Safety modeling and evaluation of Automated Highway Systems

Ossama Hamouda, Mohamed Kaâniche, Karama Kanoun

Safety Modeling and Evaluation of Automated Highway Systems[1]

Ossama Hamouda, Mohamed Kaâniche, and Karama Kanoun
CNRS; LAAS; Université de Toulouse, 7, Avenue du Colonel Roche, F-31077, Toulouse, France
Université de Toulouse ; UPS, INSA, INP ; LAAS ; F-31077 Toulouse, France
{firstname.lastname}@laas.fr

Abstract

This paper addresses safety modeling and evaluation of Automated Highway Systems, based on the use of platoons of vehicles driven by automated agents. We analyze the impact on safety of the strategy used to coordinate the vehicles' operations, inside each platoon and between platoons, when vehicles enter or exit the highway, or when maneuvers are carried out to recover from failures affecting the vehicles or their communication. To cope with the complexity of the studied system, a compositional approach based on stochastic activity networks is developed. Replicated submodels associated with each vehicle, describing the corresponding failure modes and recovery maneuvers and their severity, are composed with submodels characterizing the configuration of the platoons and their dynamic evolution. Numerical results are presented to highlight the impact of the coordination strategy and other dependability related parameters.

1. Introduction

Traffic congestion is increasingly growing especially in urban areas. One of the solutions for this problem is automated traffic. Many research programs have been carried out or are currently underway to implement Automated Highway Systems (AHS), based on automatically controlled platoons of vehicles. The investigated techniques are aimed at providing guidance for vehicles to improve the traffic flow and the highway safety by reducing accidents, while reducing fuel consumption and pollution. In this context, several studies have been dedicated to collaborative driving systems, based on coordinated vehicles on highways equipped with the necessary infrastructure (see e. g., [1-9]). They were particularly devoted to the design of control architectures for automatic driving and their verification, and to performance evaluation in terms of capacity and traffic flow [1]. To the best of our knowledge the safety modeling and quantitative evaluation of such systems have been seldom addressed. This problem is challenging in the domain of automated highway systems implemented on ad-hoc networks.

In this paper, we address safety of AHS based on platooning applications implemented in a mobile context with ad-hoc networks. A *platoon* is a series of coordinated vehicles that are moving in the same direction on a highway [2]. The vehicles are driven by more or less automated agents, interacting in a multi-agent environment [17]. Switching to manual driving is possible under specific circumstances.

Our work aims at developing evaluation approaches and models that make it possible to analyze the AHS safety taking into account several phenomena, such as accidental fault occurrences, success and failures of the recovery maneuvers, and vehicles coordination strategies. The developed models are aimed at providing support to the designers for the analysis of possible solutions of AHS, based on safety evaluation.

We consider as a case study the architectures developed in the context of the PATH project (*Partners for Advanced Transit and Highways* [10]) for which experimental validation tests have been performed. These architectures implement automatic recovery maneuvers to ensure the platoons' safety in the presence of different types of failures affecting the vehicles and their environment. We have developed models, based in particular on Stochastic Activity Networks (SAN [11, 12]), to evaluate the impact of vehicle failures as well as maneuvers failure and success, on the Automated Highway Systems safety.

The paper is organized as follows. Section 2 presents the automated highway system considered,

[1] This work was partially supported by the HIDENETS project (*Highly DEpendable ip-based NETworks and Services*), EU-IST-26979, http://www.hidenets.aau.dk/.

together with its failure mode analysis. Section 3 presents the proposed safety modeling approach and its associated SAN model. Section 4 summarizes the results obtained and discusses their impact on the design of platooning applications. Finally, Section 5 concludes our findings and depicts future directions.

2. System description

Each platoon is composed of a *leader* that is the first car of the platoon and a set of *followers*. A platoon that contains one vehicle is called *free agent*. Figure 1 shows three platoons: *p1* with three vehicles, a leader and two followers, *p2* is a neighboring platoon, and *p3* is an example of free agent. The *intra-platoon* distance (Δx) ranges usually between one to three meters. The *inter-platoon* distance between two platoons (Δp) in the same lane varies between thirty and sixty meters.

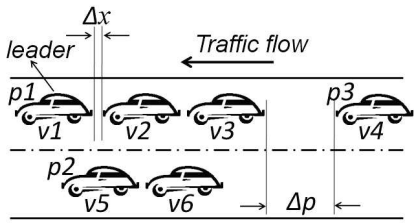

Figure 1: Context of a platooning application

The PATH research program has defined hierarchical control architectures for platooning applications. The platoons use lateral and longitudinal positioning controllers (magnetic equipments) to allow the vehicles to follow each other safely. The vehicles are coordinated by means of communications, based among other things on information from the magnetic equipments. Several maneuvers have been defined to allow the system to be in safe conditions in the absence and in the presence of failures (*fail-safe* mode).

The main maneuvers consist in splitting a platoon, merging platoons, or making a vehicle exit or enter the platoon. In case of a failure affecting a vehicle in the platoon, the maneuvers allow the vehicle to leave its platoon without any hazard, for the purpose of continuously running the platoon without any problem. Before starting a maneuver, the faulty vehicle communicates with its platoon's leader (that initializes the coordination of the maneuvers). According to the failure mode, some maneuvers may require a communication between the leaders of neighboring platoons in addition to communications with adjacent vehicles [13]. If the faulty vehicle is the leader, specific maneuvers must be applied to allow the platoon vehicles to select a new leader.

