

# Value Networks and Monetization Strategies for C-ITS Safety Use Cases

Pol Camps-Aragó<sup>a</sup>, Simon Delaere<sup>b</sup> and Ruben D’Hauwers  
*imec-SMIT, Vrije Universiteit Brussel (VUB), Brussels, Belgium*

**Keywords:** C-ITS, Value Network, Supply Chain Management, Monetization Strategies, Business Models.

**Abstract:** C-ITS safety use cases promise to reduce road accidents. However, deploying the necessary system elements that enable such use cases entails challenges in terms of value network coordination, return on investments in infrastructure and in-vehicle devices, and monetization of services. In short, this paper aims at contributing to overcome these economic challenges by (i) clarifying the overall value network and interactions amongst key stakeholders, (ii) proposing how to incentivise the fulfilment of bottleneck value network roles, (iii) providing recommendations on how to incentivise investments and the monetization of C-ITS services, and (iv) arguing for a data exchange and governance model based on regulatory and business model aspects.

## 1 INTRODUCTION

Cooperative Intelligent Transport Systems (C-ITS) enable vehicles to communicate with each other and coordinate their actions, and to interact and coordinate with road infrastructure as well, thereby enhancing the intelligence of current roads and transport systems. C-ITS covers a broad range of safety and traffic efficiency use cases: in this paper, we focus on safety-related ones, such as road works and hazards warnings and cooperative emergency braking. These specific use cases were tested within the CONCORDA European project, in the context of which our analysis was performed.


C-ITS is expected to contribute to substantial increases in road safety and traffic efficiency across Europe (European Commission, 2016). Moreover, the Commission views C-ITS technology as complementary to automated driving, and hence as a pillar of the EU’s long-term strategy on mobility.


However, in order for C-ITS to deliver its expected societal benefits, several elements need to be widely adopted, since these systems exhibit strong direct network effects: from a single vehicle’s point of view, nearby vehicles and roads must also be equipped with telecommunications technology, and digital information services must be provided without

interruption. Therefore, a key business requirement is the deployment of connected roadside infrastructure and in-car hardware elements, investments that face a ‘chicken and egg’ problem (C-ITS Platform, 2016).

In addition, the business case for isolated, individual safety-related C-ITS use cases is far from certain. Based on current and proposed European regulation, we assume that safety-related services, such as road hazards warnings, will be provided free of charge at the point of use. More specifically, both the Delegated Regulation 886/2013 and the proposed C-ITS Regulation (European Commission, 2019)—which was later rejected by the European Council due to disagreements on connectivity protocols—mention this approach. Therefore, we argue that monetizing C-ITS safety-related use cases will entail alternative revenue sources, more specifically offering them bundled with other data-based services.

Consequently, another important aspect is access to in-vehicle and user data by third parties. C-ITS systems will collect, process and aggregate large amounts of real-time traffic data, but enabling alternative revenue sources from data-based services may also require the sharing of commercially-sensitive data beyond safety-related information, and this sharing would need to be done in a standardised and timely manner.

<sup>a</sup>  <https://orcid.org/0000-0003-4521-4064>

<sup>b</sup>  <https://orcid.org/0000-0003-3775-6592>

Moreover, as digital technologies and services converge with the automotive industry, supply chains are becoming more complex, requiring an overall business ecosystem perspective. This is especially the case in C-ITS, where multiple actors from different sectors are required to cooperate and/or compete with each other (C-ITS Platform, 2017; Lang et al., 2019). Delivering the added value of C-ITS will also require the fulfilment of several crucial roles and responsibilities, which in this paper we identify and allocate to specific stakeholders.

Main challenges to C-ITS adoption are thus clarifying the value network, incentivising investment in the necessary infrastructure, monetizing the provision of C-ITS safety-related services, and having a trustworthy, efficient, and timely data sharing system in place. Furthermore, another business requirement for certain stakeholders is the transfer of part of the liability in case of accidents. Successfully addressing these issues will determine whether a sustainable business ecosystem that enables a wide adoption of C-ITS emerges. In addition, it will determine whether the associated deployment costs will have to rely mostly (or even entirely) on public funding or, on the contrary, on private investment.

