Governance & Autonomy: Towards a Governance-based Analysis of Autonomy in Cyber-Physical Systems-of-Systems

Governance & Autonomy: Towards a Governance-based Analysis of Autonomy in Cyber-Physical Systems-of-Systems

Mohamad Gharib, Paolo Lollini, Andrea Ceccarelli, Andrea Bondavalli
University of Florence - DiMaI
Viale Morgagni 65, Florence, Italy
{mohamad.gharib,paolo.lollini,andrea.ceccarelli,andrea.bondavalli}@unifi.it

***Abstract*—One of the main challenges in integrating Cyber-Physical System-of-Systems (CPSoS) to function as a single integrated system is the autonomy of its CPSs, which may lead conflicts among them due to lack of coordination. We advocate that to efficiently integrate CPSs within the overall context of the CPSoS, we need to adjust the autonomy of some CPSs in a way that enables them to coordinate their activities to avoid any conflict among one another. To achieve that, we need to incorporate the notion of governance within the CPSoS design, which defines rules that can be used for clearly specifying who and how can adjust the autonomy of a CPS. In this paper, we try to tackle this problem by proposing a new conceptual model that can be used for performing a governance-based analysis of autonomy for CPSs within CPSoS. We illustrate the utility of the model with an example from the automotive domain concerning a cooperative driver overtaking assistance system.**

***Index Terms*—Autonomy, Governance, Cyber-Physical Systems of Systems, CPSoS, SoS, Conceptual Modeling**

I. Introduction

A Systems of Systems (SoS) is an integration of a finite number of systems that are independent and operable, which are networked together to achieve a higher goal [1]. While a Cyber-Physical System-of-Systems (CPSoS) is an SoS but its component systems are Cyber-Physical Systems (CPSs), where a CPS is a system consisting of cyber components, controlled components and possibly of interacting humans [2].

Assuring that a CPSoS/SoS can function as a single integrated system to support a common mission is a main goal for the CPSoS/SoS community [1], [2]. However, such integration is not an easy task due to the unique and special nature that distinguishes CPSoS/SoS from other types of systems, and especially the autonomy of its components (e.g., CPSs) [2]. More specifically, the autonomy of CPSs may lead to conflicts and unsafe situations due to the lack of coordination among CPSs. For instance, a self-driving car that was in autonomous driving mode has hit and killed a woman that was walking outside of the crosswalk recently [3]. This is an example where the autonomy of CPSs led to a lack of coordination among CPSs that, in turn, have led to a disaster.

In a previous work [4], we argued that coordination among CPSs can be achieved by adjusting the autonomy level of some CPSs within the overall CPSoS in a way that enables them to safely perform their own activities without endangering any other CPS that is operating in the same environment. Although several researchers have suggested adjusting the autonomy level of a system based on various aspects such as its capability, motivations, behavior, etc. [5], [6]. We proposed criteria for determining the autonomy level of a CPS based on their *Awareness* concerning their operational environment as well as their capability to safely perform their activity (e.g., *Controllability*) [4]. Based on these criteria, a *CPS* can have *full, partial* or *limited autonomy* for performing a specific *activity*.

However, we did not provide *governance rules/policies* that specify who and how can adjust the autonomy of CPSs. In other words, component systems (e.g., CPSs) maintain an ability to operate autonomously, but their operational mode is subordinated to a central managed purpose [7], [8]. Such central managed purpose can be expressed by *governance rules/policies*. Governance can be defined as the set of rules, policies, and decision-making criteria that will guide the CPSoS/SoS while achieving its goals [7]. Governance is not a new concept, it is an emerging paradigm in Systems Theory [9], and it represents a cornerstone of an effective CPSoS/SoS [7]. Despite this, it did not receive enough attention from the CPSoS/SoS community [7], [9].

To this end, we advocate that in order to efficiently integrate CPSs within the overall context of their CPSoS, we need to incorporate the notion of governance within the CPSoS design. In this paper, we try to tackle this problem by proposing a new conceptual model that can be used for providing a governance-based autonomy analysis for CPSs within CPSoS. In other words, the model can be used for analyzing the autonomy level of CPSs taking into consideration governance rules defined by the CPSoS.

