) = \{\epsilon\} \\
M_c^{disc}(S, 160^0 \leq \theta_c \leq 180^0) = \{\epsilon, spark\} & M_c^{disc}(S^L, 160^0 \leq \theta_c \leq 180^0) = \{\epsilon, spark\}
\end{array}
$$

and the *continuous controller feasible move function* $M_c^{cts} : Q \times X \times \Xi \rightarrow 2^U \setminus \{\}$ described as follows: $M_c^{cts}(q, x, \xi) = \{\alpha \mid \alpha \in [0,\ \alpha_{max} = 20°]\},\ \forall (q, x, \xi)$;

- the **disturbance inputs** $T_l(t)$ and σ_e can be described by means of the domain of *continuous disturbance values* $D = [0, T_l^{\max}]$, the finite set of *discrete disturbance events* $\Sigma_e = \{on,\ off,\ run,\ run\_on,\ run\_off\}$ (where the events *on* and *off* represent opening and closing the discrete position of the clutch, the event *run* represents reaching the boundary $\theta_c = 180^0$ for the continuous state, the events *run_on* and *run_off* represent the simultaneous occurrence of a clutch operation and reaching the boundary, and $\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$ is the set of *discrete disturbance moves*), the *discrete disturbance move function* $M_e^{disc} : Q \times X \times \Xi \rightarrow$

[4] Notice that $M_c^{disc}(S_-, \theta_c = 15^0) = \{spark\}$ is a discrete control move required when the spark was not given yet and must be given now, since it is the last valid ignition time instant.

$2^{\Sigma_e^\epsilon} \setminus \{\}$ described as follows[5]:

$$\begin{array}{ll}
M_e^{disc}(S_+, \theta_c < 180^0) = \{\epsilon, \mathit{off}\} & M_e^{disc}(S_+^L, \theta_c < 180^0) = \{\epsilon, \mathit{on}\} \\
M_e^{disc}(S_+, \theta_c = 180^0) = \{\mathit{run}, \mathit{run_off}\} & M_e^{disc}(S_+^L, \theta_c = 180^0) = \{\mathit{run}, \mathit{run_on}\} \\
M_e^{disc}(S_-, \theta_c \le 15^0) = \{\epsilon, \mathit{off}\} & M_e^{disc}(S_-^L, \theta_c \le 15^0) = \{\epsilon, \mathit{on}\} \\
M_e^{disc}(S, \theta_c < 180^0) = \{\epsilon, \mathit{off}\} & M_e^{disc}(S^L, \theta_c < 180^0) = \{\epsilon, \mathit{on}\} \\
M_e^{disc}(S, \theta_c = 180^0) = \{\mathit{run}, \mathit{run_off}\} & M_e^{disc}(S^L, \theta_c = 180^0) = \{\mathit{run}, \mathit{run_on}\}
\end{array}$$

and the *continuous disturbance feasible move function*: $M_e^{cts} : Q \times X \times \Xi \to 2^D \setminus \{\}$ described as follows: $M_e^{cts}(q, x, \xi) = \{T_l \mid T_l \in [0, T_{l\,max}]\}$, $\forall\,(q, x, \xi)$;

- the **transitions** are described by $f : Q \times X \times \Xi \times U \times D \to \mathbb{R}^n$ which models the time-invariant continuous dynamics, which depend on the mode[6] and the *transition function* $\delta : Q \times X \times \Xi \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X \times \Xi} \setminus \{\}$ modeling the discrete dynamics, as depicted in Fig. 3.

4 Synthesis of Hybrid Static State Feedback Controllers

The engine control problem at hand belongs to the class of *safety* problems. A *safety property* $\mathcal{P}$ asserts that nothing "bad" happens along trajectories and can be expressed by specifying a subset *Good* of the configuration space ($Q \times X \times \Xi$). The co-set of *Good* is called *Bad*. The hybrid automaton H, with initial configurations $(Q \times X \times \Xi)_0 \subseteq \mathit{Good}$, is *safe* with respect to the safety property $\mathcal{P}$ if there exists a control strategy that guarantees all its trajectories that start in $(Q \times X \times \Xi)_0$ remain within *Good*. The maximal safe set, *Safe*, is the maximal subset $(Q \times X \times \Xi)_0$ of *Good* for which the hybrid automaton H is safe with respect to $\mathcal{P}$, i.e., the maximal robust-controlled invariant set of configurations contained in *Good*. The maximal controller is the class of all the hybrid static state-feedback control strategies that guarantee that all the trajectories starting in *Safe* remain within *Good*.

