# Motor-Transmission Drive System: a Benchmark Example for Safety Verification

Hongxu Chen
State Key Laboratory of Automotive Safety and Energy
Tsinghua University
Beijing 10084, China
herschel.chen@gmail.com

Sayan Mitra
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, IL 61801, USA
mitras@illinois.edu

Guangyu Tian
State Key Laboratory of Automotive Safety and Energy
Tsinghua University
Beijing 10084, China
tian_gy@tsinghua.edu.cn

## ABSTRACT

This paper introduces the Motor-Transmission Drive System as a benchmark example for the safety analysis of hybrid systems. In particular, we illustrate the problem of checking the gear meshing duration and the impact impulse (both of which we refer to as safety) of the Motor-Transmission Drive System. We aim to provide a complete problem description to which different verification tools or approaches for safety analysis can be applied and compared. For this reason, we first elaborate on a hybrid automaton (HA) model of the Motor-Transmission Drive System to describe the gear meshing process with uncertain initial states, and then we specify the safety property of interest. Next, we clarify the characteristic phenomena exhibited by the benchmark which make the verification problem hard to solve. Finally, we show some simulation results to illustrate the influences of the initial states on the safety property. This benchmark example can help the researchers and engineers to find appropriate methods for safety verification of this kind of hybrid system.

**Category:** industrial **Difficulty:** medium

## 1. INTRODUCTION

In recent years, hybrid systems have proved their significance in safety critical applications such as automotive control systems. However, the safety verification has always been a challenge because of their complex behavior. In practice, a rigorous tool is still not available for verifying every class of hybrid systems. For different benchmark examples, tools have shown their own strengths and weaknesses [10,11,14]. This has prompted researchers and engineers to seek efficient tools or approaches to verify the safety property of their designs. On one hand, they apply different methods to the same benchmark problem, and the comparison to the results can reveal the limits of a certain method, which are helpful to determine whether the method is suitable for a certain verification problem at all. On the other hand, if the researchers or engineers decide to use a method, knowing its limits can help them modify the model so that the method can be used.

In this paper, we introduce the Motor-Transmission Drive System that we propose as a benchmark example for evaluating and comparing tools or approaches for the safety verification of hybrid systems. Unlike traditional powertrains where a clutch disengages the power input of the engine during the shifting process, in this transmission system, the rotor of the electric motor is directly connected to the input shaft of the transmission (see Figure 1). For shifting gears, a sleeve is pushed by a shift actuator to first disengage from one gear and then to mesh with another gear. This makes the shifting process tricky. If the sleeve arrives at the target gear at an improper angular position, then it can delay the meshing process or worse still, lead to physical impacts [13] (see Figure 2). The impacts make this a hybrid system [12]: the sleeve moves continuously until it hits the gear; at which point its velocities change (al-

most) instantaneously; after which it continues to evolve continuously again.

We aim to provide a high-fidelity model to which different verification tools or approaches for safety analysis can be applied and compared. First, we elaborate on a hybrid automaton (HA) model $\mathcal{A}$ of the Motor-Transmission Drive System. More specifically, our model captures the trajectory of the sleeve relative to the target gear during the meshing process. The initial states of this model capture the uncertainties about the initial relative angular positions and speeds of the sleeve and gear. Based on the HA model, we specify the safety property of interest—the sleeve with a constant shifting force can mesh with the gear within a desired time and an impact impulse bound from every initial state. Next, we clarify that the potential non-deterministic switching at a certain condition reveals the nondeterminism of the HA model $\mathcal{A}$ and the uncertain number of guards brings a more conservative approximation. Both of the characteristic phenomena make the verification problem hard to solve. Finally, by comparing two trajectories from two different initial positions, we show the influences of the initial states on the safety property.

*Related work.* Over the years, a number of automotive control systems have been used in the literature to evaluate and compare safety verification tools or approaches (see, for example, recent proceedings of Hybrid Systems: Computation and Control (HSCC) [1,2]). Stauner et al. modeled the pneumatic suspension system in [17] as a hybrid automaton with linear dynamics, and then used HyTech to verify its safety property—the height of the car maintains within a desired bound. Later, after slight modification, simplification or additional assumptions to the model, Bemporad [5], Elia [7], and Fehnker [8] applied alternative approaches to the same safety verification problem and obtained different results. Moreover, Fehnker also used electronic throttle control system in [9] to illustrate the process that leads from the informal specification to verification. In [9], he decomposed the verification problem into a series of smaller verification problems and solved them by the CheckMate which is stated in [6]. With the reachability-based technique in [15], S. Bak designed and verified a supervisory controller that prevents rollover of an autonomous off-road vehicle in [3, 4].