The rest of this paper is organized as follows; Section II describes a motivating example we use to illustrate our work. We propose a conceptual model that can be used for providing a governance-based analysis of autonomy for CPSoS in Section III, and we illustrate its applicability to a realistic scenario from the automotive domain in Section IV. Related work is presented in Section V. Finally, we conclude and discuss future work in Section VI.

II. Motivating Example: Cooperative Driver Overtaking Assistance System

Overtaking on undivided roads is one of the most complex driving tasks, where a driver may make several decisions based on the traffic conditions [10], i.e., a driver needs to identify an acceptable size gap in the opposing traffic, the time at which he initiates the overtake as well as the time at which to return to its lane in front of the preceding vehicle [11]. In particular, overtaking is one of the major traffic safety problems, that is why there is much work towards developing driving support systems that reduce overtake-related accidents [10]–[12].

The cooperative driver overtaking assistance system aims at supporting drivers to avoid overtake-related accidents on undivided roads, where Advanced Driver Assistance Systems (ADAS), Road Side Units (RSUs), vehicles, and other road infrastructure cooperate to reduce overtake-related accidents. In particular, *RSUs* collect and disseminate information that assists drivers/ADAS to avoid overtake-related accidents. While *ADAS* aims at improving the driver's safety by a thorough task analysis of overtaking activity considering the driver's ability to complete a safe overtake. The ADAS can monitor, warn and even take control of the vehicle in case the driver is not able to perform/complete a safe overtake.

Information can be exchanged (sent and received) between the system components either directly relying on dedicated channels (e.g., wired or wireless channels), or indirectly relying on acquiring such information by sensing the domain. For example, RSUs/drivers can acquire information about close-by vehicles by sensing/seeing [13].

The main components of the system are shown in Fig. 1, and we can also identify the four **S**teps in a successful overtake: **S1.** the driver estimates the possibility of safely overtaking a preceding vehicle, **S2.** the driver initiates the overtaking, **S3.** the driver passes the preceding vehicle in the opposite lane, and **S4.** changing the lane back into the original lane of the vehicle, which completes the overtaking successfully. Considering these steps, a vehicle can be in 1- safe area, it is safe from overtaking-related hazard; 2- warning area, it can be in danger due to an overtake in process; and 3- danger area, it is in imminent danger from an overtake in process.

III. A Conceptual model for Governance-based Analysis of Autonomy in Cyber-Physical Systems-of-Systems

A conceptual model should include main constructs that represent the key *concepts* of the domain along with the *relationships* among them. To this end, the proposed conceptual model contains the required *concepts* and *relationships* that allows for performing a governance-based analysis of autonomy levels for CPSs within CPSoS.

The meta-model of the proposed conceptual model is depicted in Figure 2. In which, we can identify a *CPSoS* that *integrates CPSs*. For instance, the cooperative driver overtaking assistance system is a *CPSoS* that *integrates* several *CPSs* such as RSUs, ADAS, drivers, etc. A *CPS* can *perform activities* for achieving its own objectives and/or the objectives of the overall *CPSoS*. For example, a driver may *perform* an overtake (an *activity*) to pass a slower vehicle. Usually, an *activity* is *performed* in an operational environment (we call *Sphere of Action (SoA)* [13]), which is a part of the domain. For instance, an overtake (*activity*) can be *performed* in specific part of an undivided rural roads (*SoA*). A *SoA* can be *described* by *information*. For example, an RSU can acquire information describing the situation of the traffic concerning some part of an undivided rural road. *CPSs* can rely on one another for information, i.e., a *CPS* can provide/receive *information* depending on the *information provision* concept. For instance, a driver can depend on a RSU to provide him with information concerning the road situation.

A *CPS* must be aware of its *SoA* to operate in it, and the *awareness of* relationship between a *CPS* and a *SoA* is used to capture such relation. Following [5], we differentiate between 1- *aware by self*, when a CPS has the self-capability to be aware of its *SoA*, e.g., CPS is independent, and 2- *aware by dependency*, when a CPS needs to depend on other CPS to be aware of its *SoA*, e.g., CPS is dependent. For instance, a driver is *aware by self* of the road situation, if he has the self-capability for acquiring information describing the road situation. While a driver is *aware by dependency* of the road situation, if he depends on an RSU to provide him with such information.