The aim of this paper is therefore to provide recommendations in order to help overcome the economic challenges identified above. In section 2, we map the overall value network for C-ITS services and the necessary interactions between the main stakeholders involved. In section 3, we suggest strategies that will enable sustainable business models for C-ITS. Finally, section 4 provides recommendations based on the entire analysis.

## 2 VALUE NETWORK ANALYSIS

In order to enable market uptake of C-ITS safety use cases, a main challenge is to clarify the system's underlying complex structure of roles and responsibilities, and understand how different players must cooperate and exchange resources in the market. To address this, in section 2.1 we discuss the roles that will need to be fulfilled. Subsequently, in section 2.2 we map the main required interactions in terms of financial and liability flows.

For simplicity, we focused on two types of illustrative safety C-ITS use cases for inter-urban roads and highways: first, Day 1 information services, such as 'road hazards warning' (RHW), which notify drivers of a safety-related traffic event; second, the more advanced 'cooperative emergency braking', where a vehicle automatically 'hits the brakes'

immediately after receiving a communication that another vehicle in front of it is performing a sudden break. In both cases, a vehicle or roadside unit (RSU) notices the road 'event' and communicates it to nearby vehicles via ITS-G5 or C-V2X protocols. Next, a receiving vehicle processes the message and either warns the driver via an HMI or performs the braking function.

### 2.1 Value Network Roles

Figure 1 identifies six different layers of roles involved in the overall C-ITS ecosystem. In grey, we highlight those roles for which the actor best poised to fulfil them remains unclear. Key roles remaining empty represents a bottleneck for C-ITS adoption; hence, our analysis in section 3 will discuss options and provide recommendations regarding these roles.

First, the 'Support' layer includes those roles that will make the use cases feasible both at the technical and the financial level. First, testing and certification will ensure the quality of the RSUs and vehicle on-board units (OBUs). Such homologation role might be performed by a public authority or an industry association like the OmniAir consortium. Second, operational management deals with controlling that maintenance happens and technical operations run smoothly. Third, the security and credentials role is based on the concept of Public Key Infrastructure (PKI), in which a cybersecurity services provider issues digital certificates that are used to encrypt telecommunications messages. Additionally, the financial coverage of liability by insurance companies in case of system underperformance and the financial support or 'sponsoring' of C-ITS system components will help create a positive business case for other actors.

Second, the 'Data' layer contains those roles revolving around the huge amounts of vehicle, user and traffic data that need to be gathered, processed and distributed. The data governance role aims at enforcing data ownership and sharing rules, including the definition of standardised formats. While regulators at the European and Member State level have set principles for the processing of personal and safety-related data, several questions remain, such as what data are made openly accessible and under what terms. A related, crucial aspect concerns which platforms will play the role of data aggregation and exchange, which may or may not be the same that gather and/or process data. We will discuss these aspects in section 3.3.

Third, the 'Communications' layer describes the necessary components to enable and provide short-

and long-range communications. We assume a future hybrid scenario in which both ITS-G5 and C-V2X protocols will co-exist for short-range messages, and interoperability will be legally required. We consider the sending of messages between vehicles and infrastructure (i.e., V2I/I2V) and between these elements themselves (V2V and I2I). The actors that will take up these roles are connectivity service providers, such as mobile (virtual) network operators (MNOs and MVNOs). In addition, the role ‘Cloud/MEC’ includes the provision of (edge) cloud computing infrastructure and solutions, and the ‘network function virtualisation (NFV)’ role includes dynamic network slice provision and management. This role and the remaining ones will be played by MNOs or network equipment and solutions vendors.

Fourth, the ‘Roadside’ layer covers the ‘smart’ or connected infrastructure that is deployed along the physical road infrastructure. At both roadside and vehicle levels, the role to provide precise positioning is played by an equipment manufacturer that provides Global Navigation Satellite System (GNSS) receivers, which are integrated into OBUs and RSUs.

