A SysML-Based Modeling and Verification Method for Vehicle Safety

Chang-Won Kim[a], Ho-Jeon Jung[a], Young-Min Kim[b], Jae Lee[a]

[a]Dept. of Systems Engineering, Ajou University, [b]SPID Co., Republic of Korea.

Abstract

Vehicle safety is becoming a critical issue in developing autonomous driving technology. For example, failure propagation due to sensor failures on road obstacles will have significant impact on safe operation. Previous studies in safety design used different modeling languages in creating, analyzing, and simulating failure models. In this study, we used the system modeling language (SysML), which is widely accepted language for systems modeling, consistently in modeling component failures and analyzing them to identify failure propagation paths. Among the identified failure paths, critical ones were used to derive safety measures. SysML simulation was also used to verify the safety measures.

1. Background

In autonomous vehicles on roads, a sensor failure and its propagation can result in an accident and thus proper safety designs are needed. In previous studies, different modeling languages were used in creating and analyzing failure models (Wei, Jiao, & Zhao, 2017, Sharvia & Papadopoulos, 2015). In (Ariss, Xu, & Wong, 2011), a method for generating failure models was provided, but it lacked how to utilize the models in safety analysis and verification. In (Wei et al., 2017), deriving failure paths from the model was suggested, but how to use failure paths to secure system safety was not mentioned. To circumvent these issues, we use the system modeling language (SysML) throughout the study of modeling failures, identifying failure paths, and verifying safety measures.

2. Method

Fig. 1 shows the sequence of the activities to be performed and the associated results.

(1) Failure models are constructed using SysML. The models include the structure and behavior of components and failures.

(2) Safety analysis is performed using the generated failure model. The failure paths of a vehicle system are identified from simulation of failure model. Failure paths are ordered sets of components failures leading to an accident of the vehicle.

(3) Safety requirements are derived using identified failure paths.

(4) Safety measures are added to the failure model. Simulation of the resultant model is performed to verify them.

3. Results

In Fig. 1 the rightmost column shows an example of the generated failure models. The SysML models were constructed first to express system structure and faults, and the behavior of the system under normal, component failures, and failure propagation conditions.

Next, failure paths were identified by performing Monte Carlo simulation (initially) 100 times on the failure model. Failure rate information for each component was assigned at the time of failure model creation. The resulting failure paths contain information such as components failure, system failure, and sequence of failure propagation. By analyzing these failure paths, we can derive the frequencies of system normal behavior, system failure, and components failure.

Table 1 summarizes the resultant frequencies obtained from simulation of the failure model with and without the safety measure applied. As a result, the probability of occurrence of system failure is reduced by 0.21, and the probability of occurrence of system failure due to the failure of the local controller is reduced by 0.14.

4. Conclusions

The novelty of the SysML-based study of failure model proposed is that the activities for system design, safety analysis, and verification can be performed seamlessly. There is no need for model conversion for safety verification. It also improves the reproducibility of failure models by providing general and systematic rules for model generation. Some failure paths that are difficult to be derived from the existing method of failure mode and effect analysis (FMEA) were able to be identified using our approach. Furthermore, the calculation of the probability of occurrence of the top event as needed in the conventional fault tree analysis (FTA) method was performed automatically during the simulation.

References

Wei, Q., Jiao, J., and Zhao, T. (2017). Flight control system failure modeling and verification based on SPIN. Engineering Failure Analysis

Sharvia, S. and Papadopoulos, Y. (2015). Integrating model checking with HiP-HOPS in model-based safety analysis. Reliability Engineering and System Safety, 135, 64-80.

Ariss, O. E., Xu, D., and Wong, W.E. (2011). Integrating safety analysis with functional modeling. IEEE Transactions on Systems, Man and Cybernetics: Systems, 41(4), 610 – 624.