For the hybrid automaton described in Section 3, we define *Good* as the set of configurations for which the crankshaft speed is within the range $[770, 830]$, i.e., $\mathit{Good} = \{(q, x, \xi) \in Q \times X \times \Xi \mid 770 \le n \le 830\}$. The design of a controller requires the computation of the maximal safe set *Safe*.

Computing the maximal safe set [12]. This set is obtained by first overapproximating it with all the good configurations. Then all configurations are obtained from which the environment can drive the system into an unsafe configuration via either one discrete jump, or one continuous flow. These are the configurations from which the environment can push the system into *Bad* in one "step",

[5] Notice that $M_e^{disc}(S_+, \theta_c = 180^0) = \{\mathit{run}, \mathit{run\_off}\}$, $M_e^{disc}(S_+, \theta_c = 180^0) = \{\mathit{run}, \mathit{run\_on}\}$, $M_e^{disc}(S, \theta_c = 180^0) = \{\mathit{run}, \mathit{run\_off}\}$ and $M_e^{disc}(S^L, \theta_c = 180^0) = \{\mathit{run}, \mathit{run\_off}\}$ model discrete moves forced by the continuous state.

[6] We specify the continuous dynamics f by defining functions $f_q : X \times \Xi \times U \times D \to X$ for each $q \in Q$. The functions f_q, as specified in Figure 3, are taken from (1), (3) and (4).

and should be avoided by the controller. One iterates this computation, finding successively the configurations from which the environment can push the system into *Bad* in i steps. If the procedure terminates, we have determined the maximal safe set. The procedure is already described in full detail in [12, 3]; here, we report only the definitions of the predecessor operators required to capture the previous notions.

Discrete uncontrollable predecessors operator $Pre_e : 2^{(Q\times X\times \Xi)} \rightarrow 2^{(Q\times X\times \Xi)}$:

$$\begin{aligned} Pre_e(K) \;=\; & \{(q,x,\xi) \in Q \times X \times \Xi : \\ & \forall \sigma_c \in M_c^{disc}(q,x,\xi)\, \exists \sigma_e \in M_e^{disc}(q,x,\xi) \textit{ such that} \\ & (\sigma_c,\sigma_e) \neq (\epsilon,\epsilon) \;\wedge\; \delta(q,x,\xi,\sigma_c,\sigma_e) \not\subseteq K\}. \end{aligned}$$

Discrete controllable predecessors operator $Pre_c : 2^{(Q\times X\times \Xi)} \rightarrow 2^{(Q\times X\times \Xi)}$:

$$\begin{aligned} Pre_c(K) \;=\; & \{(q,x,\xi) \in Q \times X \times \Xi : \\ & \exists \sigma_c \in M_c^{disc}(q,x,\xi) \textit{ such that}\, \forall \sigma_e \in M_e^{disc}(q,x,\xi) \\ & (\sigma_c,\sigma_e) \neq (\epsilon,\epsilon) \;\wedge\; \delta(q,x,\xi,\sigma_c,\sigma_e) \subseteq K\}. \end{aligned}$$

Continuous uncontrollable predecessor operator[7]
$Unavoid\_Pre : 2^{(Q\times X\times \Xi)} \times 2^{(Q\times X\times \Xi)} \rightarrow 2^{(Q\times X\times \Xi)}$:

$$\begin{aligned} Unavoid\_Pre(B,E) \;=\; & \{(q,\hat{x},\xi) \in Q \times X \times \Xi \mid \\ & \forall u \in \mathcal{U}\ \exists \bar{t} > 0\ \exists d \in \mathcal{D} \textit{ such that, for the trajectory} \\ & x(t) = \psi_q(u,d,\hat{x},\xi)(t) \textit{ we have: } (q, x(\bar{t},\xi)) \in B \;\wedge \\ & \forall \tau \in [0,\bar{t}\,)\ [u(\tau) \in M_c^{cts}(q,x(\tau),\xi) \;\wedge \\ & d(\tau) \in M_e^{cts}(q,x(\tau),\xi) \wedge (q,x(\tau),\xi) \in Wait\, \cap \overline{E}]\ \} \end{aligned}$$

Figure 4 shows the fixed-point computation to obtain the maximal safe set. The procedure successively prunes away configurations that are found to lead to a bad configuration upon one additional discrete step ($Pre_e(W^i)$), or a continuous step to a bad configuration ($Unavoid\_Pre(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i))$). It is not guaranteed to stop in a finite number of steps.

