Analyzing Safety in Collaborative Cyber-Physical Systems: A Platooning Case Study

Manzoor Hussain, Nazakat Ali, Youngjae Kim, and Jang-Eui Hong
Department of Computer Science
Chungbuk National University
Cheongju, Republic of Korea
Email: {hussain, nazakatali, kyj}@selab.cbnu.ac.kr, jehong@chungbuk.ac.kr

Abstract— **Collaborative Cyber-Physical Systems (CCPS) are those systems in which several Cyber-Physical Systems (CPSs) collaborate to achieve a common goal. However, safety verification for collaborative CPSs is a significant challenge. The challenges occur due to unexpected operating conditions which are, by definition, unknown at development time or due to the lack of composite hazard analysis for collaborative CPSs. In this paper, we present an approach to perform safety analysis for collaborative CPSs by introducing an enhanced Fault Traceability and Propagation Graph based on composite hazard analysis. This graph enables to determine the fault source, propagation scope and required safety guards to mitigate the faults. We use the platooning system as a case study and modify the original VEhicular NeTwork Open Simulator (VENTOS) to verify safety for the platooning driving system in a variable environment (an unexpected event). Our simulation results show that after applying our defined safety guards, all the member vehicles in platoon managed to avoid the collision.**

Keywords-Matrix; Cyber-Physical Systems; Hazard analysis; Platooning System; Safety Verification.

I. INTRODUCTION

Cyber-Physical System (CPS) is a controlled, reliable, and extensible complex and connected physical system, in which the physical module of the system is integrated with computational, communicational, and control capabilities that can interact with the human through sensors [1].

The safety of multiple CPSs collaborating with other CPSs becomes a challenging task for safety engineers due to their complicated, diverse, variable, and uncertain operational environments. Therefore, a technique that may provide enough safety for collaborative CPSs operating in variable and uncertain environments is required. Despite ISO 26262 and IEC 61508 safety processes and procedures, the safety of multiple CPSs collaborating to achieve a common goal is a challenge as elaborated in [2]. Due to the variable and diverse operational environment of collaborative CPSs, safety assurance becomes a difficult task [3]. The unexpected behavior in collaborative CPSs can come from unintended behavior of the failure-free system due to its performance limitation or lack of robustness regarding the environmental variability (such as fog and rain) that may disturb the sensors and actuators or due to insufficient situational awareness. Collaborative CPSs, for example, platooning mostly operate in a variable, and uncertain environmental conditions such as extreme weather conditions in foggy and heavy raining scenarios.

The focus of our paper is to investigate the collaborative nature of CPSs, analyze safety issues emerging during the collaboration of CPSs due to variabilities, trace the faults originating from the system collaborating in CPSs, and analyze the impact of a fault on other systems in CPSs in detail.

In this paper, we enhance our previous Fault Traceability graph [11] by introducing new Fault Propagation and Traceability Graph (FPTG), Fault Propagation Graph (FPG), and Fault Back Traceability Graph (FBTG) to investigate the fault route, propagation scope of fault, fault origin and impact of fault other systems. This study is built on our previous work [11] that proposed a composite hazard analysis technique for collaborative CPSs based on the content relationships among the hazard analysis artifacts. We modified the original VENTOS [4] simulator to create hazardous scenarios such as fog, rain, and snow to validate our approach. After analyzing the hazards for platooning systems (an example of CCPSs) with FPTG, FPG, and FBTG, we verify the safe behavior of the platooning system at run-time by using the VENTOS simulator.

The remaining part of the paper is organized as follows: Section II presents the literature review. In Section III, we present the proposed approach, and Section IV concludes this paper with some future research directions.

II. RELATED WORK

Designing a CCPS is a thorny challenging work due to its highly integrated physical, information, and communication modules. It demands higher reliability and robustness than a common system. The authors in [5] proposed a conceptual framework called A2CPS (autonomous CPSs) aiming to design and implement an autonomous supervision and control system. The purpose of this proposed framework was to reduce the probability of vehicle collision with resilient safety measures in a run-time fashion and control loop process.

Medawar et al. [6] discussed the role of the run-time manager in SafeCOP to ensure continuous safety in truck platooning. The authors first specify the safety contracts based on the safety analysis of the local system, as well as the cooperative safety function. The study further argues that safety contracts must be examined during the design phase to check their validity. Zhang et. al [7] proposed a taxonomy that can be translated under the uncertainty of the predictive model. A self-healing model is proposed to ensure the sustainable safety of the CPSs. A domain-specific language (CyPhyML+) was proposed by [8] to identify the interaction component and their uncertainties in collaborative CPSs. This language is an extension of CyPhyML [9]. In this approach, the semantic unit for heterogenous component interaction is identified within the collaborative CPS. The primary objective of this approach was to present the safety component and identifying unknown component interaction in CPSs ensuring safety.

The behavior of a robot in a human-robot collaborative environment should be adaptable as per human actions as mentioned in [10]. The authors investigated the capability of the proposed architecture to ensure human safety in the production environment. The safety in human-robot collaboration is ensured through a closed-loop control system that is based on human vicinity to robots.