We briefly present background information on the PATH architecture that is needed to understand our safety models. We mainly focus on the failure modes considered and the recovery maneuvers used to ensure AHS safety, taking into account different strategies for intra-platoon and inter-platoon coordination.

2.1. Failure modes and recovery maneuvers

Several failure modes, with various severity levels, can affect the vehicles involved in platoons and their safety [2, 13, 14]. Depending on the failure severity, various maneuvers can be considered to ensure the safety. Some maneuvers may need to stop the faulty vehicle or help it to exit safely from the highway as soon as possible with the assistance of *adjacent vehicles*[2]. In the case where the failures have a minor effect on safety, the faulty vehicle could exit from the highway without the assistance of other vehicles.

In the following, we first present the failure modes that might affect a single vehicle, their severity and the associated maneuvers. Then, we discuss the case of failures affecting multiple vehicles. Finally, we present the catastrophic situations that could lead the automated highway system to an unsafe state. The failures of the controlling infrastructure are not considered in this paper.

2.1.1. Single vehicle failures: Six potential failure modes have been identified, presented in Table 1. This table shows for each failure mode, an example of cause leading to the failure mode, the severity class, and the maneuver that ensures the safe continuity of service despite the presence of failures.

Table 1: Failure modes and associated maneuvers

Failure mode	Example of cause	Severity class	Associated Maneuver
FM1	No brakes	A3	Aided Stop (AS)
FM2	Inability to detect vehicles in adjacent lanes	A2	Crash Stop (CS)
FM3	Inter-vehicle communication failure	A1	Gentle Stop (GS)
FM4	Transmission failure	B2	Take Immediate Exit-Escorted (TIE-E)
FM5	Reduced steering capability	B1	Take Immediate Exit (TIE)
FM6	Single failure in a redundant sensor set	C	Take Immediate Exit-Normal (TIE-N)

The severity classes associated with the failure modes are ranked by decreasing order. *Class A* is the highest, gathering the most critical failures that need to

[2] *Adjacent vehicles*: refer to the vehicles providing assistance to the faulty vehicle, for example to help it to get out of the highway.

stop the vehicle on the highway. Three maneuvers are defined for this purpose: *Gentle Stop (GS, where the fault vehicle uses its brakes smoothly to stop)*, *Crash Stop (CS, where the faulty vehicles uses maximum emergency braking)*, and *Aided Stop (AS, where the faulty vehicle is stopped by the vehicle immediately ahead)*. Specific control laws are then used to ease congestion, divert traffic away from the incident, assist emergency vehicles, and get the queued vehicles out.

The severity classes (*B* and *C*) include the failure modes that can be recovered by allowing the faulty vehicle to get out of the highway without stopping the traffic. The corresponding maneuvers can be achieved either without assistance or with the cooperation of some adjacent vehicles. Three maneuvers are defined too, namely: *Take Immediate Exit-Escorted (TIE-E)*, *Take Immediate Exit (TIE)*, *Take Immediate Exit-Normal (TIE-N)*.

It is noteworthy that the severity class also determines the priority of the corresponding maneuver. This is important when multiple failure modes occur. The priorities within each class are as follows: Within *Class A*, A3 has the highest priority and A2 has higher priority than A1. In *Class B*, B1 and B2 have equal priority. In case of occurrence of multiple failure modes in the same vehicle, the maneuver with the highest priority is applied.

Details about the atomic maneuvers composing each of the six maneuvers presented in Table 1 and the inter-vehicle coordination required to implement them, are presented in [15].

The successive failure of maneuvers may eventually lead to a state where no maneuvers are available to recover the faulty situation. This is illustrated by the state machine in Figure 2, where v_KO identifies such a state. The transitions correspond to the occurrence of failure modes, or to the results of maneuver executions that might succeed (transitions to the safe state, v_OK) or fail (KO transitions). Whether the state v_KO corresponds to an unsafe state for the AHS or not, depends on the state of the adjacent vehicles (this is discussed in section 2.1.3).

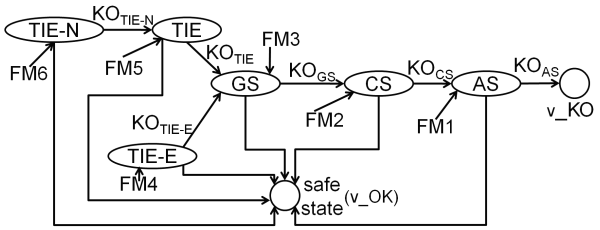

Figure 2: failure modes, maneuvers, safety impact

2.1.2. Multiple vehicles failures: When nearly simultaneous failures affect multiple vehicles, in particular adjacent vehicles, in the same platoon or in neighboring platoons, the maneuver with the highest priority is applied. The success of a maneuver depends on many factors, for example, the state of faulty vehicles in the platoon, the capability of the adjacent vehicles needed to assist the faulty vehicle to realize the maneuver (particularly the leaders concerned by the maneuver), and the traffic flow.

As an example, let us assume that a vehicle *v1* is faulty and has to perform the *TIE* maneuver. If another vehicle is already performing a maneuver with a higher priority, the maneuver requested by *v1* will be refused. Hence, *v1* will ask for another maneuver of a higher priority until the requested maneuver is accepted. Similarly, when a maneuver fails, the system evolves towards a more degraded failure mode and one of its associated maneuvers must be attempted to put the system in a safe state.

2.1.3. Impact of failures on the AHS safety: The scenarios described in Figure 2 concern a single vehicle. Catastrophic situations leading the system to an unsafe state require the occurrence of simultaneous failures affecting multiple adjacent vehicles in a small neighborhood in space and in time.