## 2. MODELING MESHING PROCESS

In this section, we describe a HA model $\mathcal{A}$ of the trajectory of the sleeve during the meshing process (see Figure 3). Consider a gear shift from first to second. As shown in Figure 4, the second gear is spread out into a plane, and 2D plane coordinates are established on it. The sleeve is modeled by a point $(p_x, p_y)$ moving

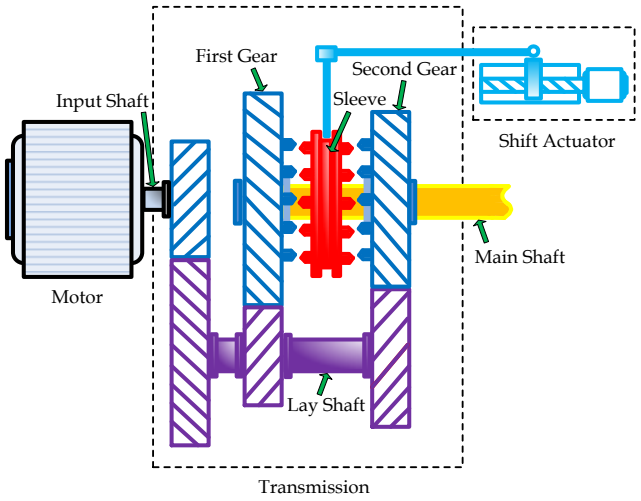
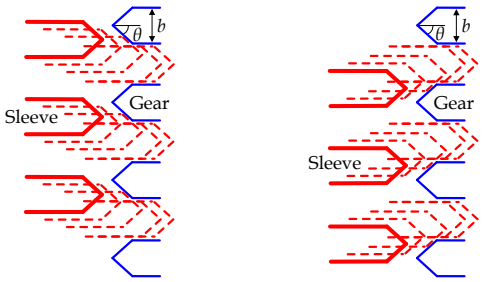



Figure 1: The configuration of the Motor-Transmission Drive System.




(a) case1 (b) case2

Figure 2: For some initial position of the sleeve relative to the target gear, direct lateral movement of the sleeve leads to impact with the gear, which delays the meshing.

on the plane according to linear differential equations called *free movement ODEs* (3). Along the $x$ direction, a constant force ($F_s$) acts on the sleeve, and the sleeve has a velocity $v_x$. Along the $y$ direction, some resisting moments ($T_f$) act on the second gear, and the gear has a relative angular speed ($\omega_r$) to the sleeve (that is, the sleeve has a velocity $v_y = \omega_r \cdot R_s$). When the point hits one of the line segments (that is, the sleeve hits the gear), a value discrete transition happens—when the point hits Line 1, the *guard* is denoted by $G_{1n}$ as $G_{1n} \triangleq \{(p_y - 2nb)/p_x \geq -tan\theta\} \wedge \{\Delta p \geq p_x \geq -b/tan\theta\} \wedge \{v_x sin\theta + v_y cos\theta > 0\}$ and the values of $\mathbf{x}$ are reset according to $\mathbf{x}' = A_1\mathbf{x}$; when the point hits Line 2, the *guard* is denoted by $G_{2n}$ as $G_{2n} \triangleq \{(p_y - 2nb)/p_x \leq tan\theta\} \wedge \{\Delta p \geq p_x \geq -b/tan\theta\} \wedge \{v_x sin\theta - v_y cos\theta > 0\}$

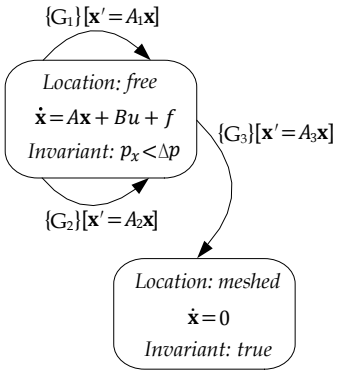



Figure 3: The hybrid automaton model specifies the continuous-time dynamics and discrete transitions of the trajectory of the sleeve during the meshing process.