III. PROPOSED APPROACH

The collaborative nature of CPSs and their operations in dynamic and uncertain environments raise safety issues. Sustainable safety at run time in adverse weather conditions is a real safety concern. The hazard analysis in CPSs makes it possible for safety engineers to identify potential failures and provides safety guards to mitigate the faults in the system. Therefore, we propose an approach to analyze safe operability for collaborative CPSs as shown in Figure 1. In the first step of our approach, we analyze the behavior of collaborative CPSs and try to consider variability factors in the behavioral analysis of CPSs at development time. In collaborative CPSs, failure in one CPS may affect other CPSs with whom it collaborates.

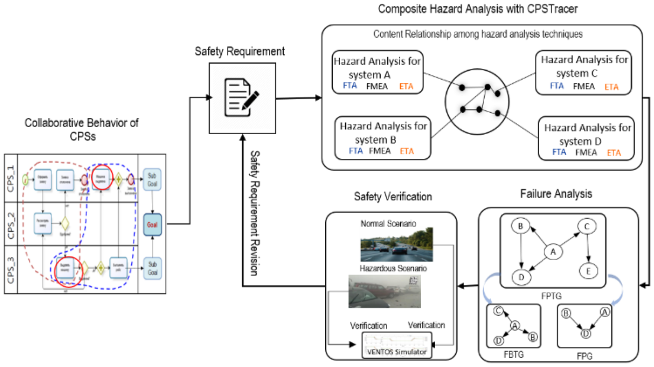


Figure 1. The proposed approach for analyzing safety in CCPS.

We introduced content-based relationships in our previous work [11] among the hazard analysis technique to envision the relationship among faults coming from different systems and the impact of a specific fault on other systems collaborating in CPSs. A single hazard analysis technique is not sufficient to ensure the safety of collaborative CPSs. Composite hazard analysis is necessary to prevent such failures by introducing safety guards in time. Therefore, to perform safety analysis of collaborative CPSs based on composite hazard analysis technique, we introduce conceptual Fault Traceability Graphs (FTG) in our previous work [11] to visualize the relationship between the faults and safety guards. However, this approach does not consider the variabilities such as environmental (fog, rain, and snow, etc.), temporal, infrastructural, and spatial variabilities. Also, the graph does not provide information about the source of the faults, and the information about the hazard analysis through which the fault is analyzed.

In this paper, we extend the FTG and developed FPTG. The FPTG aims to reflect the variabilities in CPSs and to visualize the impact of specific faults on other systems in CCPS, propagation scope, and origin of the faults. The FPTG shows the impact of a failure on other functionalities of collaborative systems and it shows the backward traceability of a fault as well, which is called FBTG. Another graph called FPG is also proposed to show all possible impacts of a specific fault on other systems. In the following subsections, we explain our proposed approach in detail.

A. *Collaborative Behaviors of CPSs*

To analyze the collaborative behavior of CPSs, we take the platooning CPS as a running example. In the platooning system, several vehicles form a platoon where the follower vehicle of the platoon maintains a short inter-vehicle distance with the preceding vehicle to improve traffic flow, reduce traffic congestion, and reduce fuel consumption [12]. The platooning system uses Cooperative Adaptive Cruise Control (CACC) where platooning vehicles communicate with each other to create synergy in their cooperation. The vehicles in the platooning system can also use an Adaptive Cruise Control (ACC) unit when necessary. In ACC mode, the platooning vehicles rely on onboard sensors instead of depending on other vehicles. As the distance among the vehicles is very short, therefore, the leader's failure can be propagated to other vehicles, as a result, a hazardous scenario may occur.

B. *Safety Requirements*

The safety requirements are those requirements that are defined to reduce the risk in any system. These requirements are also like other requirements, first specified at a high level, for example, it is needed to reduce a given risk. These requirements must be refined and then supplied to the designer. In our approach, we first analyzed the collaborative nature of CPSs, then, we extracted the safety requirements to reduce the identified faults and ensure an acceptable level of safety in collaborative CPSs. Each safety requirement is then supplied to composite hazard analysis as an input. Then, we analyze the collaborative CPSs with our composite hazard analysis tool to identify the potential faults based on the safety requirements. After performing the composite hazard analysis, we perform the failure analysis and verified whether the identified faults are removed from the system or not. This process is a loop process and this process is continued until an acceptable level of safety is achieved and the safety requirements are also revised according to fault status in the collaborative CPSs.

C. *Case Study: Composite Hazard Analysis of Platooning with CPSTracer*

In the platooning CPS, where the movement of vehicle group collaborates to reduce the inter-vehicle distance which benefits the better usage of road infrastructure by allowing more vehicles to use a given stretch of road, improve energy efficiency by reducing the aerodynamic drag [13]. On the other hand, reducing the inter-vehicle distance also leads to creating safety concerns in vehicles participating in the platooning. The safety of collaborative CPSs can be ensured by analyzing the safety of the system considering the potential uncertainties. The main objective of hazard analysis is to identify the potential hazards, analyze the faults, and measurement of possible damage. As mentioned, a composite hazard analysis technique can trace fault propagation in collaborative CPSs. In our previous work [11], we defined four relationships (i.e., *influence relationship, inheritance, overlap, and supplement relationship*) among Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA), and Event Tree Analysis (ETA). The definition of relationships are as follows

Influence Relationship: This relationship exists among the faults of the participating system in collaborative CPSs in which a fault of a system causes the failure of another participating system.

