Identifying Hazard-causing Parameters for Automotive Driving Systems

Xiao-Yi Zhang, Paolo Arcaini, Fuyuki Ishikawa

Safety analysis of automotive systems is highly demanded, as failures in such systems can lead to dramatic consequences. Usually, these systems are affected by some variabilities, including the production parameters (e.g., the car power, or the braking force) and environmental parameters (e.g., dry or slippery road). These variabilities may drastically affect the system performance and hence the safety guarantees. In this paper, we propose an approach to explore the relation of the variabilities in automotive systems with the overall safety. Specifically, we take Spectra-Based Fault Localization (SBFL), a technique in the domain of software engineering as a baseline, and adapt it to the context of automotive driving systems based on the fuzzification of each system parameter. Through our approach, we can better understand which parameters can be the factors in causing system hazards. Our approach has been experimented on a Simulink model provided by our industrial partner. Critical factors that related to the hazard were identified and explained. This paper is a summary of the work published in the proceeding of ICECCS ' 19.

1 Introduction

Cyber-physical systems (CPS), integrating both computational modules and physical phenomena, have been extensively developed recently. In our project [2], driven by our industrial collaboration with an automotive company, we consider automotive systems (having different levels of automation). Errors in Cyber-Physical Systems (CPS), especially in automotive driving systems, may lead to disruptive economic and social damages. Therefore, once some failures (e.g., collisions) are detected during the simulation of an automotive driving model. Then, making a hazard analysis to trace the most unsafe component is essential. However, due to the complexity of the structure of automotive systems, tracing the hazard-causing components is more challenging. Specifically, the following issues should be addressed:

1. how to characterize the system components whose output could be continuous values;
2. how to quantify the system hazard;
3. how to calculate the proneness of each system component in causing a hazard.

In this paper, we adapt Spectra Based Fault Localization (SBFL) [4], a typical technique in the domain of software debugging to the context of automotive systems. SBFL aims to find the components suspicious to cause program failures based on the execution information of a given test suite. Taking the advantages of SBFL, we propose an approach to analyze the hazard of automotive systems involving different variabilities.

Currently, simulation-based validation (as falsification) checks a *single* automotive product operated in some given environmental conditions under some given driving inputs. Our work is inspired by a real-life case study provided by our industrial

Xiao-Yi Zhang, Paolo Arcaini, Fuyuki Ishikawa, 国立情報学研究所アーキテクチャ科学研究系, Information Systems Architecture Science Research Division, National Institute of Informatics.

partner. It is a Simulink model of a vehicle collision avoidance system, which is also adopted as the benchmark in our case study. Our approach assumes the targeted system can be modeled by Simulink. Also, we take the model *parameters*, which reflect the system variabilities (e.g., the car power and the braking force), as the system components to investigate.

Specifically, given the Simulink model of the subject system, on the one hand, we repeatedly simulate the system and, for each simulation instance, we record the simulation data, including the values of the investigated parameters and the *hazard degree*, indicating the degree of violating the safety requirement under consideration. On the other hand, we discretize the domain of each system parameter through fuzzification and describe each partition as a fuzzy set associated with a *concept* (e.g. "large" and "very small", etc.). Finally, based on the simulation results and the characterization of the system variabilities (i.e., parameters), we use a "metric" of spectrum analysis of SBFL to assign a *hazard impact degree* to each fuzzy set, indicating the proneness of that fuzzy set of being a hazard factor. From our analysis, we can infer which system parameters are the factors in causing hazard and why these parameters can cause the hazard.

This paper is a summary of our previous hazard assessment framework published in ICECCS'19 [5]. Our approach is experimented on an industrial artifact for automotive driving, and explainable results about system hazards are obtained.

2 Problem Description

System model. Let $\mathcal{M}$ be the model of the hybrid automotive system under analysis. We assume that the components of $\mathcal{M}$ can be described as a set of *parameters* $P = \{p_1, \ldots, p_n\}$, in which each parameter p_i has its own definition domain D_i. $\mathcal{M}$ is configurable. That is to say, we can assign each parameter p with a value v. If a concrete value v is given to each parameter p, an executable *simulation instance*, denoted by $\mathcal{M}(v_1, \ldots, v_n)$ can be constructed. Then, we can run $\mathcal{M}(v_1, \ldots, v_n)$ and obtain, as output, a signal over time o. Here, we define a *simulation instance* t as the pair $t = \langle (v_1, \ldots, v_n), o \rangle$.

Problem Statement. Given system model $\mathcal{M}$ and the set of simulation instances T in which each $t \in T$ has already been executed, assume $\mathcal{M}$ is subjected to hazard (i.e., some simulations $t \in T$ can cause system failures). Then, the fundamental problem is:

How to identify and analyze the parameters $p \in P$ that are the major causes of system hazard?