The *controllability* of a *CPS* over the performance of an *activity* it aims to perform is captured relying on the *controllability* relationship, which is characterized by one attribute, namely *controllability level* that can be: 1- *Controllable*, a *CPS* is able to detect and avoid any obstacle that might prevent it from safely performing its activity in a timely manner; 2- *Uncontrollable*, a *CPS* is not able to detect and/or avoid all obstacles that might prevent it from safely performing its activity in a timely manner. For example, performing an overtake during daylight where there are no obstacles limiting/preventing the driver's visibility is *controllable* by the driver since he has the capability to detect another vehicle and avoid colliding with it in a timely manner. While performing an overtake with no support of RSUs when the driver visibility is limited might be *uncontrollable*.

To capture the autonomy level of a *CPS* concerning the performance of an activity, we extend the *perform* relationship between the *CPS* and *Activity* concepts with the *autonomy level* attribute that can be, 1- *Full autonomy,* if the *CPS* is *aware by self* of the environment, and the *activity* is *controllable* with respect to the *CPS* capability, 2- *Partial autonomy,* if it is *aware by dependency* and the *activity* is *controllable* by it, and 3- *Limited autonomy,* if the *activity* is *uncontrollable* regardless if it is *aware by self/dependency* of the environment.

In what follows, we describe the concepts, relationships and attributes that can be used for modeling governance within CPSoS. A *CPSoS* can set *Governance rules*, which can be defined as a set of rules, policies, and decision-making criteria that will guide the CPSs while achieving their goals [7]. For example, adjusting the autonomy of the driver (a *CPS*) from

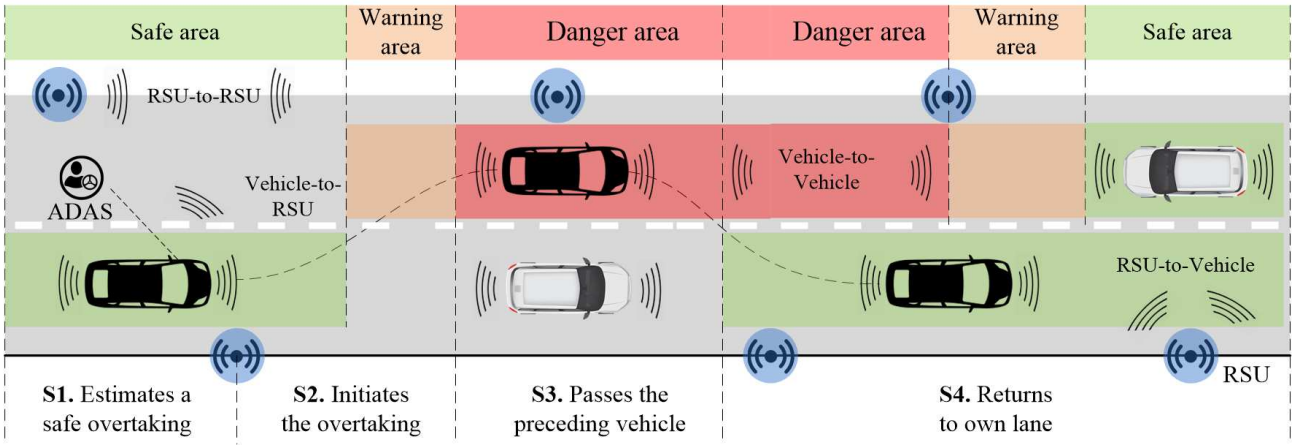

Fig. 1. A diagram of the cooperative overtaking assistance system with the critical zones

Full autonomy to *Partial* or *Limited autonomy* based on his type of *awareness* of the *SoA* and his *controllability level* concerning the activity can be specified within the *Governance rules* specified by the Cooperative Driver Overtaking Assistance System (a *CPSoS*).