Based on the analysis presented in [15], we summarize in Table 2 three catastrophic situations that would lead the AHS to an unsafe state, taking into account the number of failures affecting different adjacent vehicles and their severity.

Table 2: Catastrophic situations

Situation	Description
ST_1	At least two *Class A* failures
ST_2	At least one *Class A* failure AND { (two *Class B* failures) OR (one *Class B* AND one *Class C* failures) OR (three *Class C* failures) }
ST_3	At least four failures whose severities correspond to *Class B* or *Class C*

2.2. Vehicles coordination

Platooning applications require coordination between the vehicles in the platoon (*intra-platoon*) and with neighboring platoons (*inter-platoon*). A vehicle is involved in the coordination process when i) it creates a platoon, ii) enters an existing platoon, or iii) when it leaves a platoon to switch to manual driving. Various communication models (centralized and decentralized) have been proposed in [17] for the *inter-* and *intra-platoon* coordination, based on the PATH architecture. They are briefly summarized hereafter.

2.2.1. Inter-platoon coordination: Communications between platoons can be achieved only through the leaders, and the coordination can be centralized or decentralized.

In the *centralized coordination model* the coordination between the leaders of neighboring platoons is performed through a centralized Service Access Point (SAP) that is on the road-side. The coordination between different maneuvers is achieved at the level of the SAP. Figure 3 presents an example considering an AHS composed of two lanes with two platoons, *p1* followed by *p2* on *lane2,* and two free-agents, *v7* and *v8*, on *lane1*. Let us assume that i) *v7* and *v8*, which just entered the highway, decide to join respectively platoons *p2* and *p1*, and ii) simultaneously and independently, vehicles *v2* and *v5*, belonging respectively to platoons *p1* and *p2*, are coordinating maneuvers to exit the AHS after passing through *lane1*. The SAP determines the priorities between the maneuvers involving the four concerned vehicles and communicates its decision to the leaders of the platoons including the concerned vehicles. The decision would be to assign the highest priority to the maneuvers requested by *v7* and *v8*, because it is important to release *lane1* as quickly as possible, so that *v2* and *v5* can leave the highway.

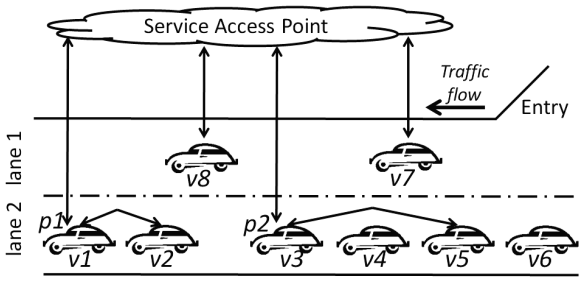

Figure 3: Centralized inter-platoon coordination

In the case of *decentralized inter-platoon coordination*, the decision is made by the leaders of the concerned platoons. The information related to the state of all vehicles is stored in an onboard system that contains a knowledge base of the neighborhood traffic. This coordination strategy has an impact on the implementation of some atomic maneuvers. Compared to the centralized strategy, it involves fewer vehicles in the accomplishment of some maneuver. Let us consider as an example the case of a faulty vehicle that needs to perform a *Take Immediate Exit-Escorted (TIE-E)* maneuver with the support of a neighboring platoon. If the inter-platoon coordination is centralized, the implementation of this maneuver involves: 1) all the vehicles in front of the faulty vehicle (including the leader) and the vehicle just behind it, and 2) the leader of the neighboring platoon. However, in the decentralized inter-platoon coordination strategy, only the leaders of the two platoons and the vehicles just in front and behind the faulty vehicle contribute to the maneuver. More details are provided in [2] [16].

2.2.2. Intra-platoon coordination:
In the *centralized intra-platoon coordination* model the coordination of operation and maneuvers involving the vehicles of a platoon is centered on one vehicle: the leader. For example, during a split maneuver that is initiated to allow the safe exit of a faulty vehicle, three vehicles are involved: the leader, the splitter, and the vehicle following the splitter (if it exists). The faulty vehicle should announce the need to initiate this maneuver to its platoon's leader. The leader then calculates the distance and the speed to be respected by the vehicles that are involved in the maneuver, and orders the involved vehicles to change them accordingly.

In the case where the *intra-platoon coordination is decentralized*, each platoon member has knowledge of the platoon formation and can react independently, by communicating directly with other vehicles. The leader is informed of changes as it is the representative of the platoon for inter-platoon coordination.

2.2.3. Coordination strategies: In our work we have considered the four strategies resulting from the combination of the above models, given in Table 3.

Table 3: Coordination strategies considered

Strategy	Inter-platoon model	Intra-platoon model
DD	Decentralized	Decentralized
DC	Decentralized	Centralized
CD	Centralized	Decentralized
CC	Centralized	Centralized

3. Safety modeling

We consider a two lane AHS with one platoon in each lane. Vehicles in each platoon can change from one platoon to the other one freely. Each platoon contains up to *n* vehicles. We model this system, taking into account the six failure modes and the associated maneuvers presented in Table 1, the catastrophic situations of Table 2 and the four coordination strategies of Table 3.

The measure evaluated corresponds to the probability that the modeled AHS is in one of the catastrophic situations described in Table 2, as a

function of time (t). This measure is referred to as system unsafety, and is denoted by $\overline{S}(t)$.

