The Challenge of Safety Tactics Synchronization for Cooperative Systems

Elena Lisova
Malardalen University
Vasteras, Sweden
elena.lisova@mdh.se

Svetlana Girs
Malardalen university
Vasteras, Sweden
svetlana.girs@mdh.se

ABSTRACT

Given rapid progress in integrating operational and industrial technologies and recent increase in the level of automation in safety-related systems, cooperative cyber-physical systems are emerging in a self-contained area requiring new approaches for addressing their critical properties such as safety and security. The notion of tactics is used to describe a relation between a system input and its corresponding response. Cooperative functionalities often rely on wireless communication and incoherent behavior of different wireless channels makes it challenging to achieve harmonization in deployment of systems' tactics. In this work we focus on safety tactics for cooperative cyber-physical systems as a response to inputs related to both safety and security, i.e., we are interested in security informed safety, and formulate a challenge of synchronization of safety tactics between the cooperating systems. To motivate the requirement on such synchronization we consider a car platoon, i.e., a set of cooperative vehicles, as an example and illustrate possible hazards arising from unsynchronized tactics deployment.

1 INTRODUCTION

Today we are witnessing a significant progress in industrial and operational technologies allowing to merge them in a system that combines physical processes and computational capabilities, can have external connections, communicate and cooperate with other systems and have different degrees of autonomy. Such cooperative cyber-physical systems (CO-CPSs) are more efficient and can have functionalities that are exceeding the onces coming from traditional systems. However, new challenges arise in these systems as well, as, e.g., wireless solutions, together with benefits in terms of reconfiguration, weight and complexity, also bring a challenge towards security due to openness of wireless channels possibly allowing an adversary to receive transmitted messages or interfere with the channel. Moreover, the majority of such systems are safety-critical as they have humans in the loop and thus, their safety has to be addressed. Safety of CO-CPSs cannot be guaranteed without incorporating security considerations, as a security breach can potentially contribute to hazards. Thus, CO-CPSs are required to have safety reactions to inputs coming from the sub-systems and surrounding environment, which might indicate on failures caused by both safety or security reasons. Moreover, given the complexity of CO-CPSs and frequent system updates due to security considerations, e.g., patches, safety reactions can be required to evolve with time. Emerging behavior is an immense challenge to address for such systems, and one of the aspects to solve in this domain is alignment of how CO-CPSs are seeing each other, e.g., common awareness of communication channels failures, and how their reactions are synchronized.

As system reactions are based on inputs from environment or other systems, communicational infrastructure and its state assessment play an important role. By assessment here we mean estimation of its current reliability level, as this level is directly connected to how much a CO-CPS can trust in correctness of inputs from other CO-CPSs and consequently to which extent the CO-CPS shall make decisions on its own. Moreover, grounds for further analyses and decision making need to be considered already during the system architecture design, once a particular architecture for collaborative systems is chosen [3].

On the system architectural level, safety can be discussed in terms of tactics. A tactic can be defined as "a design decision that influences the control of a quality attribute response" [2]. Initially this term was proposed for six quality attributes (availability, modifiability, security, performance, usability and testability), but later extended by Wu and Kelly [16] to be applied for safety. A safety tactic captures how to get a desired system safety response for various stimuli coming as inputs to the system. Each attribute can be associated with a set of attribute primitives, e.g., some of security primitives are encryption, integrity, firewalls [2]. Such primitives can be developed in architectural patterns that incorporate features necessary for such primitive being in place. The notion of tactics is defined on the system architecture level, however, system tactics influence the quality of the considered attribute, i.e., they influence the decision making process and system response. In this work we use the term tactic as it was initially proposed on the architectural level, but also to refer to its exact implementation. Thus, the discussed above challenge of safety responses synchronization and their implementations for CO-CPSs falls into safety tactics synchronization challenges. As was proposed by Wu and Kelly, safety tactics may include aim, description, rationale expressed with Goal-Structuring Notation (GSN), applicability, consequences, side effects, practical strategies and related patterns and other tactics. From what is important for our consideration, a tactic includes a logical input-processing-output chain along with deadlines for each step and can be refined further depending on the required level of details. We assume that safety tactics include possible input to the system that can be also provoked by an attack on it. Thus,

ISSA 2018, September 3-7, Barcelona, Spain

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

we advocate security informed safety tactics instead of pure safety tactics as communication interfaces of a CO-CPS significantly increase its attack surface and make it impossible to claim a CO-CPS being safe if it is not secure.