Fifth, the ‘Vehicle’ layer covers the advanced on-board systems as well as traditional hardware elements. In particular, on-board units will be integrated in cars by vehicle manufacturers, who will likely acquire components from different suppliers and assemble them into their final products. Besides the mentioned positioning sensors, OBUs also contain processing units, antennas and SIM cards.

Finally, the ‘End-user services’ layer covers information services provided to end users (i.e. passengers or drivers of personal and freight vehicles) and the devices through which they are provided. The human-machine interface (HMI) through which the end user receives these services—e.g., visual or auditory warnings of road hazards ahead—can be added in the form of a personal device, such as a tablet or mobile phone, or be incorporated in the vehicle. These devices can be interoperable with the OBU by default and be connected to it ex post. Therefore, a service provider or the OEM can control this HMI role, depending on which element is used to present information to the user. Moreover, C-ITS and end-user service providers can be mobility or connectivity service providers, vehicle OEMs, or even public entities.

### 2.2 Value Network Interactions

Next, we investigate the necessary transactions amongst stakeholders that will collectively enable C-ITS use cases and their added value. We considered various types of interactions, namely financial, qualitative (i.e., meeting societal goals), liability and data flows. For simplicity, we only plot financial and liability flows. Since C-ITS-based liability shifts will likely only arise in the case of automated actions, the liability flows only apply to the (automated) coordinated emergency braking use case.

In the following lines, we summarise those

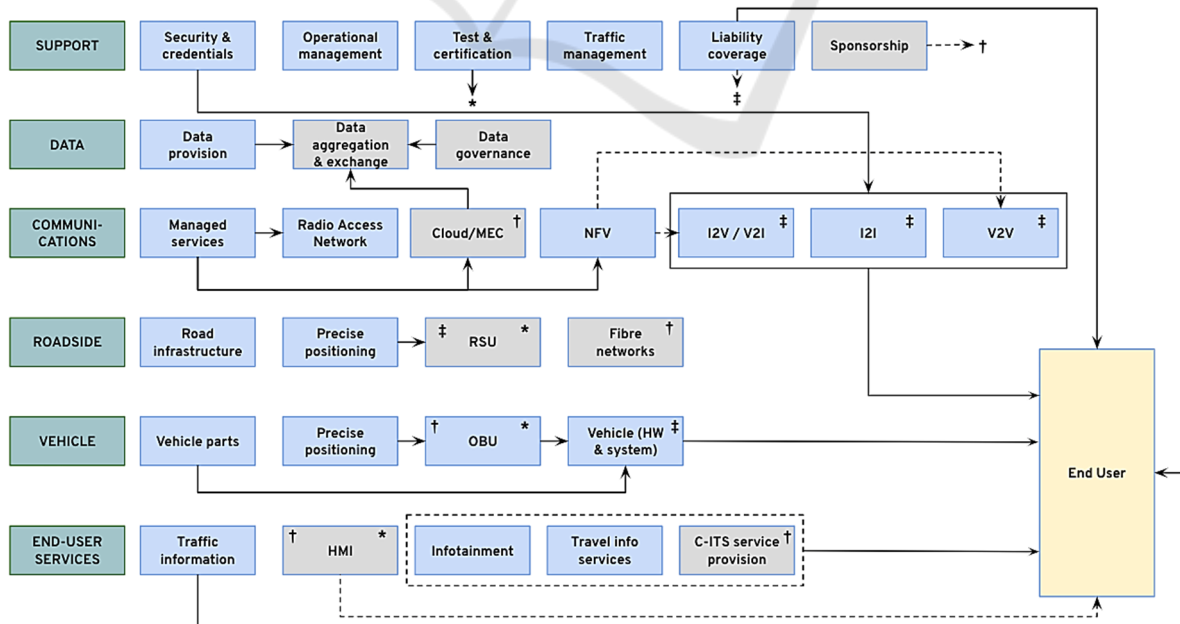


Figure 1: Revenue flows within the value network of safety-related C-ITS use cases.

economic transactions made in exchange for a financial compensation, although data and qualitative benefits may be present in parallel. We review the main ones and plot them in Figure 1. Dotted lines indicate the interaction is uncertain.