As discussed in Section 2, several factors need to be considered when analyzing the impact of failures on the safety of an AHS. In particular, the success or failure of a recovery maneuver depends on the state of the adjacent vehicles contributing to the maneuver. Thus, the models should also describe some characteristics of the configuration of the platoons as well as their dynamic evolution.

Modeling techniques based on Stochastic Activity Networks (SAN) are well suited to evaluate the system unsafety taking into account the considerations mentioned above. This formalism and the associated Möbius tool [12] provide compositional operators that are useful to master the complexity of the models, both at model construction and model processing phases. In particular, the system model can be built by the composition of atomic models using Join and Replicate operators.

In the following, we present an overview of the whole system model, and then we describe the submodels composing the whole model.

3.1. Overview of the system model

Figure 4 shows the overall structure of the model describing the AHS composed of two lanes. The model includes *2n* replicas of the One_vehicle sub model that are composed with three other submodels: Configuration, Dynamicity, and Severity.

The One_vehicle submodel describes the behavior of a vehicle as resulting from its failure modes and the maneuvers presented in Table 1. The Severity submodel describes the impact of multiple failures affecting several vehicles. The sub model Dynamicity is used to model the dynamics of the system in the absence of failures, resulting from *join* and *leave* events that correspond to vehicles entering or getting out of the highway. The Configuration submodel initializes the other submodels and synchronizes their evolution according to the whole system evolution.

In the following, we detail each submodel.

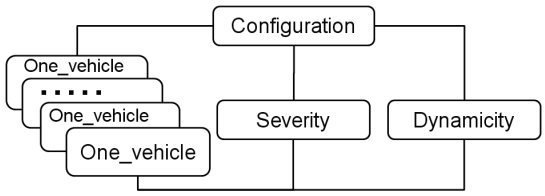

Figure 4: Model structure

3.2. Presentation of the sub models

3.2.1. One_vehicle: The SAN submodel shown in Figure 5 describing the vehicle behavior models the failure modes of the vehicle and associated maneuvers, presented in Table 1. The model consists of six interconnected elementary SANs. Each elementary SAN models the occurrence of a failure mode for a given class of severity and the associated maneuver. An elementary SAN consists of: i) two places (CC_i, SM_i), ii) two input gates (f_i, IG_i), iii) two output gates (OG_i, fm_i), and iv) two timed activities (L_i, *maneuver*). This model is replicated *2n* times (i.e., one model for each vehicle).

Places CC_i are local to each sub model. Each place CC_i will have one token when a vehicle enters the platoon (i.e., place IN is marked). Place int_id saves the ID of each vehicle in the system. Place start_id is used for the initialization of the submodel.

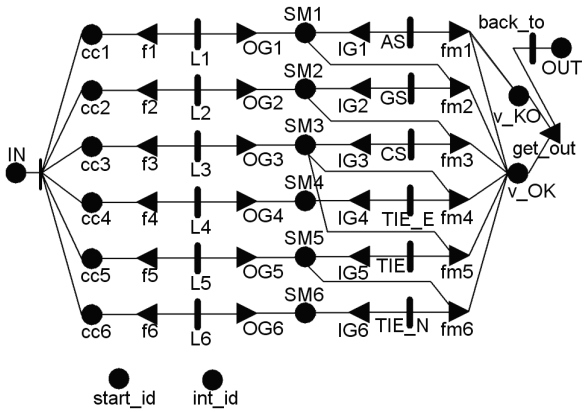

Figure 5: One_vehicle SAN model

Place CC_i identifies the initial state from which the failure mode described by timed activity L_i with firing rate λ_i could be fired. The occurrence of the failure mode activates the associated maneuver (place SM_i is marked). The selection of the appropriate maneuver (TIE-N, TIE, TIE-E, CS, GS, or AS) depends on its priority compared to other maneuvers that might be already active, and on the state of the adjacent vehicles contributing to the maneuver. The predicates and the functions associated with the input gates IG_i and the output gates fm_i manage the priority of maneuvers as defined in Table 1 and check the marking of places SM_i of the adjacent vehicles, according to the coordination strategy presented in Table 3. When a higher priority maneuver is activated, all lower priority maneuvers associated with the same vehicles are inhibited. The execution times of the maneuvers are described by exponentially distributed timed activities with firing rates ($\gamma_{TIE\text{-}N}$, γ_{TIE}, $\gamma_{TIE\text{-}E}$, γ_{CS}, γ_{GS}, and γ_{AS}).

If the maneuver succeeds, place v_OK is marked to indicate that the vehicle gets out of the highway safely.

The maneuver failure leads the vehicle to start the next higher priority maneuver, as explained in Section 2.1. Eventually, if the maneuver in highest priority AS fails, v_KO is marked, and the vehicle becomes a free agent (this is not represented in the model because it will constitute a third platoon). The two existing platoons continue their way without this vehicle.

When a vehicle gets out of the platoon by reaching one of the places v_OK or v_KO, another vehicle could join the system. This is modeled through the timed activity back_to and the marking of place OUT (see also Figure 7).

3.2.2. Severity: This submodel presented in Figure 6 describes the combination of failure modes affecting multiple vehicles that lead the system to an unsafe sate. Each time a failure mode L_i is fired in an One_vehicle submodel, the marking of the place indicating the corresponding severity class is incremented (class_A, class_B, class_C). These extended places are shared by all the submodels. Each of them is modeled as an array listing the ongoing maneuvers with the number of failure modes of the corresponding severity class that are active during the execution of the maneuver.

