Systematic Specification of a Service Safety Monitor for Autonomous Vehicles

Nikita Bhardwaj Haupt, Peter Liggesmeyer

Systematic Specification of a Service Safety Monitor for Autonomous Vehicles

Nikita Bhardwaj Haupt
Dept. of Software Engineering: Dependability,
TU Kaiserslautern
Kaiserslautern, Germany
Email: haupt@cs.uni-kl.de

Peter Liggesmeyer
Dept. of Software Engineering: Dependability,
TU Kaiserslautern
Kaiserslautern, Germany
Email: liggesmeyer@cs.uni-kl.de

***Abstract*—Autonomous vehicles are complex safety critical systems that operate in uncertain and dynamic environment. To ensure safe behavior, possibly at all times in all possible situations, they must be aware of themselves, their environment and take decisions accordingly. To this end, safety monitoring is a valuable technique that allows the vehicle to observe its behavior and trigger corrective measures in case of any violations. In this paper, we present a systematic specification for such a safety monitor. The monitor is a collection of safety rules that are obtained by performing hazard and risk analysis based on the operational mode and environmental situation of the vehicle at the time of the hazard. The rules act like safety constraints for the vehicle and in case of a violation generate a trigger to bring vehicle back to a safe state.**

Keywords: safety monitoring, safety monitor, safety rules, autonomous vehicles

I. Introduction

Autonomous vehicles are complex safety critical systems that operate in diverse and dynamic environment. Due to complexity of the system and unpredictability of the environment, it is challenging to anticipate all potential system behaviors at design time. As a consequence, it becomes difficult to determine which system behavior is appropriate in which situation at runtime. Under such circumstances, one way to ensure safe behavior is to supervise the vehicle by observing the failures causing hazardous situations and handling them at the time of its execution.

As defined in [1], safety is "the absence of catastrophic consequences on the user(s) and the environment". Based on this definition, *safe behavior* of an autonomous vehicle can be defined as the capability of the vehicle to accomplish its tasks (e.g. driving), make decisions according to the changes in itself or the environment and at the same time ensure safety. The magnitude of *safe behavior* depends upon the level of autonomy, likelihood of human intervention and the environmental context. For instance, in presence of a human driver, a system malfunction can be tolerated by switching-off the function and giving driver the complete control of the vehicle. However, in case of a fully-autonomous vehicle, in the absence of a human assistance, the vehicle must be capable of detecting and tolerating a safety critical situation on its own.

Safety critical situations can arise due to random errors in hardware components (e.g. sensors) or due to unsuitable environmental conditions at runtime. These situations often cause an *unplanned behavior* of the vehicle, which in a certain situation could result in a hazard, or even an accident, if left undetected. Since, it is unknown at design time in which situation which random error would occur and lead to a hazardous event, to maintain safe behavior, it is essential to be aware about it on the first place.

This can be achieved by monitoring the vehicle by means of a safety monitor that observes its behavior and trigger corrective measures in case of violations. Monitoring safety of the vehicle at runtime complements traditional safety assurance as it aids in finding design time as well as runtime defects that could potentially occur in software or hardware due to unexpected environmental conditions or runtime faults [2].

This way safety monitoring acts as a fault tolerance technique where, the fundamental task of the monitor is to continually administer the system for violations and bring it back to a safe state in the event of safety critical deviations [3]. A safety monitor, sometimes coined differently as safety manager [4] or safety bag [5], equipped autonomous vehicle acts like a self-aware system [6] capable of altering its behavior in response to the change in the environment or its own components to maintain safety.

In this paper, we present a systematic procedure for specifying such a *service safety monitor*, a sub-module of a *service monitor*, that monitors the vehicle for *safety critical deviations* using a set of *safety rules*. These rules are derived by performing hazard analysis of the deviations occurring in vehicle services in a particular scenario during a specific *operational mode*. The monitor ensures safe behavior of the vehicle by

triggering corresponding corrective measures in case of detected deviations.

The rest of the paper is organized as follows: In Section II, we present the definitions used in our approach followed by a detailed and a stepwise specification of the safety the monitor. In Section III, we conclude this paper summarising the proposed monitoring approach.

II. Safety Monitoring Approach

As demonstrated in Fig. 1 (a), safety monitor encompasses three modules: a *System Service Monitor* (SSM), *Configuration Evaluation* (CE) and a *Knowledge Base* (KB). SSM is the principal module of the safety monitor. It is a collection of safety rules which are obtained at design time via *Hazard and Risk Analysis* (HARA) [11]. Each rule represents planned behavior of the component and its corresponding potential safety-critical deviations.