3 Approach

Fuzzification of parameters. To characterize system parameters, the concept *fuzzy set* borrowed from fuzzy logic is introduced. Considering a parameter p defined in the domain D, let $\mathcal{F}^p = \{f_1^p, f_2^p, \ldots, f_{m^p}^p\}$ denote the set of fuzzy sets that describe certain concepts of p. Each fuzzy set $f_i^p \in \mathcal{F}^p$ is defined by a *membership function*. Then, for each concrete value v of p, f_i^p can assign a membership degree within the range of $[0, 1]$, i.e., $f_i^p : D \to [0, 1]$, indicating the degree that v belongs to f_i^p.

Fuzzy-set-based coverage. Suppose we have simulation instance t with parameter values $(v_1, \ldots, v_n)$. Define the *coverage* of a specific parameter p with value v over simulation t as the vector $\mathcal{C}^{p,t} = [f_1^p(v), f_2^p(v), \ldots, f_{m^p}^p(v)]$, where for each fuzzy set f_i^p we have $f_i^p \in \mathcal{F}^p$. Furthermore, define the term *fuzzy-set-based coverage* of the entire model $\mathcal{M}$ over simulation t as $\mathcal{C}^t = \{\mathcal{C}^{p,t} | p \in P\}$. In this way, given a specific simulation instance t, we can quantify the degree each fuzzy set of each system parameter covered by t.

Hazard degree. Considering a specified safety

requirement φ of $\mathcal{M}$, the satisfaction of φ over a given simulation t can be quantified as $\gamma_\varphi(t)$ within the interval $[0, 1]$, indicating how strongly φ is satisfied. Note that the concept of φ is borrowed from the domain of system falsification [6]. Then, we calculate the *hazard degree* of t, denoted by $h(t)$, as $h(t) = 1 - \gamma_\varphi(t)$. Given a simulation instance t, by calculating the hazard degree $h(t)$, we can measure how close that the result of executing simulation instance t to the occurence of system failures (i.e., the degree that t exposes the hazard).

Hazard assessment. Finally, we try to assign a *hazard impact score* for each parameter p, indicating the relation of p to the hazard by means of the hazard degree. The basic heuristic of our work is similar to that of SBFL. Specifically, the ith fuzzy set f_i^p of parameter p is covered by more hazard-causing simulation instances; then, it is likely that f_i^p is more likely to be the factor of system hazard. To do this, we introduce *the scoring metrics* from SBFL and extend it to our context. Given the model $\mathcal{M}$ and the set of simulation instances T, for each simulation $t \in T$, we know $\mathcal{C}^t$ and $h(t)$. Then, given a specific fuzzy set f_i^p of parameter p, i.e., $f_i^p \in \mathcal{F}^p$, we use

$$a_h^{f_i^p} = \sum_{t \in T} (f_i^p(v) \cdot h(t)) \tag{1}$$

to measure the degree that f_i^p is covered by hazard-causing executions. Similarly, concerning system safety, use

$$a_s^{f_i^p} = \sum_{t \in T} f_i^p(v) \cdot (1 - h(t)) \tag{2}$$

to measure the degree that f_i^p is covered by non-hazard executions.

Note that $a_h^{f_i^p}$ and $a_s^{f_i^p}$ represent the degrees that fuzzy set f_i^p of parameter p *contributes to* the hazard and safety, respectively. Specifically, if t covers fuzzy set f_i^p at $f_i^p(v)$ degree, then we consider the term $f_i^p(v) \cdot h(t)$ as the contribution of f_i^p to the hazard at t. Oppositely, we consider the term $f_i^p(v) \cdot (1 - h(t))$ as the contribution of f_i^p to the safety at t. Then we sum $f_i^p(v) \cdot h(t)$ for each t to calculate $a_h^{f_i^p}$; and, similarly, we sum $f_i^p(v) \cdot (1 - h(t))$ for each t to calculate $a_s^{f_i^p}$. Finally, we use a metric, involving both $a_s^{f_i^p}$ and $a_h^{f_i^p}$ (i.e., the Tarantula metric for SBFL [3]), to calculate the final *hazard impact score* of the fuzzy set f_i^p, denoted by $\Phi(f_i^p)$:

$$\Phi(f^p) = a_h^{f^p} / (a_h^{f^p} + a_s^{f^p}) \tag{3}$$

Output of our approach. After hazard assessment, we rank all the fuzzy sets of all the parameters according to their hazard impact scores $\Phi(f_i^p)$ in descending order and provide a rank list as the output of our approach. In *the rank list of fuzzy sets*, the fuzzy sets of parameters with higher ranks can have a strong relationship with the hazards, whereas those with lower ranks are less related to the hazard.