The predicates and functions associated with the input gate KO_allocation and the output gate OG_KO in Figure 6 describe the impact on the global safety of multiple failures affecting several vehicles, as presented in Table 2. When the instantaneous activity to_KO is fired, the place KO_total becomes marked indicating that the system has reached an unsafe state.

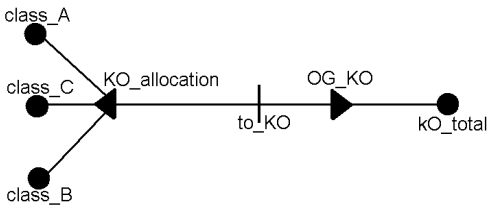

Figure 6: Severity SAN model

3.2.3. Dynamicity: The SAN submodel is given in Figure 7. There are four places (IN, platoon1, platoon2, and OUT). The two places platoon1 and platoon2 are shared between all submodels. They are extended places represented as an array of length *n*, each of them modeling one platoon. All these places have initially zero token.

When IN is marked, the instantaneous activity JP is fired indicating that a vehicle has joined a platoon. Two cases are associated with this activity corresponding to the selection of platoon1 or platoon2, each with probability 50%.

There are five timed activities (leave1, leave2, ch1, ch2, and Join). The three activities (leave1, leave2, and Join) implement the voluntary *join* and *leave* of vehicles (i.e., in absence of failures). The other two activities (ch1 and ch2) model the time spent by a vehicle for splitting from a platoon and joining the other one.

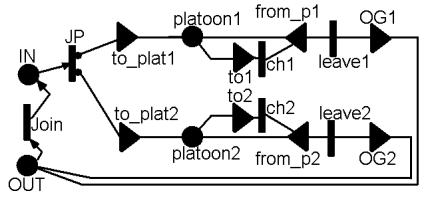

Figure 7: Dynamicity SAN model

When a vehicle leaves a platoon, the OUT place will be marked, thus another vehicle could join the highway. All other input and output gates are used for managing the vehicles positions after each *leave* and *join* event. In addition, each time a vehicle joins a platoon; it occupies the last position of the platoon.

3.2.4. Configuration: This submodel, presented in Figure 8, is used to define the initial configuration of the platoons and to initialize the One_vehicle submodels associated with each vehicle included in the platoons. Each platoon can contain up to *n* vehicles. Thus the system model is composed of *2n* replicas of the One_vehicle submodel.

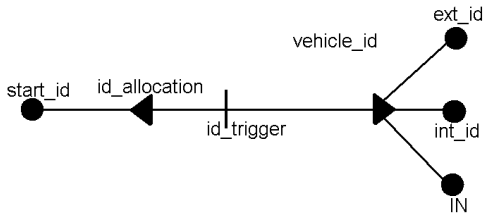

Figure 8: Configuration SAN model

The Configuration submodel contains four places; all of them have initially zero token except start_id which has one token. Places (start_id, int_id, and IN) are shared with the corresponding One_vehicle submodel replicas included in the configuration of the AHS. Initially *2n* replicas are created, *n* vehicles for each platoon. The place ext_id is a global place shared by all sub models, to act as a counter. Each time the instantaneous activity id_trigger is fired, a new vehicle is included in the system and assigned a vehicle_id. Also place IN is marked to initialize: i) the One_vehicle submodel associated with this vehicle, and ii) the Dynamicity submodel that will associate the vehicle to a given platoon. The ID assigned to the vehicle is stored in the place int_id. When a new vehicle joins the

system, int_id gets the value stored in ext_id, which in turn is incremented by one.

3.2.5. SAN system composed model: The system SAN model resulting from the composition of the SAN submodels presented in the previous sub-sections, using joining "join" and replication "Rep" composition operators, is illustrated in Figure 9.

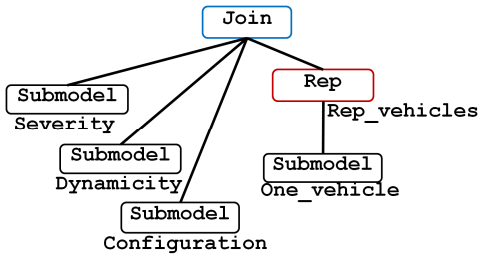

Figure 9: SAN composed model

4. Results and sensitivity analyses

We illustrate the type of results obtained from the processing of the SAN model presented in Section 3, and show sensitivity analyses with respect to various parameters impacting the AHS safety.

The unsafety measure $\bar{S}(t)$ defined in Section 3, corresponds to the probability to have a token in the place KO_total of Figure 6. The analyses focus on the impact on $\bar{S}(t)$ of the failure rates associated with the failure modes, the maximum number of vehicles per platoon, the trip duration, and the AHS coordination strategies.

4.1. Assumptions and values of the parameters

We assume that all the processes represented by timed activities in the SAN models have exponential distributions (i.e., have constant occurrence rates).

Let λ be the smallest failure rate. To facilitate sensitivity analyses, the values of the failure rates λ_i associated with the six failure modes FMi identified in Table 1 are expressed in terms of λ. In this paper, considering the contribution of all sources of failures that can lead to the considered failure mode, we have used the following values:

$\lambda_6 = 4\lambda$; $\lambda_5 = 3\lambda$; $\lambda_4 = 2\lambda$; $\lambda_3 = 2\lambda$; $\lambda_2 = 2\lambda$; $\lambda_1 = \lambda$.

The values of execution rates associated with the maneuvers ($\gamma_{TIE\text{-}N}$, γ_{TIE}, $\gamma_{TIE\text{-}E}$, γ_{CS}, γ_{GS}, γ_{AS}) range from 15/hr and 30/hr (maneuver durations between 4 and 2 minutes).