Governance rules can *specify* the *power* a *CPS* may *possess*, where *power* can be defined as the capacity or ability to direct or influence the behavior of others [14], [15], i. e., the power of a *CPS* within the *CPSoS* is the maximum potential ability of a *CPS* to influence the behavior of other *CPS* concerning some performed activity. Following [14], we adopt five bases/sources of power: 1- **R**eward power is defined as power whose basis is the ability to reward; 2- **C**oercive power is defined as power whose basis is the ability to punish; 3- **L**egitimate power is defined as power whose basis is a formal authority that an individual has, which allows it to influence another individual(s), who has/have an obligation to accept such influence; 4- Re**F**erent power is defined as power whose basis is trust, respect, and admiration between individuals; and 5- **E**xpert power is defined as power whose basis is knowledge and experience that an individual attributes to another one within a specific area.

Power determines the *authority* a *CPS* may *has* over another *CPS* concerning the performance of some activities, where *authority* can be defined as the right to give orders, make decisions, and enforce obedience [15]. For instance, the ADAS (a *CPS*) can *possess* an **E**xpert/**L**egitimate power over the driver (another *CPS*). This power gives the ADAS the *authority* over the driver performance *concerning* the overtake activity.

We differentiate between three types of *authorities*[1]: 1- **M**onitoring is the process of observing and analyzing the behavior of an individual in order to detect any undesirable behavior; 2- **W**arning is the process of informing an individual, usually in advance, of possible danger, problem, or other unpleasant situation; and 3- **C**ontroling is the process of influencing, directing or even determining the behavior of an individual. Several researchers (e.g., [14], [16], [17]) have concluded that various sources of power have different influence over the individuals' behavior, which is out of the scope of this paper. In this work, we consider **E**xpert and **L**egitimate power, where the first grants only **M**onitoring and **W**arning *authorities*, while the last grants **M**onitoring, **W**arning as well as **C**ontroling *authorities*.

For example, when the ADAS have the **E**xpert power, it can be in the passive overtaking assistant mode, i.e., it has the monitoring and warning *authorities* over the driver when the driver has a partial autonomy to perform an overtake. While when the ADAS have **L**egitimate power, it can be in the active overtaking assistant mode, i.e., it has the monitoring, warning and also controlling *authorities* over the driver when the driver has a limited autonomy to perform an overtake.

IV. Illustrating the Utility of the Conceptual Model

We illustrate the utility of the conceptual model by applying it to a realistic scenario concerning the Cooperative Driver Overtaking Assistance System. Consider for example a driver that aims at reaching his/her destination safely using an undivided (two-lanes) road. Depending on the situation of the traffic, the driver may perform several overtakes before reaching his destination. Most overtakes on undivided roads can be broadly classified under three different types:

1) *Safe overtaking in clear visual conditions,* the driver has sufficient visibility for maintaining safe separation from other vehicles/obstacles while performing the overtake, i.e., the driver can self-detect (*aware by self*) and avoid any vehicle/obstacle while performing the overtake (the overtake is *controllable*).
2) *Safe overtaking in unclear visual conditions,* the driver may not has the self-capability to detect other vehicles while performing his overtake. This could be due to the nature of the road (e.g., a sharp curve) or due to weather conditions (e.g., fog, heavy rain, etc.). In such a situation, the driver can rely on RSUs to provide him

[1]These types are not mutually exclusive, i.e., a *CPS* may have all three types of *authorities* over another *CPS*