Inheritance Relationship: This relationship exists when two or more system participating in collaborative CPSs shares the same operational and functional constraints. This relationship also exists among the faults of the participation system in CCPSs.

Overlap Relationship: This relationship exists among the faults and outcomes/consequences of failure in collaborative CPSs. There exist overlap relationships when the consequences of the failure of a system are the same as the consequences of the failure of another system.

Supplement Relationship: This relationship exists among the safety guards and failures of the system in collaborative CPSs. When a system has safety guards to cope with the failure of another system in collaborative CPSs, this relationship is then established. This means that the safety guard for the failure of a system can be supplied to another identical failure of the system in CPSs.

We developed a composite hazard analysis tool (i.e., CPSTracer) to analyze the potential hazards for collaborative CPSs. This tool helps to analyze the potential hazard with variability that a CCPS may face often. In our previous work [14], we extended FTA, FMEA, and ETA a.k.a. v_FTA,v_FMEA, and v_ETA to capture the variability in collaborative CPSs. Therefore we used our extended FTA, FMEA, and ETA to analyze the potential hazards due to variabilities (e.g., *environmental, infrastructural, temporal, and spatial variability*) for the platooning case study.

FTA is widely used for hazard and risk assessment in CPS. The FMEA is a structured method for system safety analysis to identify, evaluate, and score the potential failure for the system and its effects. ETA shows all possible outcomes stemming from a mishap event and takes into account additional events and factors i.e., whether or not installed safety barriers are working. ETA can be used to identify possible potential accident scenarios and sequences in a complex system. In the first step of the composite hazard analysis technique, an FTA is performed to identify the root cause of the failure of the platooning system. Let us consider that, one of the reasons for platooning failure is *Car Collision* (i.e., a top event in FTA). The top event in FTA is a failure of the system as a whole, which is in the case of the platooning, the participant vehicles were not collaborating, and as a result *Car Collision* has happened. An FTA consisting of five levels for the platooning is shown in Figure 2. The intermediate events and basic events are the root cause of the top event in FTA (i.e., *Car Collision*). Let us take the example of an intermediate event (i.e., *Collision event*) to analyze its root