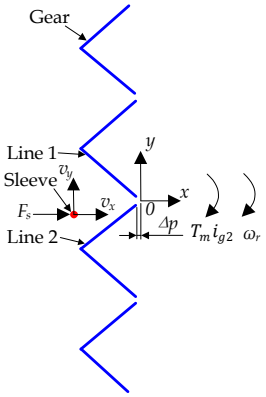



Figure 4: The gear is captured by set of stationary line segments in the 2D plane, the sleeve is modeled as a point, and the coordinates are established on the gear.

Table 1: Physical model parameters and values

| | | |
|---|---|---|
| $\zeta$ | 0.9 | Coefficient of restitution |
| $m_s$ | 3.2 $(kg)$ | Mass of sleeve |
| $m_{g_2}$ | 18.1 $(kg)$ | Mass of second gear |
| $J_{g_2}$ | 0.09 $(kg \cdot m^2)$ | Inertia of second gear |
| $i_{g_2}$ | 3.704 | Gear ratio of second gear |
| $R_s$ | 0.08 $(m)$ | Radius of sleeve |
| $\theta$ | 36 $(^0)$ | Included angle of gear |
| $b$ | 0.01 $(m)$ | Width of gear spline |
| $\Delta p$ | -0.002 $(m)$ | $p_x$ sleeve meshes with gear |
| $n$ | $0, \pm1, \pm2, \pm3, \cdots$ | Integer numbers in *guard* |

and the values of $\mathbf{x}$ are reset according to $\mathbf{x}' = A_2\mathbf{x}$; when the sleeve meshes with the gear, the *guard* is denoted by $G_3$ as $G_3 \triangleq \{p_x \geq \Delta p\}$, the *location* switches from *free* to *meshed* and the values of $\mathbf{x}$ are reset according to $\mathbf{x}' = A_3\mathbf{x}$. For each impact, the impulse between the sleeve and the gear is $\Delta I$. Integrating the $\Delta I$, we get the accumulated impact impulse $I$. Thus, the sleeve has a state, $\mathbf{x} \triangleq (v_x, v_y, p_x, p_y, I)^T$, capturing the velocity $(v_x, v_y)$ and the position $(p_x, p_y)$ of the sleeve relative to the second gear under the coordinates as well as the accumulated impact impulse $I$ between the sleeve and the second gear. Involved model physical parameters and their values are described in Table 1.

## 2.1 Free Movement ODEs

As shown in Figure 4, the sleeve, namely the point, moves laterally towards the second gear with a shifting force ($F_s = 70$ newtons) during the meshing process. Then, the movement ODEs along the $x$ direction are:

$$\begin{cases} \dot{p}_x = v_x \\ \dot{v}_x = \dfrac{F_s}{m_s}. \end{cases} \tag{1}$$

Along the $y$ direction, there are some resisting moments ($T_f$) acting on the second gear, which is assumed to be a constant (1 newton-meter). Then, the movement ODEs along the $y$ direction are:

$$\begin{cases} \dot{p}_y = v_y \\ \dot{v}_y = -\dfrac{R_s \cdot T_f}{J_{g_2}}. \end{cases} \tag{2}$$

So, if the sleeve does not hit the second gear, *free movement ODEs* are:

$$\dot{\mathbf{x}} = A\mathbf{x} + Bu + f, \tag{3}$$

where:

$$u = \begin{bmatrix} F_s \end{bmatrix},$$

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} \frac{1}{m_s} & 0 & 0 & 0 & 0 \end{bmatrix}^T,$$

$$f = \begin{bmatrix} 0 & \frac{-R_s \cdot T_f}{J_{g_2}} & 0 & 0 & 0 \end{bmatrix}^T.$$

## 2.2 Impact Equations

As shown in Figure 4, when the point hits Line 1 (that is, the sleeve hits the gear as case 1 in Figure 2a), impact happens and the velocity of the sleeve after the impact is determined by an appropriate coefficient of restitution. Due to great stiffness of the sleeve and the gear, external force and torque, including $F_s$ and $T_f$, are ignored during impacting. We divide the impact process into compression phase and recovery phase. Dynamic equation in the compression phase is

$$\begin{cases} m_s \cdot v_{x_c} = m_s \cdot v_x + \Delta I_1 \cdot sin\theta \\ m_{g_2} \cdot v_{y_c} = m_{g_2} \cdot v_y + \Delta I_1 \cdot cos\theta \\ v_{x_c} \cdot sin\theta + v_{y_c} \cdot cos\theta = 0, \end{cases} \tag{4}$$