This paper is our initial effort in tackling CO-CPS's wireless communication assessment and handling of failures originated in communication channels and related to both safety and security. These failures have to be addressed as CO-CPSs depend on communication. It is crucial to analyze how a communication channel failure can be perceived by different cooperating systems, e.g., whether the failure is detected by all communicating systems, whether detection can be done within a predefined time range and whether the cause of the failure can be assessed in a similar way by all the cooperative systems. In this paper we look at a car platoon as an example of a set of CO-CPSs that cooperate (drive and maneuverer together) to achieve a common goal, e.g., reduction of fuel consumption. Some of the questions that arise in this example are whether a failure of the leading vehicle will be perceived in the same manner by all participants and, e.g., disengaging maneuver will be performed in a safe manner, whether a failure of one of the platooning vehicles will be detected by others in time (this is important as a not detected failure of one vehicle can be hazardous to the whole platoon, e.g., if a vehicle that is compromised by an adversary ruins the string stability of the system [5]). As CO-CPSs form a relatively new domain, a gap can be observed in literature discussing their architecture principles, which include communication infrastructure, and knowledge about their practical realization [11]. Looking at platooning, there are papers describing particular aspects of in-platoon communication, e.g., a platoon leader trustworthiness [7] or communication topologies [10] for vehicles within the platoon, but it is not straightforward to find information in regard to overall communication infrastructure [1], i.e., where intelligence/decision making is placed, what the vehicles' tactics and platoon strategies are. For example, it is clear that platoon members should estimate reliability of communication channels in order to understand when to stop following the commands from the leading vehicle, however a realization of this monitoring and a logic behind making such decisions is not well presented in the literature. Even though platoon demonstrators from such manufacturers as Volvo and SCANIA exist, due to novelty of the area and its continuous development there is a lack of common agreement on how to analyze such systems. Hence, the contribution of this paper is, looking at a car platoon as an example of CO-CPSs, formulation of safety tactics synchronization challenge and a proposal on how to address it. Two scenarios of a communication failure are used to illustrate the hazards arising from safety tactics being unsynchronized. Moreover, possible ways to address the challenge are discussed and proposed as future work.

The remainder of the paper is structured as following: Section 2 introduces platooning, while the considered scenarios of failure perception are presented in Section 3. Next, Section 4 discusses the synchronization of safety tactics and Section 5 concludes the paper.

2 EXAMPLE – A PLATOON

The use case considered in this work is a platoon of vehicles which drive close together and in a collaborative manner, led by the front vehicle, Fig. 1. Each vehicle has a set of sensors, radars and other equipment to sense the road and any other cars or obstacles in the proximity. Moreover, every vehicle within the platoon is equipped with communication infrastructure to exchange information with other platoon members. It was shown before that, having all necessary sensors, vehicles are able to operate safely and detect acceleration or breaking performed by the vehicle in front even without communicating [12]. However, performance of a platoon where vehicles do not communicate with each other is significantly lower as communication provides additional source of information in the system [17]. Moreover, with communication not only the following vehicle, but also the other members of the platoon can be timely informed about a maneuver. Various communication strategies for organizing information exchange between the vehicles within a platoon exist [9, 10] including options with neighboring cars communicating only with each other or with each other and also the platoon leader, scenarios with the platoon leader sending commands to all vehicles directly or intermediate members forwarding the information. Selection of a concrete communication scheme is outside of the scope of this paper, but to have a more specific scenario we consider a case where the leading vehicle coordinates the platoon by communicating to every member directly and informing the members about its position, speed and maneuver intentions. To make this possible, there exist a communication link between every platoon member and the leader vehicle. Additionally, platoon as a whole establishes connection with the surrounding environment such as other vehicles or road infrastructure nodes. This information exchange supports the work of various safety applications such as, e.g., cooperative forward collision warning, warning about an approaching emergency vehicle, pre-crash sensing warnings, and aims at providing drivers with information about critical situations in order to prevent accidents. One important feature of cooperative driving is the way the cooperating vehicles influence each other's behavior, e.g., by triggering auto brake in following vehicles if the lead one issues such command. Performance of such collaborative schemes depends of reliability of the communication between the members and timely reaction on the changes both in behavior of the vehicles and communication quality.