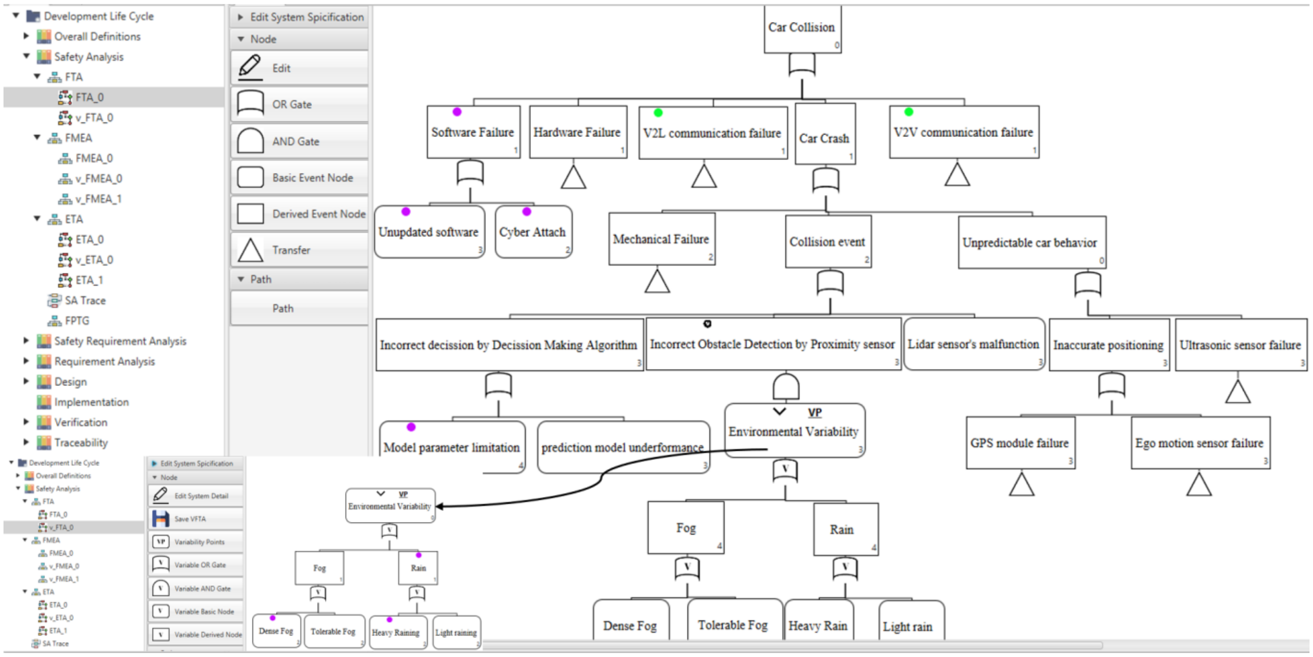
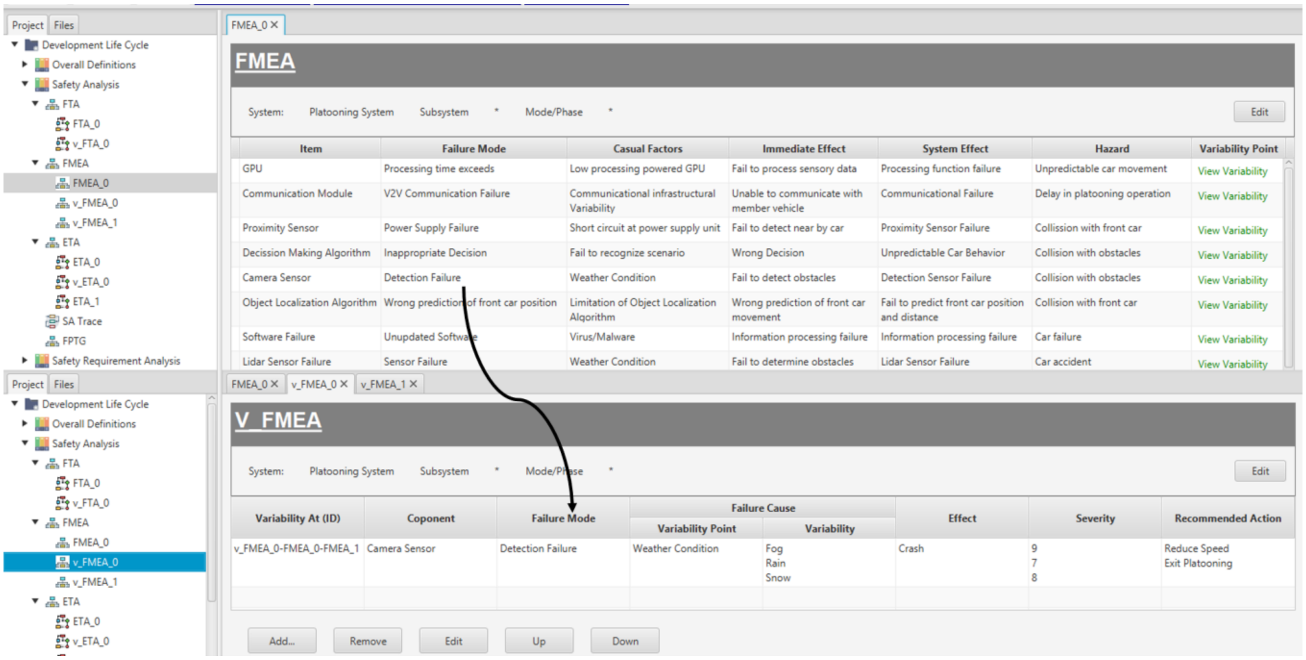


Figure 2. Hazard analysis of the platooning system with FTA and v_FTA.



FMEA

System: Platooning System Subsystem * Mode/Phase *

Item	Failure Mode	Casual Factors	Immediate Effect	System Effect	Hazard	Variability Point
GPU	Processing time exceeds	Low processing powered GPU	Fail to process sensory data	Processing function failure	Unpredictable car movement	View Variability
Communication Module	V2V Communication Failure	Communicational infrastructural Variability	Unable to communicate with member vehicle	Communicational Failure	Delay in platooning operation	View Variability
Proximity Sensor	Power Supply Failure	Short circuit at power supply unit	Fail to detect near by car	Proximity Sensor Failure	Collission with front car	View Variability
Decission Making Algorithm	Inappropriate Decision	Fail to recognize scenario	Wrong Decision	Unpredictable Car Behavior	Collision with obstacles	View Variability
Camera Sensor	Detection Failure	Weather Condition	Fail to detect obstacles	Detection Sensor Failure	Collision with obstacles	View Variability
Object Localization Algorithm	Wrong prediction of front car position	Limitation of Object Localization Algorithm	Wrong prediction of front car movement	Fail to predict front car position and distance	Collision with front car	View Variability
Software Failure	Unupdated Software	Virus/Malware	Information processing failure	Information processing failure	Car failure	View Variability
Lidar Sensor Failure	Sensor Failure	Weather Condition	Fail to determine obstacles	Lidar Sensor Failure	Car accident	View Variability

V_FMEA

System: Platooning System Subsystem * Mode/Phase *

Variability At (ID)	Coponent	Failure Mode	Failure Cause		Effect	Severity	Recommended Action
			Variability Point	Variability			
v_FMEA_0-FMEA_0-FMEA_1	Camera Sensor	Detection Failure	Weather Condition	Fog Rain Snow	Crash	9 7 8	Reduce Speed Exit Platooning

Figure 3. Hazard analysis of platooning system with FMEA and v_FMEA..