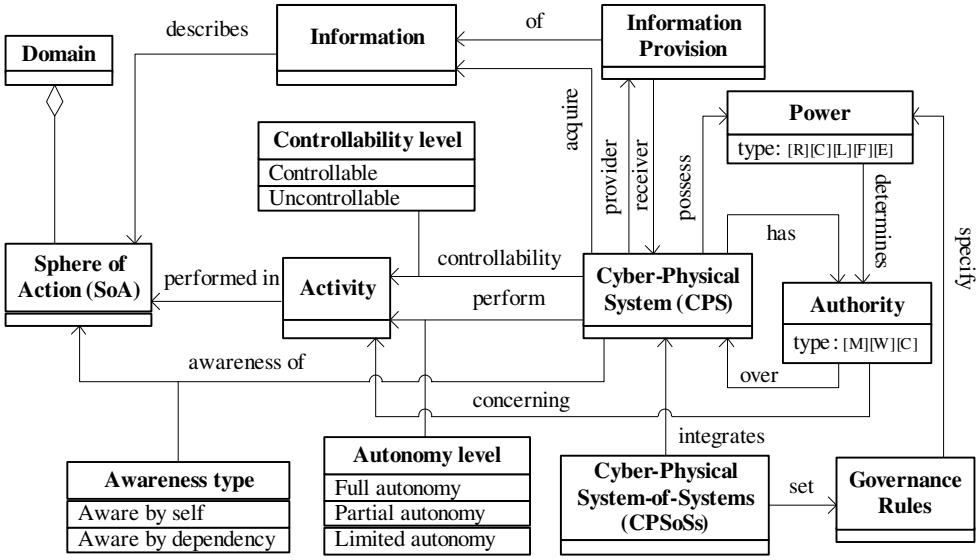

Fig. 2. The meta-model of the proposed conceptual model

with such information (i.e., *aware by dependency*). However, with such information, the overtake is considered *controllable* by the driver.

3) *Unsafe overtaking in critical conditions*, the driver is considered incapable of performing a safe overtake regardless of his type of awareness of the *SoA* (e.g., *aware by self* or *aware by dependency*). Note that the cooperative driver overtaking assistance system identifies such overtakes by analyzing the location, speed and direction of other vehicles in the maneuver area, i.e., the system can estimate whether an overtake is *controllable* or *uncontrollable* by the driver.

Taking the previous three types of overtaking, the cooperative driver overtaking assistance system and to increase drivers' safety by reducing overtake-related accidents can set *Governance rules* for specifying the autonomy allowed to drivers based on their type of *awareness* of the *SoA* and their *controllability levels* concerning the overtakes. Such rules can be interpreted into power that determines authorities over the driver's performance concerning the overtake activity.

For the first type of overtaking, the driver can have *Full autonomy* concerning any overtake he wishes to perform, i.e., the ADAS system is not granted any power/authority over the driver and it provides no assistance at all. In the second type of overtaking, the driver can have *Patial autonomy* concerning any overtake he wishes to perform. The ADAS system is granted an *Expert power* over the driver, which allows it to be in the passive assistance mode, i.e., it has the authority to monitor the driver's behavior and warn him about any possible dangerous situation. While in the last type of overtaking, the driver can have *Limited autonomy* concerning any overtake he wishes to perform. The ADAS system is granted a *Legitimate power* over the driver, which allows it to be in the active assistance mode, i.e., it has the authority not only to monitor and warn the driver but also to interrupt and control the overtake (e.g., reduces speed, applies breaks, prevents initiating the overtake, prevents changing the lane). Fig. 3 shows an abstract flow chart of a governance-based analysis of the driver's autonomy concerning the three different types of overtaking.

Due to space limitation, we only describe the task analysis concerning the driver's autonomy in unsafe overtaking in critical conditions that is shown in Fig. 4. As previously mentioned, a successful overtake in undivided roads consists of four main **S**teps.

In **S1**, the driver first decides there is a need for overtaking, which depends on the speed of the preceding vehicle, his/her desired speed, etc. After deciding there is a need for overtaking, the driver waits an acceptable gap in the opposing traffic that allows him/her to initiate the overtake. However, even if the driver believes that there is an acceptable gap in the opposing traffic, the ADAS may have another opinion as drivers might have poor judgment concerning the distance and speed of opposing vehicles, or they might not even see such vehicles until they initiate the overtake. In other words, the ADAS have better judgment than the driver, therefore, if the ADAS decides that the gap is not appropriate, it will warn the driver about that. If the driver did not comply with the warning, the ADAS will prevent him/her from initiating such overtake. In particular, the driver is allowed to initiate the overtake only if the ADAS allows that.