We suppose that the two highway lanes start initially with n vehicles in each platoon (platoon1 and platoon2). At any time each vehicle can change from its platoon to the other one, with constant change rates (respectively ch1 and ch2 for platoon1 and platoon2 as shown in the Dynamicity submodel of Figure 7). We consider the same numerical values for the two change rates equal to 6/hr.

The numerical values used are inspired from real life similar situations. However, these values can be easily modified.

Each vehicle in platoon2 leaving the highway should pass through platoon1 and stay 3 to 4 minutes in platoon1, before getting out from the highway.

The results presented in the following subsections have been obtained, using the simulator provided by the Möbius tool. Each point of the graphs has been computed as a mean of at least 10000 simulation batches, converging within 95% probability in a 0.1 relative interval. Actually, the total number of simulation batches mainly depends on the value of the failure rate considered.

4.2. Failure rate and number of vehicles impact

We first show in Figure 10 the impact of n, the maximum number of vehicles per platoon on $\bar{S}(t)$, for trip durations varying from 2 to 10 hours.

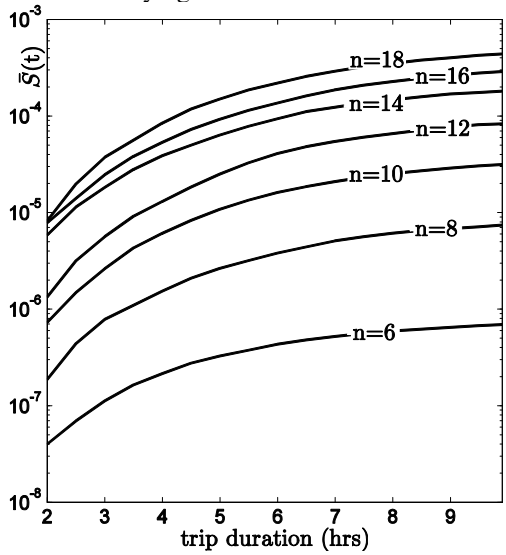

Figure 10: $\bar{S}(t)$ versus time for different *n*
$\lambda = 10^{-5}$/hr, *join* rate=12/hr and *leave* rate = 4/hr

This figure shows that:

- For a given value n, the probability of reaching the unsafe state increases by one order of magnitude when the trip duration increases from 2 to 10 hours.
- For a given trip duration, increasing n leads to a significant increase of $\bar{S}(t)$. For example, when n

is increased from 8 to 12, the unsafety is one order of magnitude higher, for a 10 hours trip duration.

For a failure rate equal to 10^{-5}/hr, the level of unsafety remains low when n is less than 10. Higher values of n lead to a more degraded safety especially when considering long trip durations.

The impact of the failure rate is illustrated in Figure 11 considering three values for λ. We notice that the probability of reaching an unsafe state is very sensitive to the value of the failure rate. For example, increasing the failure rate from 10^{-6}/hr to 10^{-5}/hr, leads to an increase of unsafety of about 175 times, for a trip duration of 6 hours. The variation of system unsafety is lower (about 40 times) when increasing the failure rate from 10^{-5}/hr to 10^{-4}/hr for the same trip duration. Additionally, it can be noticed that the sensitivity of $\bar{S}(t)$ to the trip duration is higher for lower values of the failure rate λ. For λ =10^{-6}/hr the steady state is reached very quickly.

When the failure rate is 10^{-7}/hr, the unsafety is about 10^{-13}. This is why the corresponding curve is not plotted. Similarly, for a 2 hours trip duration, the unsafety is almost 10^{-12}/hr for λ =10^{-6}/hr.

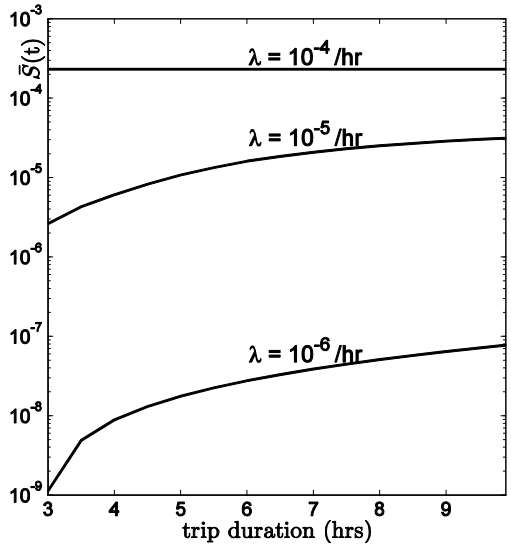

Figure 11: $\bar{S}(t)$ versus time for different λ
n=10 vehicles/platoon, *join* rate=12/hr, *leave* rate=4/hr

Figure 12 shows the impact of the failure rate on system unsafety when the maximum number of vehicles per platoon, n, increases from 10 to 18, considering 6 hour trip duration. We can see that the failure rate has more impact for smaller number of vehicles per platoon.