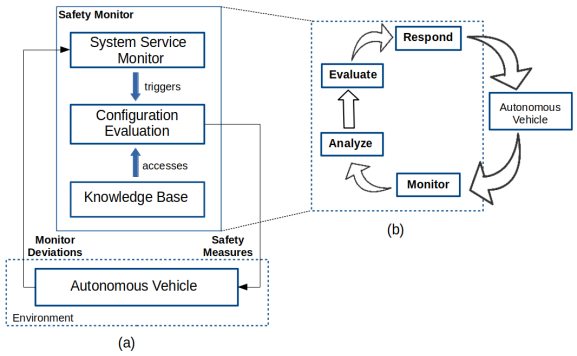

Fig. 1. Safety Monitor Specification and Monitoring Procedure

The primary task of SSM is to monitor these deviations as they occur and trigger CE for a safety measure. The main goal of CE module is to evaluate the safety of the vehicle in accordance to the currently activated operational mode and take safety measures, if necessary. This is accomplished by carrying out a runtime risk analysis [10] based on the system information stored in the KB that acts like a knowledge repository that assists CE with system evaluation at runtime. The risk assessment procedure implemented in CE is out of scope of this paper, and thus not discussed further.

A definitive step-wise procedure of runtime safety monitoring is described in Fig. 1 (b). Safety monitor implements a knowledge-based system monitoring which can be outlined as a sequence of four consecutive computations: *Monitor-Analyze-Evaluate-Respond* (MAER). The monitoring and analyses is performed by SSM. In case of safety-critical deviations, SSM triggers CE that evaluates risk associated with the vehicle and takes safety measures as a response to those deviations.

By means of a *safety monitor* we employ runtime monitoring to ensure safe operation of a vehicle (or its components). This is achieved by actively monitoring the currently activated configuration for safety critical deviations in its services. In this manner, our monitoring approach does not aim at fault prevention or fault removal but, at fault tolerance by detecting them and prompting safety measures to avoid any unsafe situations. The behavior of the monitor is a declarative collection of safety rules, where each rule represents the safety status of the vehicle and its corresponding restorative measure. To derive these rules and a systematic specification of our service monitor, we perform the following procedure:

I. *Firstly*, we determine all operational modes of the vehicle along with their potential configurations that can be activated during operation.
II. *Secondly*, we ascertain complete set of services associated with each configuration for their respective operational modes.
III. *Thirdly,* we perform hazards and risk analysis to identify the potential deviations in services that could result in hazardous situations during operation.
IV. *Lastly,* we assign these deviations an integrity level based on the risk associated them. We then analyse dependencies between services and their deviations for a given operational mode and environmental situation, followed by constructing safety statuses and corresponding measures to form the rules.

Step I. Operational Modes and Configurations: First and foremost, we begin with determining all possible operational modes (*OPM*) that a vehicle is capable of. An OPM represents the level of autonomy with which system is operating. We classify them into: fully-autonomous (*AM*), semi-autonomous (*SM*) and manual mode (*MM*). A fully-autonomous mode is where all configurations of the vehicle are capable of carrying out all operations automatically i.e. without the presence of a human driver. However, in case of the other two, presence of a human driver is always required.

Subsequently, we determine the potential configurations for each operational mode. At the moment, all configurations are pre-determined at design-time. Each mode can have multiple configurations out of which only one can be activated at a time. Normally, configurations differ from each another in terms of functionality or redundancy. For instance, in case of Tractor Implement Automation (TIA) [8], a tractor (*Trac*) can have separate configurations for different implements[1] e.g. a baler or a harvester, or

[1]An implement is a device or component that is attached to a tractor to perform a specific task like: a *harvester* for harvesting purposes.

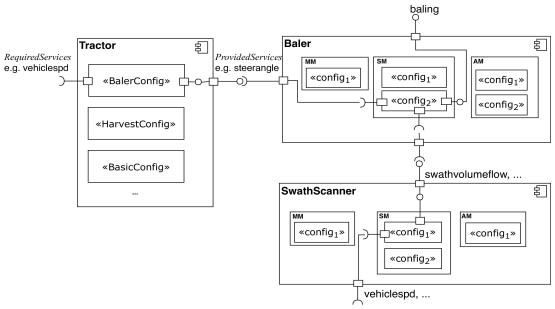

Fig. 2. Operational Modes & Configurations of TIA Vehicle

redundant configurations in case of graceful degradation or maintainance purposes. Similarly, implements like baler (*Bal*) and swath scanner (*SwSc*) can have multiple configurations in different operational modes for baling specific tasks.