In **S2**, the driver starts accelerating and steering aiming at changing lanes, if the ADAS detects any obstacle/vehicle in the opposing lane that may prevent the driver from safely changing lanes, it warns the driver, stops acceleration and prevents the driver from changing lanes if it has to, i.e., the ADAS halts the overtake and the driver stays behind the preceding vehicle. Otherwise, the driver is allowed to change lanes. The driver starts **S3** by accelerating to pass the preceding vehicle, yet if

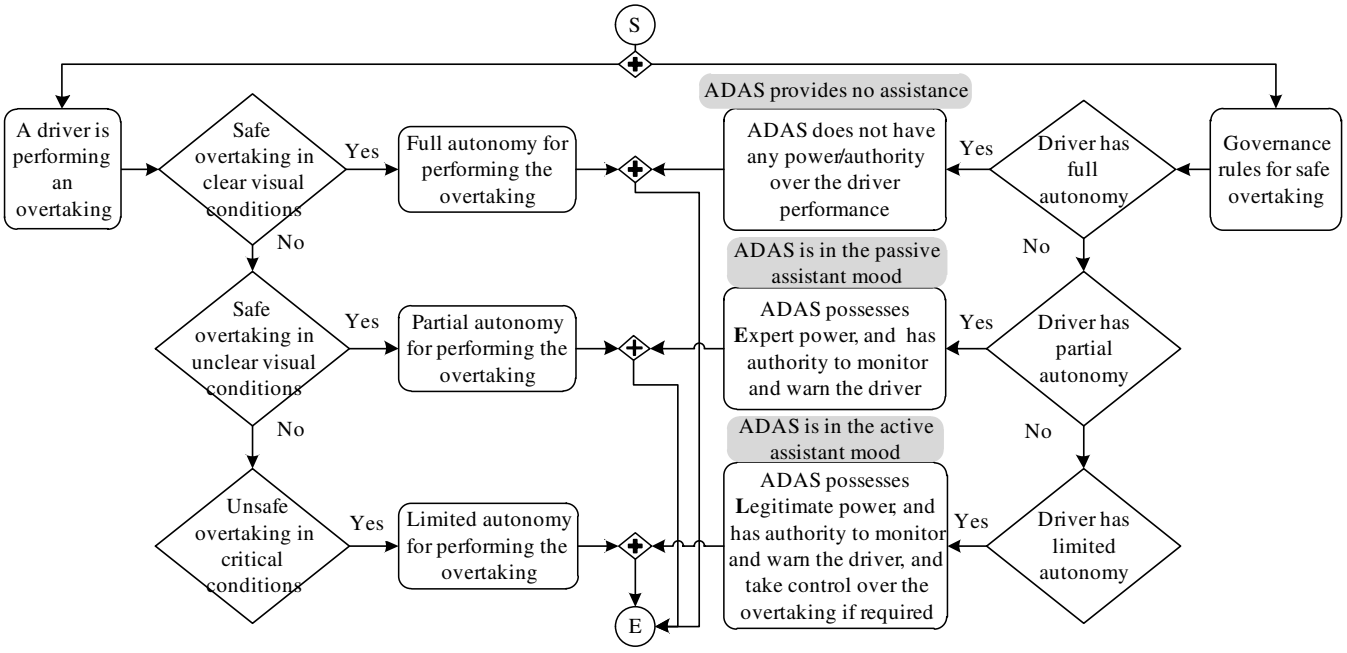

Fig. 3. An abstract flow chart of a governance-based analysis of the driver's autonomy

the ADAS decided that the driver cannot safely complete the overtake, it halts the overtake and the vehicle returns behind the preceding vehicle.

After passing the preceding vehicle, **S3** completes and **S4** starts. In which, the driver maintains his/her speed trying to find an acceptable space to return to its original lane in front of the preceding vehicle(s). However, the driver is allowed to do that only if the ADAS decides that the available gap is adequate for completing the overtake. Otherwise, the ADAS warns the driver that the space is not sufficient/adequate, and if the driver tries to change lanes, the ADAS will prevent that. In such case, the driver can maintain his/her speed and stay at the opposing lane waiting for adequate space/gap if there is no vehicle in the opposing direction. While if there is a vehicle, the ADAS will halt the overtake and the vehicle will return behind the preceding vehicle.

V. Related work

As previously mentioned, governance did not receive enough attention from the CPSoS/SoS community [7], [9]. Despite this, several researchers have devoted effort toward researching governance for CPSoS/SoS. For instance, Morris et al. [8] survey the available literature concerning information technology (IT) governance and identify six key characteristics of good IT governance that can be used for SoS. Moreover, Vaneman and Jaskot [7] worked toward developing a criteria-based framework for SoS governance by conducting a survey of governance practices within the IT community with the main aim of identifying elements of good SoS governance. Keating [9] explores the implications of Complex System Governance (CSG) trying to find suggestions or even solutions for similar governance challenges faced in the development of the System of Systems Engineering (SoSE) area. Based on [9], Keating and Bradley [18] presented a preliminary reference model suitable for the emerging field of CSG.