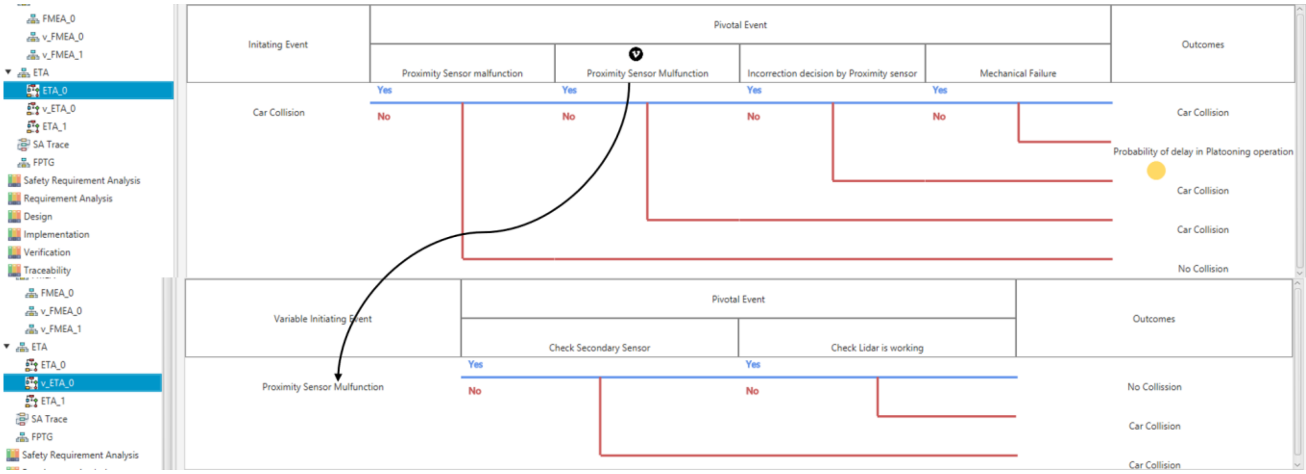


Figure 4. Hazar analysis of platooning with ETA and v_ETA.

cause in detail. We assume that the root cause of the *Collision vent* may be the *Lidar sensor's malfunction* or *incorrect decision by decision making algorithm* or may be due to *Incorrect Obstacle Detection by Proximity Sensor*. In general, FTA doesn't consider variability. The traditional FTA cannot capture the variability factors that lead to unexpected events at run time. We need to consider the variabilities while performing hazard analysis for collaborative CPSs. In our case study, we further investigated the intermediate event *Incorrect Obstacle Detection by Proximity Sensor* to find the more basic reason due to which *Incorrect Obstacle Detection by Proximity Sensor* event has happened with our extended FTA a.k.a v_FTA. Hence we come up with more basic events like *Dense Fog*, *Tolerable Fog*, *Heavy Rain*, and *Light Raining*.

In the second step of our composite hazard analysis technique, we analyzed the potential hazards for the platooning with FMEA and extended FMEA also known as v_FMEA. We also introduce a new column in FMEA. This column contains the safety guards for each fault. Let us take the example of the *Camera Sensor* failure, the causal factors of the *Camera Sensor Failure* may be due to *weather conditions*. To explore the more basic cause of *Camera Sensor Failure*, we investigate the more basic cause of *Camera Sensor Failure* with the v_FMEA. As we can see in Figure 3, after analyzing the *Camera Sensor Failure* with the v_FMEA, it is clear that the more reasonable causes of *Camera Sensor failure* are due to *Fog, Rain, and snow*.

In the last step, we analyze the platooning with ETA in our composite hazard analysis tool. We analyze the variability factor for *Proximity Sensor Malfunction* with v_ETA. We investigated the *Proximity Sensor Malfunction* for variability. Figure 4 shows the hazard analysis of platooning with ETA, as well as v_ETA.

D. Failure Analysis

Collaborative CPSs require more effective safety analysis to provides better fault traceability, fault propagation, fault sources, impact analysis of the fault, and potential safety guards for faults. The identification of fault propagation is a challenging task especially in collaborative CPSs for safety engineers. The proposed FPTG can be used as a means of failure analysis in collaborative CPSs because it can visualize the potential faults that may lead to the failure of collaborative CPSs. We developed an algorithm that detects the content relationship among the hazard analysis artifacts and generates the FPTG.

The FTPG is a directed graph in which the vertices represent the faults and safety guards, and the edges denote the relationships among the faults also relationships among faults and safety guards. Each node on the FPTG has complete information about the fault, its origin, and the hazard analysis technique used to analyze the faults. The colored edges on FPTG show the four content relationships as mentioned earlier. The arrow direction on FPTG determines the propagation of faults in collaborative CPSs.

As CCPS consists of highly interconnected systems, a fault in a participant system may lead to activating many other faults in other systems. The information on the nodes of FPTG can also help the safety engineers to determine where exactly a safety guard should be provided to eliminate the fault and stop its propagation to another system. The fault traceability determines the fault routes in collaborative CPSs. It is necessary to demonstrate that a safety-critical system must fulfill the safety goal, and all identified potential hazards were eliminated. The FPTG can identify the safety guards to mitigate potential faults. Both FPG and FBTG are also directed graphs. In our developed tool, after generating the FPTG we can select any fault on FPTG to know about its propagation scope and its route by clicking on a particular fault. A separate subgraph also known as FPG is generated for that specific fault which tells us the propagation route of that specific fault. It also clearly depicts how much a certain fault on FPGT is critical for the collaborative system's safety. The FBTG shows the traceability of a specific fault. By clicking on any fault on FPG, we can generate FBTG which shows the back traceability of that specific fault.