End users are the receiving entity for the following transactions (from top to bottom in the figure): (a) insurance policies with potentially lower premiums due to a lower risk of accidents; (b) a connectivity subscription, either coming with the vehicle or acquired separately from a connectivity service provider; (c) C-ITS-enabled vehicles in the form of a sale or lease; (d) an HMI device, acquired from a technology company or service provider, in case it is not incorporated in the vehicle (thus plotted as uncertain); (e) C-ITS information services, delivered by either a traffic management authority, a vehicle manufacturer or a (connectivity) service provider, possibly bundled with other data-based services in exchange for the purchase of or subscription to an app; and (f) traffic information.

IT security services providers issue digital certificates (security and credentials) for communications messages, based on the mentioned PKI. Furthermore, network solutions providers offer, besides managed services, cloud and virtualization infrastructure to connectivity service providers. Even though who will provide cloud services is unclear, data aggregation and exchange servers will be hosted at these edge or central clouds. Further, an MNO may issue a dedicated network slice for vehicle-to-everything (V2X) communications: in case vehicle manufacturers play the role of providing V2V connectivity, they would be the customers of this service, hence the dedicated possible transaction.

In the transactions represented by the symbol ‡, insurance companies receive financial compensation for the potential transfers of liability discussed later. It can also be that no financial compensation is included if the expected overall lower risk of accidents (thus lower costs) compensates the extra liability taken (premiums remaining equal). An alternative is that they re-invest these benefits to provide financial support to deploy different infrastructure and in-vehicle elements and services, i.e. playing the role of a sponsoring entity, which is represented by the symbol †, and which may be played by other entities as well. Likewise, tests and certifications of RSUs and OBUs, involving a fee in return, are represented by an asterisk in Figure 1.

Other interactions are not plotted because the financial benefit arises from the overall system, i.e., the safety use cases, being in place. Besides intangible societal gains, public authorities benefit

from reductions in expenses from lower accidents (e.g., from awareness campaigns and healthcare). Furthermore, the added value for road operators resides mainly in the replacement of physical infrastructure by digital messaging in order to bring information to road users.

Subsequently, Figure 2 presents the liability transfers that would arise in the case of automated functions, in which the driver would not take action (e.g., in the case of an emergency brake), and thus may not be held liable in case of accident. Interactions #1.1 and #1.3 imply a financial compensation in return for the liability transfer to another party. On the contrary, #1.2 flows entail no financial compensation, since they refer to the shift in liability in case there is an accident for which the vehicle manufacturer is not to blame because the failure or underperformance happened at the connectivity or the data processing level (except in the case where the OEM is responsible for V2V communication).

Connectivity or managed service providers will be subject to a higher risk in the future, as they may be held responsible in certain situations, such as when an accident happens due to a failure in connectivity. This might lead to standard contractual arrangements providing security to each party by identifying their liability in advance. Furthermore, it may also lead to higher costs due to a higher redundancy of the network, in order to increase reliability. Of course, it will be subject to future legal mandates as well.

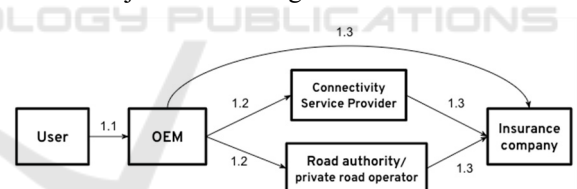


Figure 2: Liability shifts in case of automated braking.

### 3 MONETIZING C-ITS

The challenge of fulfilling certain roles arises from the uncertainty about earning a return on infrastructure investments and monetizing C-ITS service provision. This uncertainty is not only due to the costs associated with deployment and the lack of a standalone business case for safety services, but also about the risk of all the other required, enabling system elements not being concurrently in place. Therefore, the question of which actors will be able to take care of the necessary infrastructure and service deployment is of key importance. In turn, enabling the monetization of services requires having a time-

sensitive and sustainable data sharing system in place. Consequently, the present section provides a discussion on how to address these aspects.