3 FAILURE PERCEPTION IN A PLATOON

As demonstrated in Fig. 1, we consider two scenarios of a failure occurrence and its propagation in a platoon. In *Scenario A*, one of the platooning vehicles experiences a failure of its communication channel to the leading vehicle, i.e., this vehicle cannot rely on timely and correct transmission of its messages and cannot trust in correctness of incoming packets (if any comes). We do not consider a particular cause of the failure, e.g., packet losses or delays, failure of receiving hardware [6], but assume that it can be triggered by causes associated with both safety and security domains. We assume that such failure is detected by the platooning vehicle and a decision about consequent actions, i.e., safety mechanisms, aligned with the corresponding safety tactic is made. In *Scenario A*, there are two aspects to consider. First, is whether the failure is detected in a similar way by both ends of this communication channel, i.e., if both the leading and the platooning vehicles recognize the failure and if they do it synchronously, i.e., the difference between moments of failure detection is below a certain threshold. Upon failure detection, both vehicles are supposed to activate safety mechanisms from their predefined safety strategies; obviously, these tactics have to be aligned with each other. If the failure is not recognized in the same way by the two vehicles, then, for example, the platooning vehicle can make a decision about leaving the platoon (one of possible safety mechanisms for the platooning vehicle upon a communication failure), while there is no command from the leading vehicle to the rest of the platoon to make space for the disengaging vehicle (for disengaging, the distances between the vehicle leaving the platoon and its neighbors have to be increased). We assume alike mechanisms for channel reliability estimation and failure detection being deployed within communicating nodes, however the same mechanism does not guarantee the same response as nodes communicating over the same wireless channel might not experience the same channel quality.

The second aspect to consider in *Scenario A* is the perception of such failure by other platooning vehicles. It is important both that other platoon members cooperate and allow the vehicle that detected the failure to disengage, but also that they have situation awareness in general (i.e., which failures have been detected and by whom), which may be of interest for all platooning vehicles as they all influence each-other's decision making process. Such awareness of the status of platooning vehicles can be seen as redundant and not needed during the normal operation of the platoon, given that control of the platoon is managed by the leading vehicle. However, it can be of use when failures occur, especially if they are caused by related attacks as then additional measures may be required to take back the control over vehicles.

Scenario B represents a situation where the platoon leader experiences a communication failure, e.g., its communication hardware has failed or its communication channels have been jammed. Obviously, such a failure needs to be recognized by the platooning vehicles and a corresponding action has to be taken, e.g., the whole platoon can disengage or it has to be reconfigured into a platoon with a new leader. Different vehicles can assess the same wireless communication channel differently and thus, timely detection of a failure in such communication channel is a challenge from a CO-CPS design point of view. Moreover, to disengage, vehicles need to increase the distances between each other, which requires cooperation and negotiation to complete the maneuver. And, as such maneuver is a part of safety tactics of platooning vehicles, we again see the need for synchronization of the safety tactics.

These examples of communication failures and how they are perceived by CO-CPSs are indicating that the challenge of synchronization of CO-CPSs' safety tactics (which include a particular failure and its cause, safety reaction to the failure and timing requirements for the reaction) needs to be addressed.

4 SAFETY TACTICS SYNCHRONIZATION FOR CO-CPSS

In the previous section we showed how a failure in a wireless communication channel can be perceived differently within a set of CO-CPSs and how it can potentially contribute to a hazard. Based on the considered example we can distinguish three levels of required synchronization in CO-CPSs' safety tactics. Accordingly, we formulate three following sub-challenges:

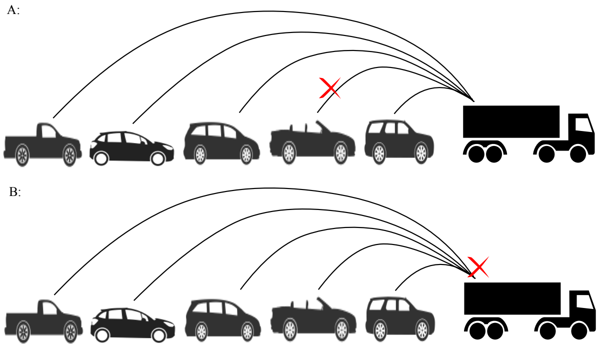

Figure 1: Examples of failure scenarios in a platoon: A – communication failure of a single platooning vehicle; B – communication failure of the leading vehicle.

(1) Alignment of sets of the predefined safety tactics in different CO-CPSs (e.g., having in mind different manufactures).
(2) Sufficient synchronization of communication reliability assessment done by different CO-CPSs.
(3) Synchronized deployment of selected safety tactics by CO-CPSs.