The relationships on FPTG, FPG, and FBTG are illustrated by color legends, as shown in Figure 5, Figure 6, and Figure 7. The *inheritance relationship* is represented with a green-colored edge, *influence relationship* with a purple edge, *overlap relationship* with a yellow edge, and *supplement relationship* with a red-colored edge. All variability nodes like environmental variability in the platooning system are represented by a black-bordered white colored circle to reflect the variability on FPTG, FPG, and FBTG. The node *Dense Fog.[Platooning System.v_FTA_0]* is an example of variability in Figure 5. In our case study, the node *Wrong Decision.[Platooning System.FMEA_0]*, influences the node *Collision event.[Platooning System.FTA_0]* and *Unpredictable car behavior.[Platooning System.FTA_0]*. Same as the node *V2V communication failure.[Platooning System.FTA_0] and V2L communication failure.[Platooning System.FTA_0]* inherits *Communicational Failure.[Platooning System.FMEA_0]*. As discussed earlier, the Overlap relationship exists when the failures of the

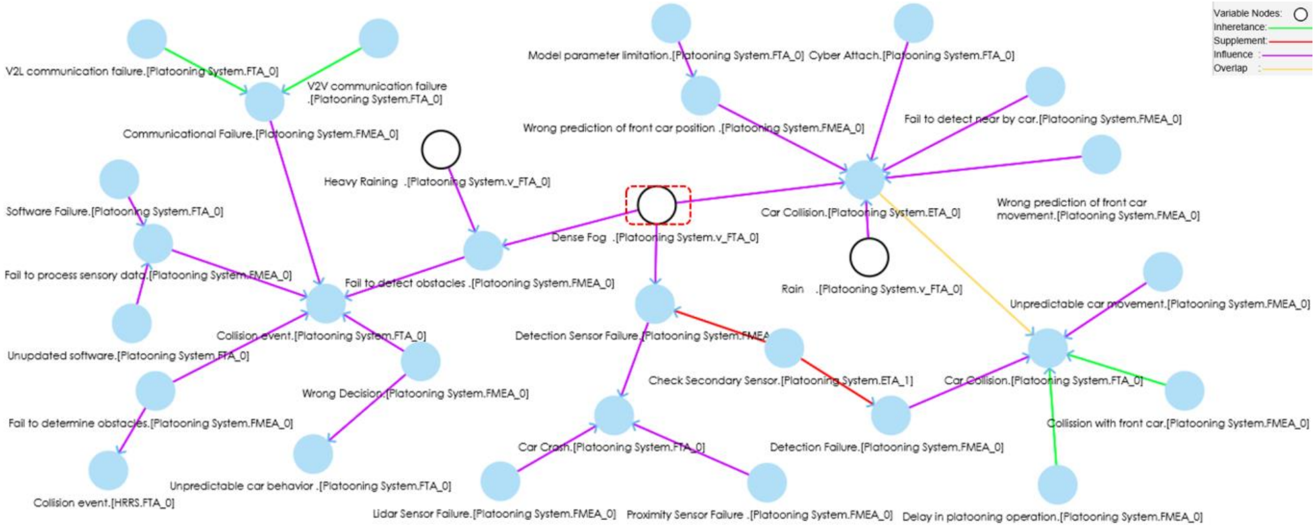


Figure 5. Fault Propagation and Traceability Graph for platooning.

systems in CPSs are the same. The node *Car Collision.[Platooning System.FTA_0]* overlaps the node *Car collision.[Platooning System.ETA_0]*. The Supplement Relationship provides safety guards. The node *Detection Failure.[Platooning System.FMEA_0]* is supplemented by *Check Secondary Sensor.[Platooning System.ETA_1]*. This means that the *Check Secondary Sensor.[Platooning System.ETA_1]* is supplied as safety guards to mitigate the effect of *Detection Failure.[Platooning System.FMEA_0]* and so on. Figure 5 shows the FPTG for platooning.

The information within the square brackets represents the source of faults and the hazard analysis technique used to analyze the system to perform hazard analysis. For example in the node *Collision event [Platooning system.FTA_0]* on FTPG, *Collision event* is the description of the fault, *Platooning system* within the square bracket represents the system being analyzed and the origin of the fault. *FTA_0* represents, the Fault Tree Analysis technique used to analyze the platooning system.

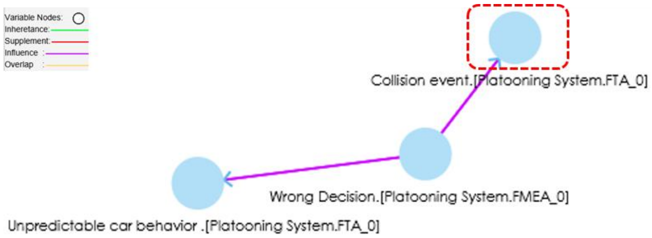


Figure 6. Fault Propagation Graph of platooning.