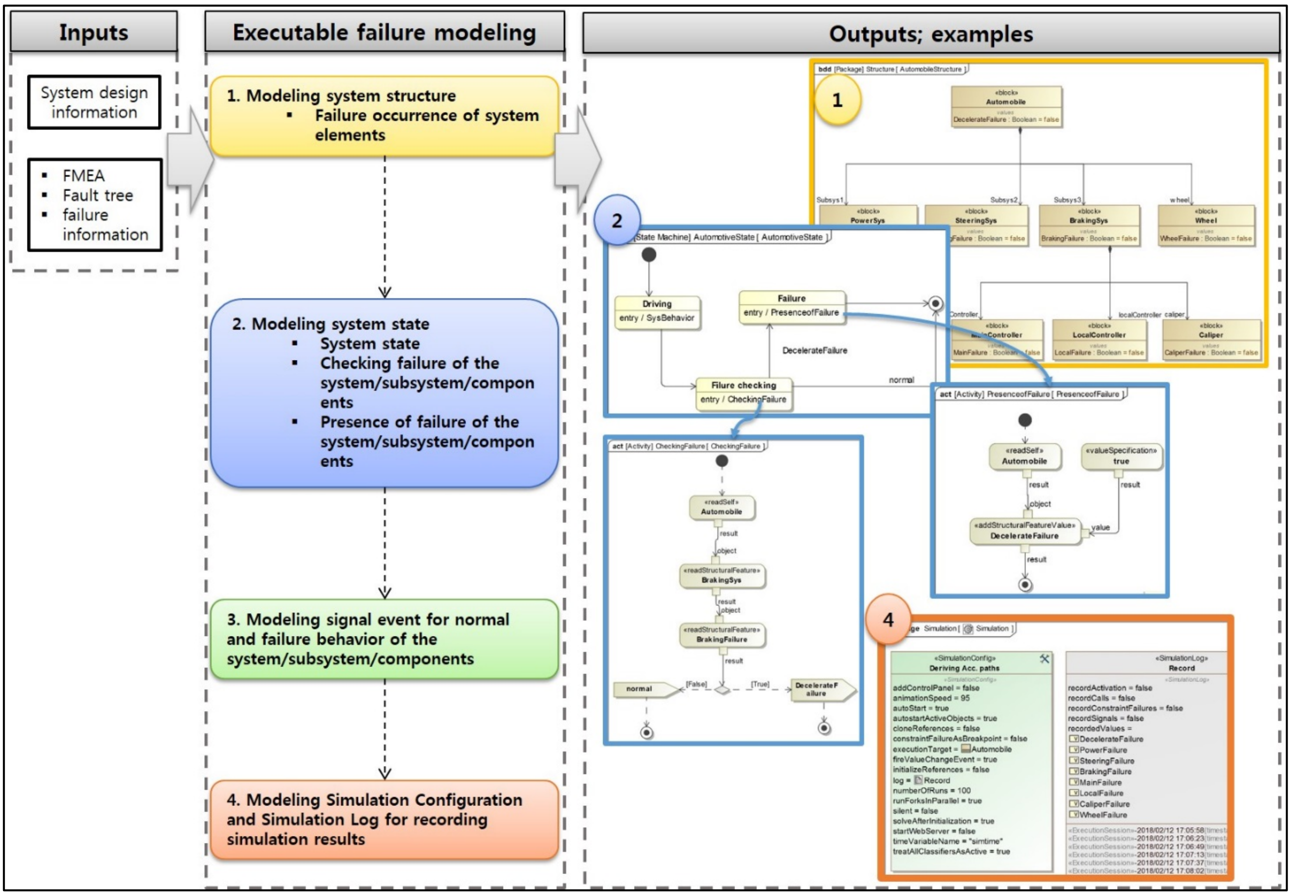
Inputs
System design information
FMEA
Fault tree
failure information
Executable failure modeling
1. Modeling system structure
Failure occurrence of system elements
2. Modeling system state
System state
Checking failure of the system/subsystem/components
Presence of failure of the system/subsystem/components
3. Modeling signal event for normal and failure behavior of the system/subsystem/components
4. Modeling Simulation Configuration and Simulation Log for recording simulation results
Outputs; examples
1
Automobile
PowerSys
SteeringSys
BrakingSys
Wheel
MainController
LocalController
Caliper
2
Driving
entry / SysBehavior
Failure
entry / PresenceofFailure
DecelerateFailure
normal
Filure checking
entry / CheckingFailure
Automobile
BrakingSys
BrakingFailure
normal
[False]
[True]
DecelerateFailure
4
Deriving Acc. paths
Record

Figure 1. A procedure for generating SysML-based failure model and outputs.

Table 1. Comparison of frequencies before and after applying safety measure to systems failure model.

Category of system behavior	Frequency/probability before applying safety measure	Frequency/probability after applying safety measure	Frequency Difference
System normal behavior	47	60	+13
System failure caused by components or subsystems failures	46	25	-21
Components or subsystems failures without system failure	7	15	
Occurrence of Local controller failure	16	9	
System failure caused by Local controller failure	16	2	-14
Probability of normal behavior of the system	0.47	0.60	+0.13
Probability of system failure	0.46	0.25	-0.21