$$\begin{aligned} \{Trac^{AM}_{Cf_1}, Trac^{SM}_{Cf_1}, ...\} &= Bal\_Trac^{OPM_i}_{potCf_j}, \\ \{Bal^{AM}_{Cf_1}, Bal^{AM}_{Cf_2}, Bal^{SM}_{Cf_1}, ...\} &= Bal^{OPM_m}_{potCf_n} \end{aligned} \tag{1}$$

Identification and categorization of the potential configurations based on their operational modes has a twofold advantage: On the one hand, it assists in ascertaining the possible collaborations profiles (*CollabProf*) between multiple configurations of the vehicle and its implements in different operational modes. On the other hand, it aids in an intensive hazard analysis. This due to the fact that, both the risk, associated with a particular deviation, and the magnitude of the corresponding safety measures to ensure safety, depends upon the activated configuration and the mode in which vehicle is operating.

$$\begin{aligned} \langle Trac^{AM}_{Cf_1} :: Bal^{AM}_{Cf_1} :: SwSc^{AM}_{Cf_1} \rangle \in CollabProf_1, \\ \{CollabProf_1, CollabProf_2, ...\} = {CollabProf_n}^{Bal} \end{aligned} \tag{2}$$

In TIA, for each implement, there exist at least one collaboration profile to carry out the implement specific task. The equations above manifest an exemplary collaboration profile that consists of configurations of a *Trac*, *Bal* and a *SwSc* collaborating together to render baling. In this case, the tractor as well as the baler support multiple operational modes and configurations. Thus there exist multiple potential collaboration profiles for carrying out baling specific tasks.

Step II. Services and Potential Configurations: Once we have all operational modes along with their potential configurations, the next step is to determine services associated with each of those configurations. Each configuration has a set of services that includes both required and provided services. Required services (*rs*) are the ones that a configuration receives from another components, whereas provided services (*ps*) are the services that a configuration renders for other components and their configurations.

$$\{vehspd_{rs}, steerang_{ps}, ...\} = Trac^{AM}_{Cf_1} \tag{3}$$

The reason behind ascertaining all services of a configuration is to filter the safety critical services from the non-safety critical ones. Typically, deviation in a required service influences the provided service thereby, causing an unplanned behavior of the entire configuration. For instance, a deviation in the speed sensor of the tractor results in an incorrect value of vehicle speed (*vehspd*). As a consequence, the tractor doesn't decelerate while steering thereby, loosing control over itself. However, it is also possible that the provided service suffers a deviation despite of no deviation(s) in the required services. Regardless of whether the deviation is at the required service or at the end of provided service, it results in an unsafe and unplanned behavior of the configuration thereby, in a hazardous situation of the entire vehicle.

Step III. Hazard and Risk Analysis: After identifying the set of safety critical services, we perform hazard and risk analysis to analyse their possible deviations and their consequences. We classify these deviations based on their discrepancies attributed to time, value or provision. For instance, in case of a tractor, if the service *vehspd* must be generated within 10ms from request time, but is generated after a delay of 2ms, then the service suffers a deviation attributed to time. In a fully-autonomous mode, even such small time-deviation might result in a hazardous situation as the tractor is unaware of its own speed for this duration. Moreover, if the speed generated after the delay (i.e. at 12ms) is incorrect, the safety of the vehicle, along with its implements, gets more vulnerable.

A particular deviation in a service can have different severities based on the operational mode and the environmental situation during vehicle operation. For instance, an incorrect value of *vehspd* in an autonomous mode is highly critical compared to in the semi-autonomous mode when the driver is present and can take control of the vehicle almost immediately. Moreover, when another tractor is driving ahead in the field, a delay in *vehspd* can result in delayed deceleration and thus collision of the two vehicles. However, in case of no additional vehicle ahead delay deviation in *vehspd* would be still critical but, would not have collision as an outcome. Therefore, while performing hazard analysis, we take the operational mode of the vehicle and its context into consideration as it aids in an in-depth analysis of the consequences of the deviations in services.

Step IV. Safety Statuses and Corresponding Measures: Subsequent to hazard identification, we estimate the risk associated with the deviations and assign them a corresponding integrity levels. Since we have an autonomous agricultural vehicle, we do the risk estimation in accordance with standard ISO 25119 [7] and consider the parameters: *Severity* of the accident caused by the deviation, the *likelihood* of the accident and the *controllability* of the situation to assign agricultural performance levels (AgPL) from 'a' to 'e' [9] for different levels of risk.

$$\langle if\ SafStatus \Rightarrow SafMeasure \rangle \in SRule \quad (4)$$

Following the AgPL assignment, the very last step is to construct safety statuses (*SafStatus*) for the safety rule (*SRule*). Each status acts like a condition which when true, indicates the vehicle being in an unsafe state and thereby, triggers a corresponding countermeasure (*SafMeasure*). Equation 5 is an exemplar safety rule for TIA-Baling system. In case of a delay in front obstacle sensor signal, all autonomous configurations, for *Trac, Bal* and *SwSc*, are reconfigured to semi-autonomous mode.