By clicking on a particular fault on FPTG, we can generate FPG. The algorithm generates the FPG which represents all possible impacts of a fault on other systems. This helps the safety engineers to make possible steps to mitigate the faults by apply suitable safety guards. From FPTG, we clicked the node *Wrong Decision.[Platooning System.FMEA_0*] to generate the FPG, as shown in Figure 6.

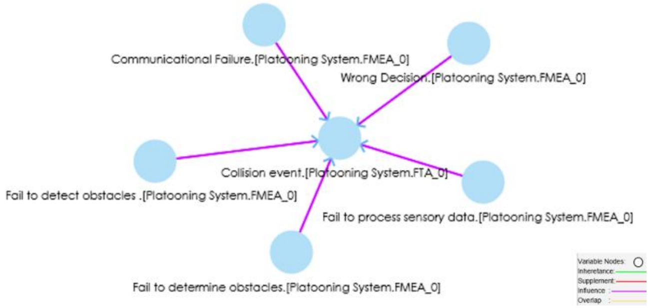


Figure 7. Fault Back Traceability Graph of platooning.

To know about the root cause of the occurrence of a specific fault, we just need to click on the nodes on FPG. From FPG we clicked on the node *Collision event.[Platooning System.FTA_0]* to generate the FBTG. Figure 7 shows the FBTG for the node *Collision event.[Platooning System.FTA_0].*

E. Safety Verification

In platooning, vehicles may face several environmental variabilities such as fog, rain, snow, and rushing objects on the road that might affect the vision of platooning vehicles, and collision may occur. The effect of environmental variability on the platooning vehicle's vision may lead to the collision of the whole platooning system. For example, if the platooning leader's vision sensor is affected due to dense fog or heavy rain then it may cause the collision of follower vehicles because the distance between platooning vehicles is supposed to be short.

After performing the hazard analysis for platooning with our developed tool we verify the behavior of platooning. The safety verification is necessary to confirm whether or not the identified faults in the system were removed. During the hazard analysis of platooning, we found that environmental variabilities such as fog, rain, and snow affects the vision (sensors) of cars in the platooning. We identified the potential faults that lead to the platooning collision during our composite hazard analysis. We first present a normal scenario, a hazardous scenario, safe scenario by applying a defined safety guard and then simulate these scenarios in VENTOS. In our simulation, we implement a platoon of size 5 (one leader denoted V0 and four followers denoted by V1..V4).

Normal Scenario: Five vehicles are running in a platoon on a highway with a speed of 25km/h (max speed in VENTOS simulator), inter-vehicles distance (minimum) 4m, and V2V (vehicle-to-vehicle) and L2V (leader to vehicles) communication modes. The leader communicates with the roadside unit and obtains road status information and receives no accident or traffic congestion information. The platoon continues to drive on its route under normal weather conditions. The speed and inter-vehicle for the normal scenario of the platooning system are shown in Figure 8.

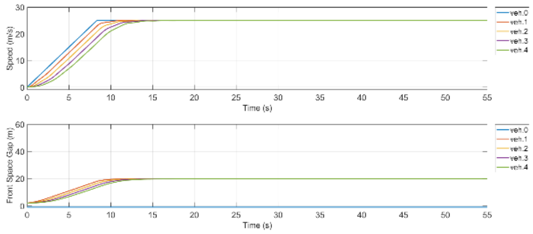


Figure 8. Speed and inter-vehicle distance for the normal scenario.

Hazardous Scenario: The vehicles in the platoon were on the way to their final destinations under normal weather conditions. We modify the original VENTOS simulator to create unexpected scenarios such as fog, rain, and snow. At some point, the platoon faces dense fog, and the platoon leader transmitted a reduction of speed command to its followers. The platoon reduced its speed accordingly. Suddenly, the platoon leader collided with a non-platooning vehicle due to its perception failure. The immediate follower of the leader also collided with the leader while the last three platooning vehicles managed to stop without collision. The vehicles changed their mode from CACC to ACC, changed their lane, and continue to drive. Figure 9 shows the simulation result of a hazardous scenario in terms of speed and inter-vehicle space.

As we see, at the time point 25, the leader vehicle faced dense fog and reduced speed gradually. At time point 27, a non-platooning vehicle suddenly came in front of the leader vehicle and a collision has happened due to the inaccurate decision of the proximity sensor. However, vehicles V2, V3, and V4 managed to stop without collision and changed their mode to ACC, changed their lane, and formed a new platoon to continue their journey.

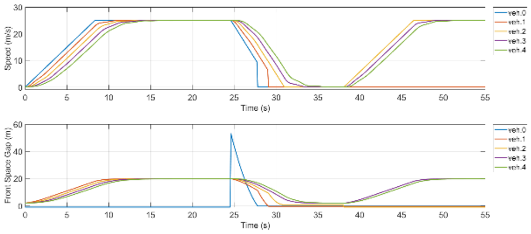


Figure 9. Speed and inter-vehicle distance for the hazardous scenario.