Unlike existing solutions, we propose to link the governance concept to the concepts of power and authority when adjusting the level of autonomy of some CPS within the CPSoS.

VI. Conclusions and Future Work

In this paper, we advocate that to efficiently integrate CPSs within the overall context of their CPSoS, we need to adjust the autonomy of some CPSs. To achieve that, we incorporated the notion of governance within the CPSoS design, which defines rules for clearly specifying who and how can adjust the autonomy of a CPS. Moreover, we proposed a conceptual model that can be used for performing a governance-based analysis of autonomy for CPSs within CPSoS. Additionally, we illustrated the utility and applicability of our model by applying it to a realistic example from the automotive domain.

For future work, we intend to further investigate other aspects that might influence the autonomy levels of CPSs. We will also refine the proposed concepts aiming at performing more expressive analysis. Finally, we will extend our model-based approach presented in [4] with the new concepts and relationships proposed in this paper.

References

[1] M. Jamshidi, "System of systems engineering - New challenges for the 21st century," *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 5, pp. 4–19, 2008.

[2] P. Lollini, M. Mori, A. Babu, and S. Bouchenak, "AMADEOS sysML profile for SoS conceptual modeling," in *Lecture Notes in Computer Science*. Springer, 2016, vol. 10099 LNCS, pp. 97–127.

[3] S. Levin and J. C. Wong, "Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian — Technology — The Guardian," p. 1, 2018.