The first sub-challenge belongs to the design phase of CO-CPSs and requires corresponding standardization grounds. Having platooning as an example, in a perspective it is expected that all platoon eligible vehicles would be able to join an existing platoon, regardless of their manufacturer. This can be addressed via a corresponding legislation, making manufacturers synchronize the set of safety tactics between each other, or at least have the same minimum set of required tactics. From a design point of view, to achieve such unification among vehicle components responsible for failure detection and deployment of corresponding safety mechanisms, one can look at the concept of Safety Element out of Context (SEooC) proposed by the automotive functional safety standard ISO 26262 [8]. The SEooC concept enables design of an element outside of the context of a specific system, but upon assumptions about safety relevant properties that need to be validated later during integration of the element. Given that such CO-CPS component needs to be reused in all communicating CO-CPSs, its development may be required to comply with high integrity demands. In this regard, SEooC development and assurance process have been already extended with semi-formal assumption/guarantee contract methodology [14]. Thus, the concept of SEooC can be a good candidate to be used for component design for CO-CPSs responsible for assessment of communication quality.

The second sub-challenge is provoked by the nature of wireless communication. Packets transmitted over wireless media are subjects to bit errors and packet delays and losses caused by pathloss, i.e., degradation of the signal strength with distance, multipath fading and shadowing. Moreover, wireless channels are not necessary symmetrical in both directions, change their characteristics with time and in space. Thus, communicating nodes might observe different levels of packet errors and losses, making channel estimation and common agreement on its reliability level a challenging task.

If a communication channel is not reliable anymore, all CO-CPSs using this channel need to make the same estimation and decision about channel reliability. This is required as correct operation of the system needs cooperation. When channel quality estimation is done at the communication end-points, the "black channel" model proposed in IEC 61508 [4] can be used for handling the inherent unreliability of wireless links. This model implies that we cannot guarantee communication properties of the channel and a challenge of communication assessment and corresponding reactions should be handled by the CO-CPSs.

The last sub-challenge refers to a necessity for a CO-CPS "to understand" what other CO-CPSs are doing, what they are responding to and what may follow, i.e, which particular safety tactic is being currently deployed. It may be of high importance for a CO-CPS to be aware if one of other CO-CPSs has detected a communication failure and whether its cause comes from safety or security domain. This is important as it may, for example, indicate a general problem with communication that can affect other channels with time or a security breach that can lead to jeopardizing all involved CO-CPSs. Distinguishing between security and safety causes of a failure is a separate challenging task and may require additional techniques being deployed to determine the origin of the failure. Identification of the cause is crucial, as, e.g., in case of a security breach some of the usual fail-safe modes as shutting down and rebutting can make the situation worse, unless the adversary is located and isolated from communication network. Otherwise, the adversary can gain even more advantage if being present during the network reboot.

As the first step to address the challenge of safety tactics synchronization presented by a combination of sub-challenges above, we propose to design a CO-CPS channel state manager. Such manager can be developed as a part of a CO-CPS aiming to assess the reliability of the black channel in light of communication anomalies. This can be done by, e.g., extending the SEooC contract-based development process by detailing it further for a particular case of a CO-CPS channel state manager. To be able to assess the reliability level of communication, the channel state manager needs to have an incorporated monitor assessing parameters that are chosen based on related security and safety analyses. Even though traditionally safety and security analyses are conducted separately [13], for such monitor we need to consider them jointly as we want to catch possible interdependencies. Thus, first we need to develop a methodology of such monitor design as it will require corresponding joint analyses to determine relevant failure modes and attacks. The next step in regard to the CO-CPS channel state manager is its evaluation in terms of effectiveness and applicability. Further, the CO-CPS channel state manager needs to be integrated into a CO-CPS state manager [15], which is responsible for making a decision about the current system state and a particular safety mechanism being deployed, as information gained from the channel state manager can affect the decisions made by the CO-CPS state manager.

5 CONCLUSIONS

In this paper we formulated and motivated a challenge of safety tactics synchronization for cooperative systems. We considered two scenarios of possible failure occurrences in a system of platooning vehicles that illustrate the need of common perception of a wireless communication channel state among the collaborating systems. The challenge was refined into three sub-challenges reflecting the need for design of common safety tactics, coherent failure perception and synchronization of corresponding safety reactions. We also proposed a CO-CPS channel state manager as the fist step in addressing the formulated challenges.