Safe Scenario: The vehicles in the platoon were on the way to their final destinations under normal weather conditions. At some point, the platoon faces dense fog, and the platoon leader transmitted a reduction of speed command to its followers. The followers reduced their speed as directed. The vehicles in the platoon were moving under fog by reducing their speed, a non-platooning vehicle suddenly changed its lane and came in front of the platoon.

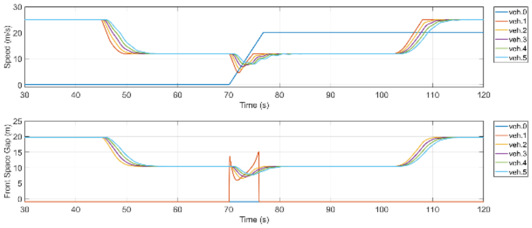


Figure 10. Speed and inter-vehicle distance for safe scenario

The leader vehicles detected it under dense fog and reduced its speed further to avoid the collision, by applying a safety guard, i.e., 'Urgent Brake". Figure 10 shows the implemented safe scenario in VENTOS.

IV. CONCLUSION

Collaborative CPSs are systems where multiple CPSs collaborate to achieve a common goal. However, safety remained a thorny challenge in collaborative CPSs due to the complex, diverse and variable operational environment of CCPS. The failure in one CPS of a collaborative CPSs may lead to the failure of other participant systems. Therefore, we proposed FPTG, FPG, and FBTG based on composite hazard analysis and content-based relationship to perform safety analysis. It enables to determine the fault route, the origin of faults, and its impact on other systems in a CCPS. We perform the safety analysis of platooning systems considering variability by using our developed tool and took the advantage of the VENTOS to verify the safe behavior of a platooning system. We are working on a learning-based approach to ensure safety verification in an on-the-fly situation by predicting the potential misbehavior in CPSs.

ACKNOWLEDGMENT

This work is supported by the Korea National Research Foundation of the Ministry of ICT and Science (NRF-2020R1A2C1007571).

REFERENCES

[1] N. Ali and J. E. Hong, "Failure detection and prevention for cyber-physical systems using ontology-based knowledge base," Computers, vol. 7, no. 4, Dec. 2018, p.68, doi: 10.3390/computers7040068.

[2] X. Lyu, Y. Ding, and S. H. Yang, "Safety and security risk assessment in cyber-physical systems," IET Cyber-Physical Systems: Theory and Applications. 2019, pp.221-232, doi: 10.1049/iet-cps.2018.5068.

[3] F. Platbrood and O. Gornemann, "Safe robotics-safety in collaborative robot systems," Sick AG, Waldkirch, Ger., vol. 980, 2017.

[4] M. Amoozadeh, H. Deng, C. N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Veh. Commun.*, 2015, pp.110-123, doi: 10.1016/j.vehcom.2015.03.004.

[5] J. K. Naufal et al., "A2CPS: A Vehicle-Centric Safety Conceptual Framework for Autonomous Transport Systems," IEEE Trans. Intell. Transp. Syst., 2018, pp.1925-1939, doi: 10.1109/TITS.2017.2745678.

[6] S. Medawar, D. Scholle, and I. Šljivo, "Cooperative safety-critical CPS platooning in SafeCOP," 2017, pp. 1-5, doi: 10.1109/MECO.2017.7977210.

[7] M. Zhang, B. Selic, S. Ali, T. Yue, O. Okariz, and R. Norgren, "Understanding uncertainty in cyber-physical systems: A conceptual model," 2016, pp. 247-264, doi: 10.1007/978-3-319-42061-5_16.

[8] H. Daneth, N. Ali, and J. E. Hong, "Automatic Identifying Interaction Components in Collaborative Cyber-Physical Systems," 2019, pp. 197-203, doi: 10.1109/APSEC48747.2019.00035.

[9] G. Simko, D. Lindecker, T. Levendovszky, S. Neema, and J. Sztipanovits, "Specification of cyber-physical components with formal semantics - Integration and composition," 2013, pp. 471-487, doi: 10.1007/978-3-642-41533-3_29.

[10] N. Nikolakis, V. Maratos, and S. Makris, "A cyber-physical system (CPS) approach for safe human-robot collaboration in a shared workplace," *Robot. Comput. Integr. Manuf.*, 2019, pp.233-243, doi: 10.1016/j.rcim.2018.10.003.

[11] H. Daneth, N. Ali, and J. E. Hong, "Towards enhancement of fault traceability among multiple hazard analyses in cyber-physical systems," Proc. IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), IEEE Press, July 2019, pp. 458-464, doi: 10.1109/COMPSAC.2019.10249.

[12] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surv. Tutorials*, 2016, pp.263-284, doi: 10.1109/COMST.2015.2410831.

[13] J. Axelsson, "Safety in vehicle platooning: A systematic literature review," *IEEE Trans. Intell. Transp. Syst.*, 2017, pp.1033-1045, doi: 10.1109/TITS.2016.2598873.

[14] N. Ali, M. Hussain, and J.-E. Hong, "Analyzing Safety of Collaborative Cyber-Physical Systems Considering Variability," *IEEE Access*, 2020, pp.162701-162713, doi: 10.1109/access.2020.3021460.