表 1 System parameters

Name	Unit	Domain
T_safe	second	$[0, 5]$
Radius_tire	meter	$[0.3, 0.37]$
Power_max	kW	$[70, 130]$
Torque_max	Nm	$[150, 450]$
Weight	kg	$[800, 1500]$

(a) Production

Name	Unit	Domain
T_init	second	$[1, 5]$
A_back	G	$[0.1, 1]$
T_behav	second	$[0.5, 5]$
V_init	km/h	$[20, 160]$
R_gear	-	$[2.5, 10]$
Ay_init	-	$[0, 0.5]$
Myu_road	-	$[0.2, 1]$

(b) Enviromental

4 Case Study

Model description. To examine the effectiveness of our approach, we introduce the experimental results in [5]. The benchmark is a Simulink model of a *collision avoidance system* of an automotive vehicle provided by our industrial partner. In the basic situation, the vehicle drives on a straight lane and spots an obstacle in front. When the driver pushes the brake pedal, an active safety

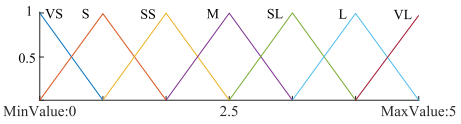

図 1 The membership functions of the fuzzy sets of parameter t_safe

feature is triggered to decide whether and when to shut down the engine if it is necessary to avoid an accident. The system has both production parameters related to the type of the car and environmental parameters related to the road condition and initial behavior of the car. All the model parameters and their types are listed in Table 1.

The initial distance between the car and the obstacle is the product of the initial inter-vehicle time `T_init` and initial vehicle speed `V_init`. Note that, the inter-vehicle can also be a static obstacle. Upon spotting the obstacle, the driver will push the brake pedal after `T_behav`, and the active safety feature will shut down the engine after `T_safe`. The evasive backward acceleration is `A_back`, and the ratio between engine RPM and wheel RPM is `R_gear`. The vehicle has tires with a radius equal to `Radius_tire`, an engine with the maximum horsepower and torque equal to `Power_max` and `Torque_max`, respectively, and weights `Weight`. `Myu_road` describes the friction of the road, and `Ay_init` is the initial lateral force.

Fuzzification of the systems parameters. For this benchmark model, since we do not have extra domain knowledge, for each parameter p having domain $D{=}[d_l, d_u]$ (see Table 1), we defined seven triangular fuzzy sets f^p_{VS}, f^p_S, f^p_{SS}, f^p_M, f^p_{SL}, f^p_L and f^p_{VL}, indicating the concepts of "Very Small", "Small", "Slight Small", "Medium", "Slight Large", "Large", and "Very Large". A triangular fuzzy set f^p_i is defined by a lower bound $\underline{S_i}$, an upper bound $\overline{S_i}$, and a kernel center K_i with $\underline{S_i} < K_i < \overline{S_i}$ and $f^p_i(\underline{S_i}) = f^p_i(\overline{S_i}) = 0$ and $f(K_i) = 1$. Then, the seven fuzzy sets determine a *regular fuzzy partition* [1], i.e., they have equidistributed kernel centers $K_1 \ldots K_7$, with $K_i = \overline{S_{i-1}} = \underline{S_{i+1}}$ for $i \in \{2, \ldots, 6\}$, $K_1{=}d_l$, and $K_7{=}d_u$. For example, for parameter `T_safe` having domain $[0, 5]$, $f^{\texttt{T\_safe}}_S(1) = 0.8$ and $f^{\texttt{T\_safe}}_{SS}(1) = 0.2$.

Definition of hazard degree. The basic safety requirement φ of this model is described as follows: "*The car should stop before* d^{Th} *meters from the obstacle and, if not possible, it should stop as soon as possible before the obstacle.*" The robustness satisfaction γ_φ gives a quantitative characterization of the satisfaction/violation of φ. The robustness value of a simulation t is defined as follows:

$$\gamma_\varphi(t) = \begin{cases} 0 & \text{mindis}(o_t) = 0 \\ \frac{d^{Th}/3 + \text{mindis}(o_t)}{4d^{Th}/3} & 0 < \text{mindis}(o_t) < d^{Th} \\ 1 & \text{mindis}(o_t) \geq d^{Th} \end{cases} \tag{4}$$

where mindis computes the minimum distance in the output signal. In (4), d^{Th} is the threshold of the safe distance. If the minimum distance is larger than or equal to d^{Th}, then t is considered as completely safety; in the experiments, d^{Th} has been set to 30. If mindis(o_t) reaches 0, it indicates that the collision occurred during simulation and the robustness value will be 0. Finally, if $0 < \text{mindis}(o_t) < d^{Th}$, it means that the collision did not occur, but the vehicle was not completely safe during the simulation. In order to distinguish the cases of *complete collision* and *close to collision*, we set the minimal robustness γ_φ of *close to collision* to 0.25. Then, we calculate the hazard degree of t by $h(t) = 1 - \gamma_\varphi(t)$ as discussed above. Note that γ_φ is normalized within $[0, 1]$.