### 3.1 Deployment of Key Components

For C-ITS to yield its expected safety benefits, several elements should be pervasively deployed, both in terms of geographic reach and vehicles covered. However, since a given actor's decision to invest is contingent on its expectations regarding the investment actions of authorities and competitors and the market penetration of C-ITS use cases, there exists a 'chicken-egg' conundrum: a lack of a clear business case disincentivizes investment, while insufficient investment makes the prospective business case financially infeasible. This would cause firms to take a reactive approach. In addition, the prospect of competitors taking advantage of interoperability obligations would disincentivise potential first-movers to bear the initial costs and risks. Similarly, if public authorities were to signal that they would take responsibility for all investments in case private companies do not, this would reinforce the passive approach of firms. All these scenarios would be detrimental, due to a resulting under-provision of C-ITS services or a delay in their introduction. In the sections below, we discuss strategies to incentivise the investment and deployment of specific, crucial system elements.

#### 3.1.1 On-board Units and HMIs

While the cost of an individual on-board unit may be low compared to the overall price of a car, OBUs and aftermarket devices represent most of the incremental investment required for C-ITS (C-ITS Platform, 2016).

We can expect European regulation to mandate that all new vehicles incorporate OBUs, as the current 'eCall' regulation does for SIM cards. However, customer willingness to pay for the extra costs, and thus the timely replacement of current vehicles, is a challenge. A traditional strategy is to partly subsidize vehicle sales, while a complementary option is for OEMs to monetize the extra costs of OBUs by selling vehicle-generated data to third parties.

Furthermore, aftermarket devices can be attached to current vehicles and used as HMIs to deliver C-ITS information services. They could be bought from service providers, and complementary services (location-based, infotainment, etc.) would be provided through them as well. Regulation would require that C-ITS safety information be given

priority over any other service provided via the same interface (as established by Delegated Regulation 886/2013 for non-safety-related traffic information), and these devices would need to be designed in a way that avoids distracting drivers. In addition, they would need to be certified to ensure reliability, since adding an extra data processing element would increase the risk of a message being communicated to drivers with delay. Since shifts of liability away from the driver are not expected for warning use cases (C-ITS Platform, 2016), homologation would limit such a risk by making sure HMI devices conform to minimum requirements.

In addition, by providing a direct contact with the end user, the role of the HMI will yield a valuable commercial relationship and knowledge of the customer. On the one hand, OEMs may be reluctant to let others gain access to in-vehicle data, and subsequently choose to install their own HMI in vehicles. On the other hand, third-party deployment of an HMI device would shift costs away from OEMs. Moreover, since the device has more applications outside the car, this cost would be easier for (connectivity or app) service providers to monetize.

#### 3.1.2 Telecommunications Infrastructure

Regarding roadside telecommunications infrastructure, the need for pervasive and timely deployment, together with the societal gains in safety and traffic efficiency, justifies public investment. In addition, early commitment by public authorities to deploy enabling infrastructure will be crucial to trigger industry investment in other elements and services, as it would lower uncertainty regarding other enabling system elements not being in place.

However, financing these investments through a kind of premium toll for C-ITS enabled vehicles runs the risks of disincentivizing user adoption. An alternative is that connectivity providers contribute to densely deploy RSUs. MNOs will be able to split the costs of radio access networks across many use cases, beyond automotive ones. Therefore, they will benefit from economies of scale by also using their infrastructure for (enabling) C-ITS use cases. However, given the recent experience of having had to write off the value of assets from previous generation networks, MNOs will be risk-averse when assessing these investment decisions. To counteract that, regulators may exceptionally allow active network sharing among different MNOs.