where $v_{x_c}$ represents the reset value of $v_x$ when compression has finished, $v_{y_c}$ represents the reset value of $v_y$ when compression has finished, and $\Delta I_1$ represents the compression impulse. Dynamic equation in the re-

covery phase is

$$\begin{cases} m_s \cdot v_{x_r} = m_s \cdot v_{x_c} + \Delta I_2 \cdot sin\theta \\ m_{g_2} \cdot v_{y_r} = m_{g_2} \cdot v_{y_c} + \Delta I_2 \cdot cos\theta, \end{cases} \tag{5}$$

where $v_{x_r}$ represents the reset value of $v_{x_c}$ when recovery has finished, $v_{y_r}$ represents the reset value of $v_{y_c}$ when recovery has finished, and $\Delta I_2$ represents the recovery impulse. According to the definition of the coefficient of restitution $\zeta$, we have

$$\begin{cases} \zeta = \dfrac{\Delta I_2}{\Delta I_1} \\ \Delta I = \Delta I_1 + \Delta I_2. \end{cases} \tag{6}$$

By solving the equations 4, 5, 6, we obtain

$$\begin{cases} v_{x_r} = \dfrac{(m_s \cdot cos^2\theta - m_{g_2} \cdot \zeta \cdot sin^2\theta) \cdot v_x}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} + \\ \qquad \dfrac{(-\zeta - 1) \cdot m_{g_2} \cdot sin\theta \cdot cos\theta \cdot v_y}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} \\ v_{y_r} = \dfrac{(-\zeta - 1) \cdot m_s \cdot sin\theta \cdot cos\theta \cdot v_x}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} + \\ \qquad \dfrac{(m_{g_2} \cdot sin^2\theta - m_s \cdot \zeta \cdot cos^2\theta) \cdot v_y}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} \\ \Delta I = \dfrac{(\zeta + 1) \cdot m_s \cdot m_{g_2} \cdot sin\theta \cdot v_x}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} + \\ \qquad \dfrac{(\zeta + 1) \cdot m_s \cdot m_{g_2} \cdot cos\theta \cdot v_y}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta}. \end{cases} \tag{7}$$

That is, *impact equations* are equivalent to $\mathbf{x}' = A_1\mathbf{x}$, where $A_1$ is the matrix:

$$\begin{bmatrix} \frac{m_s \cdot cos^2\theta - m_{g_2} \cdot \zeta \cdot sin^2\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{-(\zeta+1) \cdot m_{g_2} \cdot sin\theta \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 0 \\ \frac{-(\zeta+1) \cdot m_s \cdot sin\theta \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{m_{g_2} \cdot sin^2\theta - m_s \cdot \zeta \cdot cos^2\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \frac{(\zeta+1) \cdot m_s \cdot m_{g_2} \cdot sin\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{(\zeta+1) \cdot m_s \cdot m_{g_2} \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 1 \end{bmatrix}.$$

On the other hand, as shown in Figure 4, when the point hits Line 2 (that is, the sleeve hits the gear as case 2 in Figure 2b), impact happens. Similarly, *impact equations* are equivalent to $\mathbf{x}' = A_2\mathbf{x}$, where $A_2$ is the matrix:

$$\begin{bmatrix} \frac{m_s \cdot cos^2\theta - m_{g_2} \cdot \zeta \cdot sin^2\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{(\zeta+1) \cdot m_{g_2} \cdot sin\theta \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 0 \\ \frac{(\zeta+1) \cdot m_s \cdot sin\theta \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{m_{g_2} \cdot sin^2\theta - m_s \cdot \zeta \cdot cos^2\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \frac{(\zeta+1) \cdot m_s \cdot m_{g_2} \cdot sin\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & \frac{-(\zeta+1) \cdot m_s \cdot m_{g_2} \cdot cos\theta}{m_s \cdot cos^2\theta + m_{g_2} \cdot sin^2\theta} & 0 & 0 & 1 \end{bmatrix}.$$

When the sleeve meshes with the gear, impact happens to stop the lateral movement of the sleeve (that is, $v'_x = 0$) and remove the angular speed difference $\omega_r$ (that is, $v'_y = 0$). Hence, *impact equations* are $\mathbf{x}' = A_3\mathbf{x}$, where

$$A_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ m_s & m_s & 0 & 0 & 1 \end{bmatrix}.$$