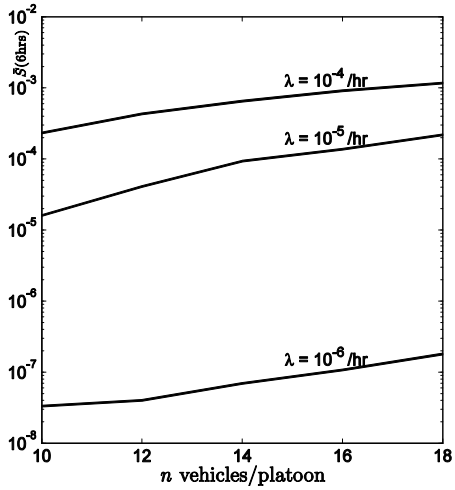

Figure 12: $\bar{S}(t)$ at t=6 hrs versus n for different λ
join rate=12/hr, and *leave* rate=4/hr

4.3. Influence of *leave* and *join* rates

Actually, the system unsafety should depend on the number of vehicles in each platoon that might be affected by failures. The number of vehicles depends on the frequency at which vehicles join and leave the platoon. In order to have a better understanding of the combined influence of the *join* and *leave* rates, we analyze the evolution of system unsafety as a function of the load of the system $\rho=\frac{join\_rate}{leave\_rate}$.

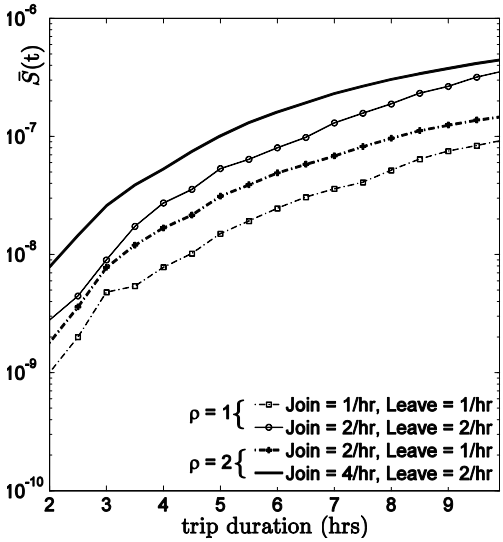

Figure 13: $\bar{S}(t)$ versus trip duration
different *join* and *leave* rates, λ=10^{-5}/hr, n=8

The results are plotted in Figure 13 considering the case ρ=1 and ρ=2, with different values for the *join* and

leave rates. It is interesting to see that similar trends are observed for all the curves corresponding to the same ρ, with the highest unsafety observed for the highest join rate.

Comparison of the results corresponding to different values of ρ and a fixed value of the *leave* rate shows that the highest value ρ leads to the highest level of unsafety. However, the results are of the same order of magnitude.

4.4. Influence of coordination strategy

All the results presented in Sections 4.2 and 4.3 correspond to the case of a decentralized inter- and intra-platoon coordination strategy (DD). Figure 14 compares the unsafety for the four strategies presented in Table 3: DD (Decentralized inter- and intra-platoon) DC (Decentralized inter-platoon and Centralized intra-platoon), CD (Centralized inter-platoon and Decentralized intra-platoon), and CC (Centralized inter- and intra-platoon). We can see that the inter-platoon strategy has more impact than the intra-platoon, with a higher safety observed for the decentralized inter-platoon strategy. This is due to the fact that more vehicles are involved in the centralized inter-platoon coordination (see Section 2.2.1).

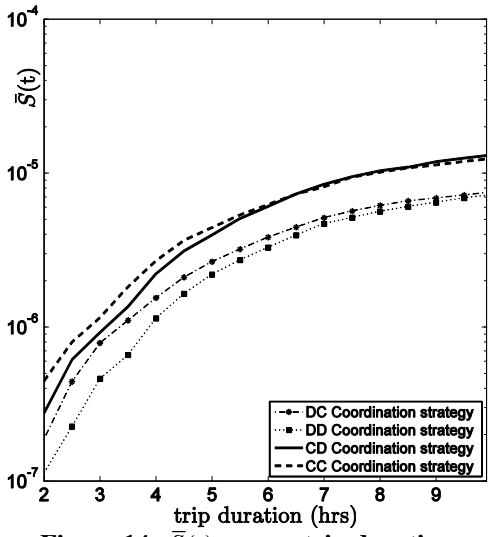

Figure 14: $\bar{S}(t)$ versus trip duration
n=10, λ=10^{-5}/hr, *join* rate=12/hr, *leave* rate=4/hr

The impact of the coordination strategy is low even for higher values of n. This is shown in Figure 15 where the system unsafety at t = *6hrs* is plotted for different values of n.

5. Conclusion and future work

In this paper, we have presented a modeling approach to evaluate the safely of an automated highway system. The models take into account the failure modes affecting vehicles, their severity level, and their associated recovery maneuvers. The modeling approach has been designed to master the complexity of the models taking into account the dynamic evolution of the highway system. The proposed models are based on stochastic activity networks. The system model is elaborated based on submodels characterizing the vehicles' behavior resulting from failures and recovery maneuvers, that are then replicated and composed with other submodels describing the system configuration and its dynamic evolution as the result of vehicles joining and leaving the highway.

To illustrate the feasibility of the approach and the kind of results that can be achieved, we considered the case of a highway composed of two platoons. We performed sensitivity studies to analyze the impact of several parameters on the safety of an automated highway system: the failure rates associated with failure modes affecting vehicles, the maximum number of vehicles per platoon, and different coordination strategies. In particular, the analyses we made have allowed us to quantify and perform a comparative analysis of the level of safety that can be expected with the system studied for different configurations and parameters ranges.