$$\langle if\ (FObstSignal\ delay \leq 400ms\ while\ VSpeed \geq 15) \Rightarrow\ (AutoC_{f1}\ to\ SemiAutoC_{f1}) \rangle \in SRule_1 \quad (5)$$

During the TIA case study, we observed that not all deviations, despite being in the safety critical services, result in hazardous situations. These are the deviations that are either improbable to occur or are easily controllable and thus, have a corresponding AgPl of 'a' or below (QM). We filter such deviations and consider the ones that have AgPL 'b' or higher for the safety statuses. Besides, we realised that creating safety statuses and an equivalent corrective measure for each individual service would result in a safety rule explosion. Especially, when the number of safety critical services is higher. Moreover, there exist certain associations between the some services where, a particular deviation in one along with a certain deviation in the other, in a specific operational mode, results in a hazardous situation with potentially catastrophic consequences.

To this end, a safety rule consists of a safety status that represent an unsafe state of the vehicle caused either due to individual service deviation or a deviation due to the associated services having an AgPL of 'b' or above, in a particular operational mode during a specific scenario. As a safety measure, we reconfigure the system to a configuration that brings the system back to a safe state. For each safety status, safety measure is a set of potential configurations that the vehicle can configure to. At runtime, the currently activated configuration as well as the other potential configurations are evaluated using a complexity based risk metrics [10].

III. Summary and Conclusion

This paper presented a stepwise specification for a service safety monitor, a sub-module of a safety monitor, that administers an autonomous vehicle for safety critical deviations during its execution. The monitor is a collection of safety rules obtained by performing hazard and risk analysis at design time. We believe that for distributed autonomous system like TIA, such a safety monitor not only aids in achieving fault tolerance by prompting safety measures in form of reconfiguration, but aids in self-awareness and allows it to adapt its behavior to sustain a safe behavior at runtime.

Presently we are implementing the monitor in autonomous vehicles in the agricultural and road vehicle domain. As future work, we plan to explore the benefits and tackle challenges associated with its implementation and validation. Escalating complexity of safety rules owing to higher dependencies among and due to increasing amount of system services, structural decisions like centralized or decentralized monitor for the system with regards to functional and non-functional properties like performance and efficiency and validation of the monitor itself are one of the many challenges to be investigated systematically as a part of our research.

References

[1] A. Avizienis et. al, *Basic Concepts and Taxonomy of Dependable and Secure Computing*, IEEE Transactions on Dependable and Secure Computing, IEEE, Vol.1, 2004.

[2] P. Koopman, *Challenges In Representing CPS Safety*, In Workshop on Developing Dependable and Secure Automotive Cyber-Physical Systems from Components, 2011.

[3] Amina Mekki-Mokhtar et. al, *Safety Trigger Conditions for Critical Autonomous Systems*, In The 18th IEEE Pacific Rim International Symposium on Dependable Computing, 2012.

[4] C. Pace and D. Seward, *A safety integrated architecture for an autonomous safety excavator*, In International Symposium on Automation and Robotics in Construction, 2000.

[5] P. Klein, *The safety-bag expert system in the electronic railway interlocking system Elektra*, Expert Systems with Applications, 3:499 506, 1991.

[6] J. Schlatow et. al., *Self-Awareness in Autonomous Automotive Systems*, In Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017, 2017.

[7] ISO 25119-2:2010 *Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 2: Concept phase*, https://www.iso.org/standard/45048.html, 2018.

[8] M. Hoyningen-Huene et. al., *Tractor-Implement-Automation and its application to a tractor-loader wagon combination*, Machine Control & Guidance, pp. 171–185, 2010.

[9] R. K. Benneweis, *FACILITATING AGRICULTURE AUTOMATION USING STANDARDS*, Club of Bologna, In Proceedings, Vol. 17, 2006.

[10] N. Bhardwaj and P. Liggesmeyer, *A Conceptual Framework for Safe Reconfiguration in Open System of Systems*, In 6th International Workshop on Software Engineering for Systems-of-Systems, pp. 17–20, SeSOS '18, 2018.

[11] N. Bhardwaj and P. Liggesmeyer, *A Runtime Risk Assessment Concept for Safe Reconfiguration in Open Adaptive Systems*, In: Computer Safety, Reliability, and Security, SAFECOMP 2017. Lecture Notes in Computer Science, Vol.10489, Springer, Cham, 2017.