## 2.3 Uncertain Initial States

Along the $y$ direction, both the initial velocity $v_{y_0}$ and the initial position $p_{y_0}$ of the sleeve are uncertain. On one hand, before meshing, the motor synchronizes the angular speed of the second gear with the sleeve (that is, $\omega_r \to 0$) by regulating the angular speed of the motor ($\omega_m$) to the value of $i_{g_2}\omega_s$ where $\omega_s$ is the angular speed of the sleeve. However, motor can hardly maintain its angular speed at a fixed value due to control and measurement accuracy. Then, $\omega_r$ may be non-zero within a range of $[-\Delta\omega, +\Delta\omega]$ where $\Delta\omega = 1$ rad/s. That is, the initial velocity of the sleeve along the $y$ direction ($v_{y_0}$) is within a range of $[-\Delta\omega R_s, +\Delta\omega R_s]$. On the other hand, the uncertain initial position of the sleeve along the $y$ direction ($p_{y_0}$) is within a range of $[-b, +b]$, as shown in Figure 2.

## 2.4 Executions, Reach Sets, and Safety

An *execution fragment* $\alpha$ of automaton $\mathcal{A}$ is a sequence of trajectories $\alpha = \xi_0, \xi_1 \ldots$, where $\xi_{i-1}.\mathsf{lstate} \to \xi_i.\mathsf{fstate}$. The first state of $\alpha$, $\alpha.\mathsf{fstate}$ is denoted by $\xi_0.\mathsf{fstate}$. If $\alpha$ is a finite sequence ending with a closed trajectory $\xi_n$, then its last state $\alpha.\mathsf{lstate}$ is defined as $\xi_n.\mathsf{lstate}$ and its duration $\alpha.\mathsf{dur} \triangleq \sum_{i=0}^{n} \tau.\mathsf{ltime}$. An execution fragment is an *execution* if it starts at an initial state, that is, $\alpha.\mathsf{fstate} \in \Theta$. The set of all executions is denoted by $\mathsf{Execs}_{\mathcal{A}}$. The set of executions and execution fragments up to time $T$ are denoted $\mathsf{Execs}^T_{\mathcal{A}}$ and $\mathsf{Frags}^T_{\mathcal{A}}$.

A state $\mathbf{v}$ is *reachable* if there exists an execution $\alpha$ with $\alpha.\mathsf{lstate} = \mathbf{v}$. $\mathsf{Reach}_{\mathcal{A}}(0, t_f)$ is defined as $\mathbf{v} \in \mathsf{Reach}_{\mathcal{A}}(0, t_f)$ if there exists an execution $\alpha \in \mathsf{Execs}_{\mathcal{A}}$ and a time $t \in [0, t_f]$ such that $\alpha(t) = \mathbf{v}$. We write $\mathsf{Reach}_{\mathcal{A}}(t, t)$ simply as $\mathsf{Reach}_{\mathcal{A}}(t)$ and $\mathsf{Reach}_{\mathcal{A}}(0, T)$ as $\mathsf{Reach}^T_{\mathcal{A}}$.

Given a time $t_b$ and a set of *safe* states $\mathcal{S}$, $\mathcal{A}$ is said to be *safe* if $\mathsf{Reach}_{\mathcal{A}}(t_b, t) \subset \mathcal{S}$ for all $t \geq t_b$. Otherwise, it is said to be *unsafe*.

## 2.5 Safety Property of Interest

For the HA model $\mathcal{A}$ in this paper (see Figure 3), meshing duration is required to be less than $t_b$, that is, the sleeve meshes with the gear within $t_b$; impact impulse during the meshing is required to be less than $I_b$.

Hence, $\mathcal{S} \triangleq \{\mathbf{x} | p_x \geq \Delta p \wedge I \leq I_b\}$. For this special system, it can be seen from Section 2 that if $p_x \geq \Delta p$ at time $t_1$, then the *location* switches from *free* to *meshed*, and the values of $\mathbf{x}$ remain unchanged for $\dot{\mathbf{x}} = 0$ at *location=meshed*. So, this HA model is *safe* if *location=meshed*, $p_x \geq \Delta p$ and $I \leq I_b$ at time $t_b$. In this specific system, we set the $t_b$ to 0.20 second and $I_b$ to 20 newton-meters.