A hybrid controller watches the entire state of the system at all times, and decides whether to (1) take discrete control actions that may cause an instantaneous change in the configuration, or to (2) let time pass under a continuous input u with the continuous variables evolving according to dynamics at the current mode. The formal definition of a safe hybrid controller and the rules which allow its extraction by the description of the maximal safe set are described in [4].

[7] We define $\mathcal{U} = \{u(.) \in PC^0 | u(t) \in U, \forall t \in \mathbb{R}\}$ and $\mathcal{D} = \{d(.) \in PC^0 | d(t) \in D, \forall t \in \mathbb{R}\}$, and we denote by *Wait* the set of configurations in which both players may choose not to play a discrete move, but instead wait for time to pass: $Wait = \{(q,x,\xi) \mid \epsilon \in M_c^{disc}(q,x,\xi) \text{ and } \epsilon \in M_e^{disc}(q,x,\xi)\}$. Trajectories at location q from initial state $(\hat{x},\xi)$ following $u \in \mathcal{U}$ and $d \in \mathcal{D}$ are denoted $\psi_q(u,d,\hat{x},\xi)$.

$W^0 := \mathit{Good}$
$i := -1$
repeat {
  $i := i + 1$
  $W^{i+1} := W^i \setminus [\mathit{Pre}_e(W^i) \cup \mathit{Unavoid\_Pre}(\mathit{Pre}_e(W^i) \cup \overline{W^i}, \mathit{Pre}_c(W^i))]$
} until $(W^{i+1} = W^i)$
$\mathit{Safe} := W^i$

Fig. 4. Computation of Maximal Safe Set [12].

5 Computation of the Maximal Safe Set for the Engine System

The parameters of the hybrid model M of the engine running at idle have been identified by measurements provided by the Powertrain Division of Magneti Marelli on a commercial engine.

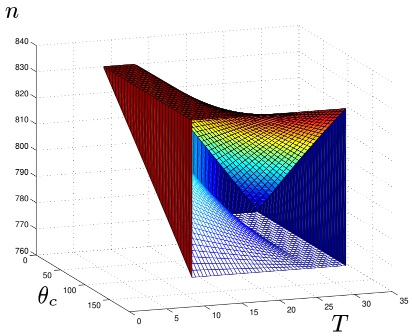
In this section, for simplicity, we restrict the computation of the maximal safe set to the case in which only a positive spark advance is considered. In this case, the engine system is represented by the hybrid automaton M which consists of four discrete modes (S, S_+, S^L, S_+^L).

In M, there is a symmetry between the modes S, S_+ (subsystem M_2) and the mirror modes S^L, S_+^L (subsystem M_2^L). This allows the computation of the maximal safe set as follows: first, the maximal safe set is computed for the system M_2 representing the engine with the clutch open; then, using the previous results, the maximal safe set is derived for M_2^L representing the engine with the clutch closed; finally, the maximal safe set for the overall system M is obtained.

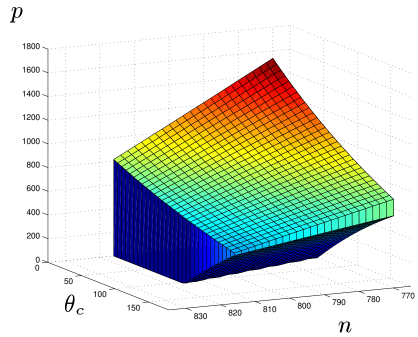
The procedure reported in Section 4 is quite complex when applied to M_2, due to the dimension of the continuous state space. However, since the set *Good* involves only the variable n, and variables (n, T, θ_c) are de-coupled from the remaining ones, we can apply a divide-and-conquer strategy: the procedure is applied first in the subspace (n, T, θ_c); then, using (2), the safe values for the variable m_C are obtained in terms of n, T, θ_c and θ_s. Finally, from the safe values of the air mass, the safe values for the manifold pressure p are obtained, so that the overall maximal safe set Safe^{M_2} for the hybrid subsystem M_2 is derived. For the engine parameters of our model, this computation terminates in six iterations.