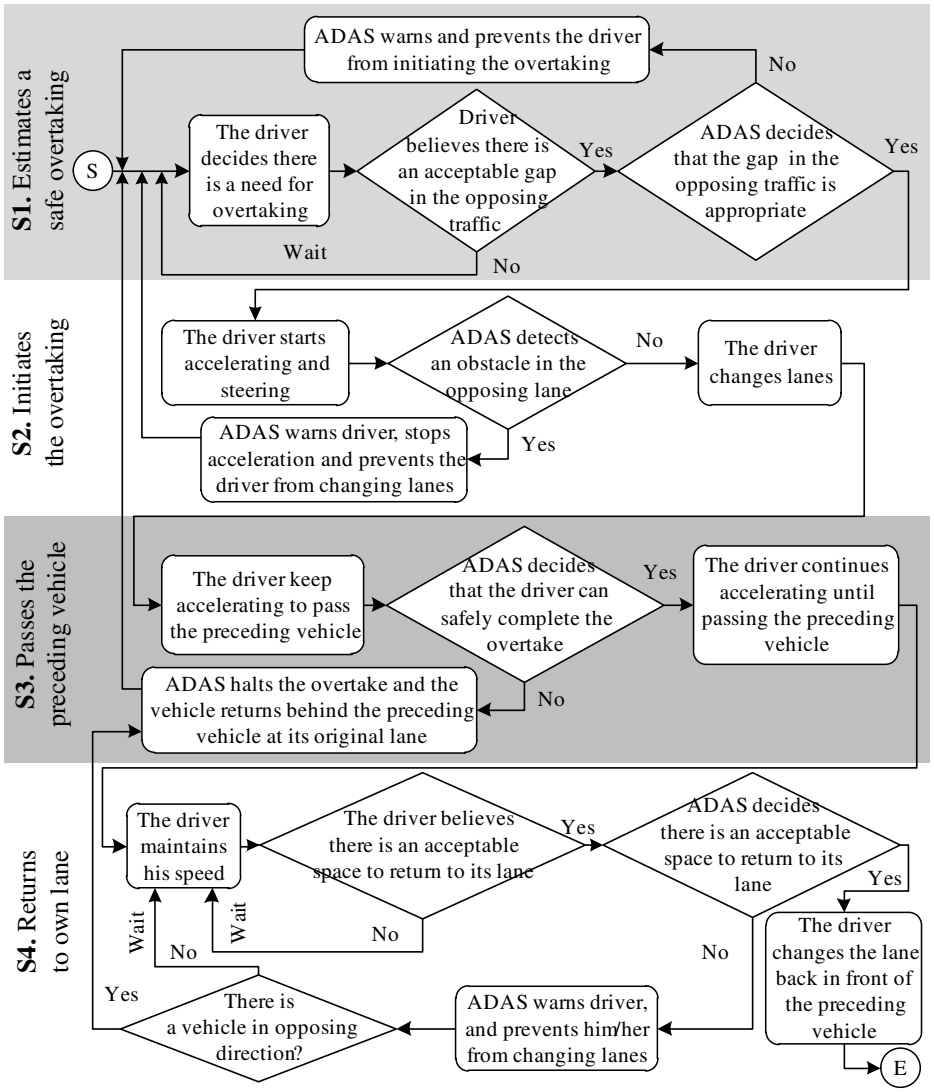

Fig. 4. An flow chart of a governance-based analysis of the driver's autonomy in *Unsafe overtaking in critical conditions*

[4] M. Gharib, L. D. Da Silva, H. Kavalionak, and A. Ceccarelli, "A Model-Based Approach for Analyzing the Autonomy Levels for Cyber-Physical Systems-of-Systems," in *Proceedings - 8th Latin-American Symposium on Dependable Computing, 2018*, pp. 135–144.

[5] C. Castelfranchi, "Guarantees for autonomy in cognitive agent architecture," in *Intelligent agents*. Springer, 1995, pp. 56–70.

[6] C. E. Martin and K. S. Barber, "Multiple, simultaneous autonomy levels for agent-based systems," in *the 4th international conference on control, automation, robotics, and vision*. , 1996, pp. 1318–1322.

[7] W. K. Vaneman and R. D. Jaskot, "A criteria-based framework for establishing system of systems governance," *SysCon - 7th Annual IEEE International Systems Conference, Proceedings*, pp. 491–496, 2013.

[8] E. Morris, P. Place, and D. Smith, "System-of-Systems Governance: New Patterns of Thought," Carnegie Mellon Uni. Pittsburgh, Software Engineering Institute (SEI), Tech. Rep., 2006.

[9] C. B. Keating, "Governance implications for meeting challenges in the system of systems engineering field," *Proceedings of the 9th International Conference on System of Systems Engineering: The Socio-Technical Perspective, SoSE 2014*, pp. 154–159, 2014.

[10] A. C. Figueira and A. P. C. Larocca, "Analysis of the factors influencing overtaking in two-lane highways: A driving simulator study," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 69, pp. 38–48, 2020.

[11] J. M. Jenkins and L. R. Rilett, "Application of distributed traffic simulation for passing behavior study," *Transportation Research Record*, vol. 1899, no. 1899, pp. 11–18, jan 2004.

[12] G. Hegeman, K. Brookhuis, and S. Hoogendoorn, "Opportunities of advanced driver assistance systems towards overtaking," *European Journal of Transport and Infrastructure Research*, vol. 5, no. 4, pp. 281–296, 2020.

[13] M. Gharib, P. Lollini, and A. Bondavalli, "A conceptual model for analyzing information quality in System-of-Systems," in *12th System of Systems Engineering Conference, SoSE17*. IEEE, 2017, pp. 1–6.

[14] J. R. French and B. Raven, "The bases of Social Power," *Experimental brain research. Experimentelle Hirnforschung. Experimentation cerebrale*, vol. 110, no. 2, pp. 196–204, 1959.

[15] D. Garland, "Oxford University Press," pp. 1–55, 1985.

[16] J. Rodin and I. L. Janis, "The social power of health-care practitioners as agents of change," *Journal of Social Issues*, vol. 35, no. 1, pp. 60–81, 1979.

[17] G. Yukl and C. M. Falbe, "Importance of different power sources in downward and lateral relations." *Journal of applied psychology*, vol. 76, no. 3, p. 416, 1991.

[18] C. B. Keating and J. M. Bradley, "Complex system governance reference model," *International Journal of System of Systems Engineering*, vol. 6, no. 1/2, p. 33, 2015.