Future work includes development of a design methodology for a CO-CPS channel state manager in which safety and security are threated jointly and its further evaluation. The latter includes simulations to evaluate applicability and effectiveness of the manager and later implementation. In parallel, we plan to consider how a system response is handled, i.e., to integrate the CO-CPS channel state manager into the system state manager.

ACKNOWLEDGMENTS

The work is supported by the Swedish Foundation for Strategic Research (SSF) via the Future factories in the Cloud (FiC) and the Secure and Dependable Platforms for Autonomy (Serendipity) projects.

REFERENCES

[1] J. Axelsson. 2017. Safety in Vehicle Platooning: A Systematic Literature Review. *IEEE Trans. on Intelligent Transportation Systems* 18, 5 (2017), 1033–1045.

[2] L. Bass, P.C. Clements, and R. Kazman. 2003. *Software Architecture in Practice.* Addison-Wesley, London.

[3] B. Bauer, J. P. Müller, and S. Roser. 2008. Decentralized Business Process Modeling and Enactment: ICT Architecture Topologies and Decision Methods. In *Programming Multi-Agent Systems.* 1–26.

[4] CENELEC. 2007. IEC 61508: Functional Safety of E/E/PE Safety-Related Systems. Part 2: Requirements for E/E/PE Safety-Related Systems.

[5] S. Dadras, R. M. Gerdes, and R. Sharma. 2015. Vehicular Platooning in an Adversarial Environment. In *Proc. of the 10th ACM Symp. on Information, Computer and Comm. Security (ASIA CCS '15).* 167–178.

[6] S. Girs, I. Sljivo, and O. Jaradat. 2017. Contract-based assurance for wireless cooperative functions of vehicular systems. In *IECON 2017 - 43rd Annual Conf. of the IEEE Ind. Electronics Society.* 8391–8396.

[7] H. Hu, R. Lu, Z. Zhang, and J. Shao. 2017. REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET. *IEEE Trans. on Vehicular Tech.* 66, 2 (2017), 1786–1797.

[8] International Organization for Standardization (ISO). 2011. ISO 26262: Road Vehicles - Functional Safety.

[9] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen. 2016. A Survey on Platoon-Based Vehicular Cyber-Physical Systems. *IEEE Comm. Surveys Tutorials* 18, 1 (2016), 263–284.

[10] F. Michaud, P. Lepage, P. Frenette, D. Letourneau, and N. Gaubert. 2006. Coordinated Maneuvering of Automated Vehicles in Platoons. *IEEE Trans. on Intelligent Transportation Systems* 7, 4 (2006), 437–447.

[11] P. Pop, D. Scholle, I. Šljivo, H. Hansson, G. Widforss, and M. Rosqvist. 2017. Safe cooperating cyber-physical systems using wireless communication: The SafeCOP approach. *Microprocessors and Microsystems* 53 (2017), 42 – 50.

[12] S. Sheikholeslam and C. A. Desoer. 1993. Longitudinal control of a platoon of vehicles with no communication of lead vehicle information: a system level study. *IEEE Trans. on Vehicular Tech.* 42, 4 (1993), 546–554.

[13] A. Čaušević. 2017. A risk and threat assessment approaches overview in autonomous systems of systems. In *Proc. of the XXVI Int. Conf. on Information, Comm. and Automation Techn. (ICAT).* 1–6.

[14] I. Šljivo, B. Gallina, J. Carlson, and H. Hansson. 2015. Using Safety Contracts to Guide the Integration of Reusable Safety Elements within ISO 26262. In *Proc. of the IEEE 21st Pacific Rim Int. Symposium on Dependable Computing (PRDC).* 129–138.

[15] I. Šljivo, B. Gallina, and B. Kaiser. 2017. Assuring Degradation Cascades of Car Platoons via Contracts. In *Proc. of the 6th Int. Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems.* 317–329.

[16] W. Wu and T. Kelly. 2004. Safety tactics for software architecture design. In *Proc. of the 28th Annual Int. Computer Software and Applications Conf., 2004. COMPSAC 2004.*, Vol. 1. 368–375.

[17] L. Xu, L. Y. Wang, G. Yin, and H. Zhang. 2014. Communication Information Structures and Contents for Enhanced Safety of Highway Vehicle Platoons. *IEEE Trans. on Vehicular Tech.* 63, 9 (2014), 4206–4220.