Due to symmetry, the maximal safe set for M_2^L is computed as the one for M_2, yielding a result differing only in the coefficients of the crankshaft speed: when the clutch pedal is released the crankshaft inertial load increases, and $a_n^L < a_n$; $b_n^L < b_n$. Comparing the maximal safe sets for M_2 and M_2^L, it holds:

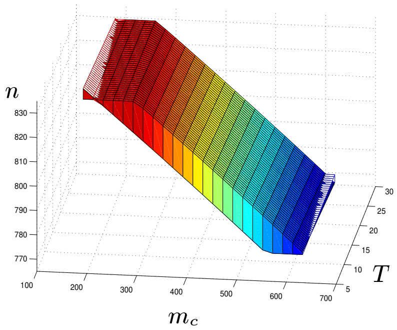
$$\begin{aligned} \mathit{Safe}^{M_2}|_S &\subset \mathit{Safe}^{M_2^L}|_{S^L}, \\ \mathit{Safe}^{M_2}|_{S_+} &\subset \mathit{Safe}^{M_2^L}|_{S_+^L}. \end{aligned} \tag{5}$$



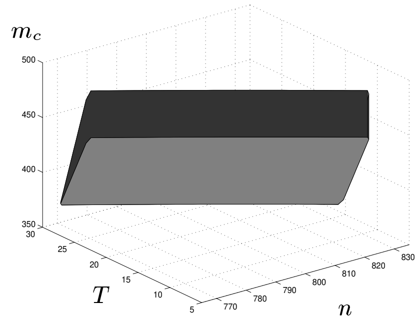
(a) Modes S and S^L, space (n, T, θ_c)



(b) Modes S and S^L, space (p, n, θ_c), with $T = 15Nm$ and $m_C = 480\mu g$



(c) Modes S_+ and S_+^L, space (n, T, m_C), with $\theta_c = 180° - \theta_s$ and $\theta_s = 10°$



(d) Modes S and S^L, space (n, T, m_C), with $\theta_c = 0°$

Fig. 5. Maximal Safe Set for the Engine System M

Finally, we consider the system M which contains the subsystems M_2 and M_2^L together with the uncontrollable transitions $S \leftrightarrows S^L$, $S_+ \leftrightarrows S_+^L$, $S \leftrightarrows S_+^L$ and $S^L \leftrightarrows S_+$. In summary, one can prove the following:

Proposition 1. *If $Safe^M$ is the maximal safe set for the engine system M,*

$$\begin{aligned} Safe^M|_S &= Safe^M|_{S^L} = Safe^{M_2}|_S, \\ Safe^M|_{S_+} &= Safe^M|_{S_+^L} = Safe^{M_2}|_{S_+}. \end{aligned} \tag{6}$$

The maximal safe set for M is shown in Figure 5. Since the dimensions of the safe set are higher than three, it is difficult to visualize it. The three figures are projections of the safe set on different axes. The projection of the safe set on the subspace n, T, θ_c, shown in Figure 5(a) for modes S and S^L, does not depend on the value of the other state components p, m_C, θ_s. Note that the range of safe values for the speed n increases as θ_c increases, whenever a given torque T is considered. This corresponds to the fact that the greater the values of θ_c, the shorter is the interval of time on which the load torque may act to drive n outside the good range $[770, 830]$, before the next dead point is reached and a new driving torque T may be applied.

Figure 5(b) presents the dependencies among p, n, θ_c, in modes S and S^L, for given values of T and m_C. Note that the safe values for θ_s are obtained by (2), which holds in S and S^L. For a fixed value of θ_c, there is an inverse dependence between the safe values of p and those of n. In fact, the greater the values of n, the smaller the values of p have to be in order to produce a small torque in the next expansion phase.

For modes S_+ and S_+^L, safe set projections similar to those in Figure 5(a) and Figure 5(b) can be shown.

The safe values for θ_s are given by the relationship with n, T, m_C, and θ_c depicted in Figure 5(c). Note the inverse dependence between the safe values of m_C and the ones of n. The reason for this dependency is that, for high values of n, small values of m_C need to be applied in order to produce low values of torque T in the next expansion phase, so as to prevent the engine speed from exceeding the upper limit 830.

Figure 5(d) shows, for each safe couple (n, T) at the beginning of the engine phase ($\theta_c = 0$), the interval of values to which m_C must belong to produce a torque that maintains the speed engine n in the good range, provided that an appropriate value of θ_s is chosen.