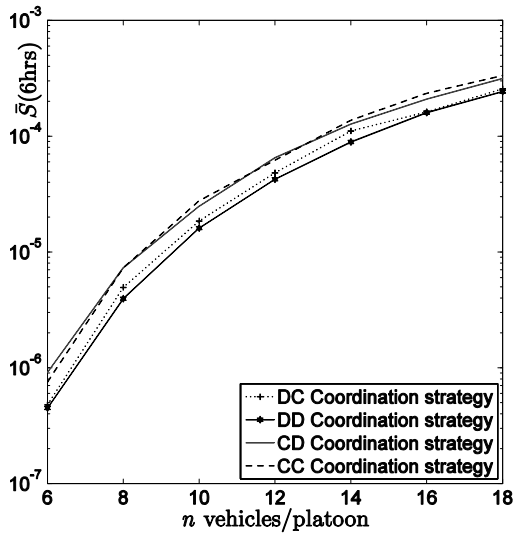

Figure 15: $\bar{S}(t)$ at t=6hrs versus n
λ=10^{-5}/hr, *join* rate=12/hr, *leave* rate=4/hr

The work and results presented in this paper can be considered as a preliminary step in addressing the safety evaluation of automated highway systems. Nevertheless, the results already provide some preliminary indication about the following factors: 1)

the optimal size of platoons; 2) the maximum trip duration; 3) the most suitable coordination strategy of the platoons that lead to better safety. Future work is needed to analyze how to control these factors in an operational context to optimize safety. For the parameters considered in our study, the size of the platoons should not exceed 10 which is consistent with the numbers considered in experimental tests, as reported in [10] for example.

The models presented in this paper can be easily extended to analyze highways composed of a larger number of platoons, considering more complex scenarios. Also, further work is planned to evaluate other collaborative driving systems using e.g., the concept of teamwork for platoon formations [16].

6. References

[1] F. Burggraf, W. N. Carey, P. Johnson, and K. B. Woods, *Intelligent Transportation Systems and Vehicle-Highway Automation*, 2007.

[2] D. N. Godbole, J. Lygeros, E. Singh, A. Deshpande, and A. E. Lindsey, "Towards a Fault Tolerant AHS Design Part II: Design and Verification of Communication Protocols," Institute of Transportation Studies, University of California, Berkeley, Paper UCB-ITS-PRR-96-15 1996.

[3] Fenton, et al., "On the Steering of Automated Vehicles: Theory and Experiment," *IEEE Transaction on Automatic Control*, vol. AC-21, pp. 306-315, June 1976.

[4] R. E. Fenton and R. J. Mayhan, "Automated Highway Studies," in *IEEE Transaction on Vehicular Technology*, vol. 40. the Ohio State University, 1991, pp. 306-315.

[5] P. Varaiya, "Smart Cars on Smart Roads: Problems of Control," *IEEE Transaction on Automatic Control*, vol. 38, pp. 195-207, Feb. 1993.

[6] Y. Furukawa, "Status and Future Direction of Intelligent Drive Assist Technology," *IEEE Intelligent Transportation Systems*, pp. 113-118, 2000.

[7] J. Masayasu, S. Shigeki, U. Ken'ya, and M. Hiroshi, "Design of Lane-Keeping Control with Steering Torque Input," *Transaction of Society of Automotive Engineerings of Japan*, vol. 53, pp. 163-168, 2003.

[8] M. Tsuji, R. Shirato, H. Furusho, and K. Akutagawa, "Estimation of Road Configuration and Vehicle Attitude by Lane Detection for Lane Keeping system," *Society of Automotive Engineers*, pp. 45-51, 2001.

[9] Th. Benz, A. Braun, R. Krause, Pochmuller, W.H. Schulz, M. Schulze, J. Sonntag, "*CHAUFFEUR - TR 1009 User, safety and operational requirements". Project Deliverable D3.1.1, August1996*.

[10] M. Miller and PATH., "Societal and Institutional Issues of Automated Highway Systems," *Intellimotion Paper News*, vol. 6, No. 3, 1997.

[11] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts," *In Lectures on Formal Methods and Performance Analysis*, pp. 315-343. Springer Verlag, 2001.

[12] D. Daly, D. D. Deavours, J. M. Doyle, P. G. Webster, and W. H. Sanders, "Möbius: An extensible tool for perfomance and dependability modeling," *In 11th International Conference, TOOLS 2000*, vol. Lecture Notes in Computer Science, pp. 332-336, Schaumnurg, IL B.R. Haverkort, H. C. Bohnenkamp, and C. U. Smith (Eds.), 2000.

[13] J. Lygeros, D. N. Godbole, and M. Broucke, "Towards a Fault Tolerant AHS Design Part I: Extended Architecture," Institute of Transportation Studies, University of California, Berkeley, PATH Technical Report UCB-ITS-PRR-96-14 1996.

[14] J. Lygeros, D. N. Godbole, and M. Broucke, "A Fault Tolerant Control Architecture for Automated Highway Systems," *Control Systems Technology*, vol. 8, pp. 205-219, March 2000.

[15] J. Lygeros, et al., "Design of an Extended Architecture for Degraded Modes of Operation of IVHS," presented at American Control Conference, UCB-ITS'PWP'95'3, 1995.

[16] S. Hallé and R. J. Chaib-draa, "Collaborative Driving System Using Teamwork for Platoon Formations," *In Applications of Agent Technology in Traffic and Transportation, Whitestein Series in Software Agent Technologies, F. Klügl et al (Eds.), Birkhäuser Verlag,*, 2005.

[17] S. Hallé, "Automated Highway Systems: Platoons of Vehicles Viewed as a Multiagent System," in *Faculté des études supérieures de l'Université Laval*. Québec, 2005, pp. 194.