Result and Analysis. For the case study, we run 10000 independent simulations and collected the results in T. Then, we calculated the hazard impact score for each fuzzy set of each parameter (see Eq. (3)). The results are shown in Table 2.

The result is the rank list of different fuzzy sets of

表 2 **Hazard Impact Score – Ranked list R of parameters fuzzy sets**

Rank	Parameter	Fuzzy set	Rank	Parameter	Fuzzy set
1	T_init	VS	16	T_behav	SL
2	A_back	VS	17	Power_max	SL
3	V_init	VS	18	R_gear	SL
4	T_safe	VL	19	T_safe	M
5	T_safe	L	20	R_gear	L
6	Weight	VS	...	...	...
7	V_init	S	76	V_init	SL
8	T_safe	SL	77	T_init	SS
9	T_behav	VL	78	V_init	VL
10	T_behav	L	79	V_init	L
11	T_init	S	80	T_safe	VS
12	Power_max	VL	81	T_init	M
13	Power_max	L	82	T_init	SL
14	A_back	S	83	T_init	VL
15	Weight	S	84	T_init	L

different system parameters presented in Table 2. From these results, we can get an overall picture of the potential factors leading to the hazard of collision. For different parameters and fuzzy sets, hazard impact scores are also different. For example, fuzzy set $f_{VS}^{\texttt{T\_init}}$ (i.e., very small values of `T_init`) ranks the first, indicating that when the initial inter-vehicle distance is "very small", it is more likely that the hazard (i.e., the collision) occurs. In addition to this, from the rank list of fuzzy sets, we can observe that the collision may be potentially caused also by the low ability of backward acceleration (i.e., when `A_back` belongs to $f_{VS}^{\texttt{A\_back}}$), the very small initial velocity (i.e., `V_init` belongs to $f_{VS}^{\texttt{V\_init}}$), and the long time needed by the safety equipment to activate (i.e., `T_safe` belongs to $f_{VL}^{\texttt{T\_safe}}$ or $f_{L}^{\texttt{T\_safe}}$).

5 Conclusion

In this paper, we introduce an approach to identify hazard-causing system parameters for automotive driving systems. Our approach relies on a set of system simulations and attaches a *hazard impact score* to each system parameter. Then we can assess and explain the system hazard better based on the rank list according to these hazard impact scores. Our approach is based on a lighted-weighted technique, Spectrum-Based Fault Localization (SBFL), to deal with the complex structure of automotive systems. Meanwhile, we introduce fuzzy sets to characterize the various system parameters, which makes our results more understandable and explainable. On the other hand, our work generalizes the SBFL technique itself to the domain automotive systems, which improves its applicability.

Acknowledgment The authors are supported by ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), JST. Funding Reference number: 10.13039/501100009024 ERATO.

参 考 文 献

[1] Guillaume, S., Charnomordic, B., and Loisel, P.: Fuzzy partitions: A way to integrate expert knowledge into distance calculations, *Information Sciences*, Vol. 245(2013), pp. 76–95.

[2] Hasuo, I.: Metamathematics for Systems Design, *New Generation Computing*, Vol. 35, No. 3(2017), pp. 271–305.

[3] Jones, J. A., Harrold, M. J., and Stasko, J.: Visualization of test information to assist fault localization, *Proceedings of the 24th international conference on software engineering (ICSE'02)*, ACM, 2002, pp. 467–477.

[4] Xie, X., Chen, T. Y., Kuo, F.-C., and Xu, B.: A Theoretical Analysis of the Risk Evaluation Formulas for Spectrum-based Fault Localization, *ACM Trans. Softw. Eng. Methodol.*, Vol. 22, No. 4(2013), pp. 31:1–31:40.

[5] Zhang, X.-Y., Arcaini, P., and Ishikawa, F.: Assessing the Relation Between Hazards and Variability in Automotive Systems, *2019 24th International Conference on Engineering of Complex Computer Systems (ICECCS)*, IEEE, 2019, pp. 190–199.

[6] Zhang, Z., Ernst, G., Sedwards, S., Arcaini, P., and Hasuo, I.: Two-Layered Falsification of Hybrid Systems Guided by Monte Carlo Tree Search, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 37, No. 11(2018), pp. 2894–2905.