## 3. KEY OBSERVATIONS

Whether a tool or an approach to safety verification can be used for a certain problem often depends on the kinds of dynamics. The benchmark example that was presented in Section 2 exhibits some characteristics that may make the safety hard to analyze.

### 3.1 Nondeterminism

From some initial position $p_{y_0}$ and velocity $v_{y_0}$, the sleeve may reach the intersection of two adjacent guards (the vertex of the gear). In this situation, the reset value of the state may be defined by one of the guards, which is a non-deterministic choice, and the simulation can show just one possible trajectory. For the whole meshing process, even the stochastic simulation can not cover the complete behavior of the sleeve. Thus, the nondeterminism makes the Motor-Transmission Drive System be an appropriate benchmark example for safety verification. However, for some approaches—such as the one in [16]—with limits to the transitions at sampling time, it may be ineffective to verify the safety of the benchmark example with a non-deterministic HA model $\mathcal{A}$.

### 3.2 Uncertain Number of Guards

From Figure 2 and Figure 4, we can see that the sleeve may fail to mesh with a gear tooth due to impacts when it moves forward to the gear. In this situation, the sleeve would move backward. After some time, however, the sleeve with the shifting force $F_s$ would move forward again to try to mesh with the same gear tooth or the others, which may be an adjacent gear or even a further one (as shown in Figure 5). Thus, there is a symbol $n$ in the guard expressions, which represent all of the integer numbers. However, we always choose a finite set—such as $\{-3, -2, -1, 0, 1, 2, 3\}$—to model the meshing process. Certainly, this simplification makes the safety verification more conservative. For improving the accuracy, other abstraction approaches are expected.

## 4. SIMULATION RESULTS

We defined and executed the HA model $\mathcal{A}$ in the Simulink and Stateflow. In this section, we show the trajectories of the sleeve with respect to two different initial states. We first take the initial state $\mathbf{x}(0) = (0, 0, -0.0165, 0.003, 0)$ as an example, and with a shifting force $F_s$ (70 newtons) the trajectory of the sleeve is shown in Figure 5. From it, we can find that the meshing duration is 0.1495 second, the impact impulse is 15.008 newton-meters, and the impact times is 4. And then, we only change the initial position $p_{y_0}$ to 0, and the trajectory of the sleeve is shown in Figure 6. For this initial state, the meshing duration is 0.0350 second, the impact impulse is 0.2368 newton-meter, and the impact times is 1.

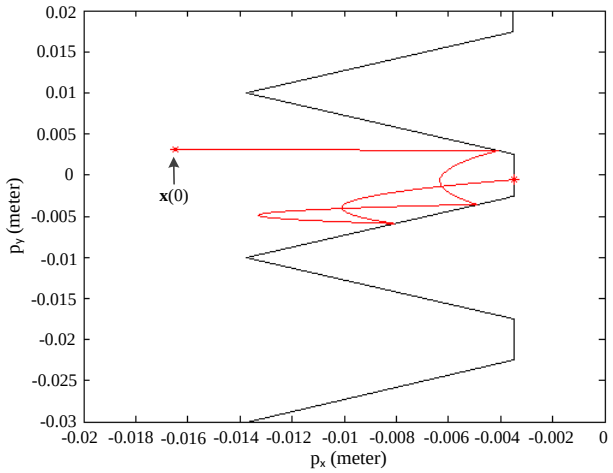



Figure 5: Trajectory of the sleeve with respect to $\mathbf{x}(0) = (0, 0, -0.0165, 0.003, 0)$.

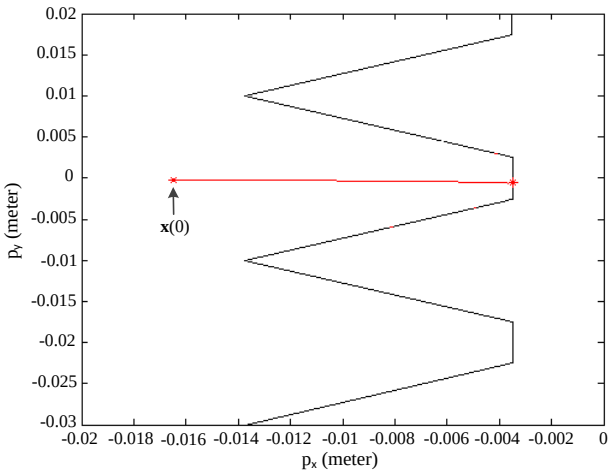



Figure 6: Trajectory of the sleeve with respect to $\mathbf{x}(0) = (0, 0, -0.0165, 0, 0)$.