The condition under which a non-empty maximal safe set exists for the engine hybrid model has been analytically determined in terms of the model parameters. By this result, the maximum value of the torque load for which there exists a non-empty maximal safe set was found to be 12.8 Nm for an engine of a commercially available vehicle.

6 Conclusions

The problem of maintaining the crankshaft speed within a given range has been formalized for the first time as a safety specification for the closed-loop system modeled as a hybrid automaton, where continuous and discrete variables retain their distinctive nature. By applying a systematic procedure to the hybrid model of the engine, the maximal safe set for the idle control has been determined. We also obtained as a by-product the entire set of possible controllers that satisfy the constraints. This, in addition to the capability of modeling in a separate but integrated manner discrete and continuous signals, is a definite advantage over other approaches that approximate the system by relaxing it to continuous or discrete sampled representations. This result is the first of its kind in idle control, and allows us to determine tightly the maximum range of allowed torque disturbances, given the maximum interval of angular speed values. Further, from an application point of view, the relevance of this computation lies in the fact that it provides the upper bounds on the best performance achievable by an idle speed control strategy for a given engine.

The systematic procedure for the safe set computation cannot be guaranteed to converge in a finite number of steps in the general case. However, in the engine model available to us it converged in six steps. We are presently investigating the properties of the model and the range of parameters with respect to the size and the shape of the the corresponding maximal safe set for the idle engine control problem.

7 Acknowledgments

This research is sponsored in part by CNR, the CNR MADESS Project, a grant from Magneti Marelli and from Cadence Design Systems. The support of and the interaction with Dr. Carlo Rossi and Dr. Gabriele Serra of Magneti Marelli, Power-train Division, is gratefully acknowledged.

References

1. M. Abate and V. Di Nunzio. Idle speed control using optimal regulation. Technical Report 905008, SAE, 1990.
2. E. Asarin, O. Maler, A. Pnueli, and J. Sifakis. Controller synthesis for timed automata. In *Proceedings of System Structure and Control*. IFAC, Elsevier, July 1998.
3. A. Balluchi, L. Benvenuti, H. Wong-Toi, T. Villa, and A. L. Sangiovanni-Vincentelli. A case study of hybrid controller synthesis of a heating system. In *Proc. 5th European Control Conference*, Karlsruhe, Germany, September 1999.
4. A. Balluchi, L. Benvenuti, H. Wong-Toi, T. Villa, and A. L. Sangiovanni-Vincentelli. Controller synthesis for hybrid systems with lower bounds on event separation. In *Proc. 37th IEEE Conference on Decision and Control*, December 1999.
5. K. R. Butts, N. Sivashankar, and J. Sun. Application of ℓ_1 optimal control to the engine idle speed control problem. *IEEE Trans. on Control Systems Technology*, 7(2):258–270, March 1999.
6. C. Carnevale and A. Moschetti. Idle speed control with H_∞ technique. Technical Report 930770, SAE, 1993.
7. D. Hrovat and B. Bodenheimer. Robust automotive idle speed control design based on μ-synthesis. In *Proc. IEEE American Control Conference*, pages 1778–1783, S. Francisco, CA, 1993.
8. D. Hrovat and J. Sun. Models and control methodologies for IC engine idle speed control design. *Control Engineering Practice*, 5(8), August 1997.
9. L. Kjergaard, S. Nielsen, T. Vesterholm, and E. Hendricks. Advanced nonlinear engine idle speed control systems. Technical Report 940974, SAE, 1994.
10. C. H. Onder and H. P. Geering. Model-based multivariable speed and air-to-fuel ratio control of a SI engine. Technical Report 930859, SAE, 1993.
11. D. Shim, J. Park, P. P. Khargonekar, and W. B. Ribbens. Reducing automotive engine speed fluctuation at idle. *IEEE Trans. on Control Systems Technology*, 4(4):404–410, July 1996.
12. C. Tomlin, J. Lygeros, and S. Sastry. Synthesizing controllers for nonlinear hybrid systems. In Thomas Henzinger and Shankar Sastry, editors, *First International Workshop, HSCC'98, Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science 1386, pages 360–373, 1998.

13. S. Yurkovich and M. Simpson. Crank-angle domain modeling and control for idle speed. *SAE Journal of Engines*, 106(970027):34–41, 1997.