Comparing the two trajectories, we can find the significant influence of the uncertain initial states on the safety property. For instance, if we reduce the meshing duration bound $t_b$ to 0.12 second, we may get the conclusion of that the Motor-Transmission Drive System is *unsafe* from some initial states.

## 5. CONCLUSIONS

This paper presented a benchmark example for safety verification of hybrid systems by elaborating on the HA model of the Motor-Transmission System and specifying its safety property of interest. Moreover, the characteristic phenomena exhibited by the benchmark example—nondeterminism and uncertain number of guards—were also present. All of the information was helpful for the researchers and engineers to apply advanced model-based safety analysis methods for this kind of hybrid system.

The benchmark example will be maintained on a website (`http://cps-vo.org/`), and we will also put the Simulink-Stateflow model on it. Furthermore, we will also improve the scalability of the benchmark example to satisfy the different requirements of verification problems for hybrid systems.

## Acknowledgments

Hongxu Chen and Guangyu Tian were supported by the Ministry of Science and Technology of China under a '973' Project (2011CB711202) and the China Scholarship Council under a scholarship (201206210199). Sayan Mitra was supported by the NSF CAREER Grant number CNS 10-54247.

## 6. REFERENCES

[1] Marco Caccamo. *HSCC '11: Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control*, New York, NY, USA, 2011. ACM. 100111.

[2] Dang Thao. *HSCC '12: Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control*, New York, NY, USA, 2012. ACM. 100121.

[3] S. Z. Bak, A. Greer, and S. Mitra. Hybrid cyberphysical system verification with simplex using discrete abstractions. In *Real-Time and Embedded Technology and Applications Symposium (RTAS), 2010 16th IEEE*, pages 143–152. IEEE, 2010.

[4] S. Z. BAK. *Verifiable COTS-based cyber-physical systems*. PhD thesis, Purdue University, 2013.

[5] A. Bemporad and M. Morari. Verification of hybrid systems via mathematical programming. In *Hybrid Systems: Computation and Control*, pages 31–45. Springer, 1999.

[6] A. Chutinan and B. H. Krogh. Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations. In *Hybrid Systems: Computation and Control*, pages 76–90. Springer, 1999.

[7] N. Elia and B. Brandin. Verification of an automotive active leveler. In *American Control Conference, 1999. Proceedings of the 1999*, volume 4, pages 2476–2480. IEEE, 1999.

[8] A. Fehnker. *Automotive control revisited linear inequalities as approximation of reachable sets*. Springer, 1998.

[9] A. Fehnker and B. H. Krogh. Hybrid system verification is not a sinecure. In *Automated Technology for Verification and Analysis*, pages 263–277. Springer, 2004.

[10] G. Frehse. PHAVer: algorithmic verification of hybrid systems past HyTech. In *HSCC*, pages 258–273, 2005.

[11] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. HyTech: A model checker for hybrid systems. In *Computer aided verification*, pages 460–463. Springer, 1997.

[12] D. K. Kaynar, N. Lynch, R. Segala, and F. Vaandrager. The theory of timed I/O automata. *Synthesis Lectures on Distributed Computing Theory*, 1(1):1–137, 2010.

[13] L. Lovas, D. Play, J. Marialigeti, and J. Rigal. Mechanical behaviour simulation for synchromesh mechanism improvements. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, 220(7):919–945, 2006.

[14] S. Ratschan and Z. She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. In *Hybrid Systems: Computation and Control*, pages 573–589. Springer, 2005.

[15] L. Sha. Using simplicity to control complexity. *IEEE Software*, 18(4):20–28, 2001.

[16] B. I. Silva and B. H. Krogh. Modeling and verification of hybrid systems with clocked and unclocked events. In *Decision and Control, 2001. Proceedings of the 40th IEEE Conference on*, volume 1, pages 762–767. IEEE, 2001.

[17] T. Stauner, O. Müller, and M. Fuchs. Using HyTech to verify an automotive control system. In *Hybrid and Real-Time Systems*, pages 139–153. Springer, 1997.