Moreover, the use of network slicing technology (i.e., the role of NFV), can further incentivise the deployment of telecommunications infrastructure by

MNOs. Network slicing would reduce capital expenditures by enabling multiple virtual network ‘slices’ to run on top of a shared physical infrastructure. These slices would be tailored to the distinct requirements of different use cases. For instance, C-ITS and content distribution for in-car entertainment differ in terms of their latency, reliability and bandwidth needs. Therefore, network slicing would allow to launch communications services in a more agile and cost-efficient manner (NGMN Alliance, 2015; Afolabi et al., 2018).

### 3.1.3 Multi-access Edge Computing

As C-ITS increases the need to aggregate and process real-time data, it will in turn increase QoS requirements in terms of ultra-low latencies, as well as big data analysis (Knieps, 2019). The reliance of C-ITS functions on time-sensitive data raises the question of where to locate data aggregation and processing functions within the network, and thus about the relative use of centralized cloud architectures versus multi-access edge computing (MEC) nodes (Satyanarayanan, 2017).

MEC provides cloud computing capabilities at the edge of the network, which can be located within the radio access network next to base stations, thus closer to users and road infrastructure, thereby lowering latency (Hu et al., 2015; Beck et al., 2014).

While a centralized cloud architecture can cost-efficiently provide computation and storage at scale, distributed computing architectures are more expensive in comparison, since multiple data centres need to be deployed (Chang et al., 2014). On the other hand, edge cloud computing allows to perform tasks such as storing and processing content on local datasets at the edge of the network; by doing so, MEC servers provide an increased QoS and can enhance privacy (Satyanarayanan, 2017; Beck et al., 2014).

However, some open questions remain, for example regarding who will set up, own and manage the infrastructure of MEC nodes. MNOs could deploy both private or public edge cloud servers within their own networks, possibly contracting network equipment and solutions vendors for maintenance and operation of the cloud hosting environment. Alternatively, more open ownership approaches exist, such as the one described by Ai, Peng & Zhang (2018)—consisting of an open RAN where MNOs host third-party applications and content at the MEC level—or the one described in Satyanarayanan (2017), which is based on an open-source platform. Both authors argue that these open models would incentivise investment and the quick and competitive

deployment of innovative solutions.

## 3.2 Bundling of Services

The lack of a stand-alone business case for C-ITS safety services is a bottleneck for private provision. For service providers, MNOs, or OEMs, these C-ITS services will likely be valorised only when bundled with other services or solutions across their portfolio. Therefore, delivering safety C-ITS services in combination with complementary services—i.e., those also based on digital interfaces, mobility data and connectivity—incentivises investment from private firms. Examples of such services include navigation, travel planning, truck tolling, mobile connectivity, infotainment, etc. Real-life examples of this business model already exist, such as the mobility apps of Be-Mobile.

Furthermore, if service providers adopt the C-ITS service provision role they will alleviate the need of traffic authorities to do complex data processing, as the service provider will integrate real-time traffic data collected by roadside infrastructure. Moreover, from the perspective of users, bundling enhances the value of C-ITS services in front of a potential stand-alone delivery, thereby increasing user willingness to pay to deploy external HMIs in cars.

An alternative monetization strategy is sponsorship. A sponsor is a third-party stakeholder that has an indirect monetary interest in the adoption of C-ITS, and is therefore willing to provide financing for the C-ITS service. Insurance companies could fulfil this role, since an increase in road safety would lower their expected future costs from claims.

Next, one aspect to specifically consider is the communications service. While traffic messages are to be delivered for free at the end user’s point of use, this does not imply they are not priced somewhere else, for example within a connectivity subscription.

The subscription to the connectivity service could be incorporated and priced in the vehicle. In that case, the OEM would pay the connectivity service provider (CSP). On the contrary, the subscription could be purchased independently by each individual user. Only in the second case the user would directly choose the CSP or even be aware of it. However, that scenario would add the risk that the user is not willing to pay for the connectivity subscription. As a result, public authorities may prefer making the connectivity service provision mandatory for either the vehicle manufacturer or the user; and comparatively, the first option would limit the risk of non-compliance. If connectivity subscriptions were mandatory, ceiling prices or rules to limit price-fixing by CSPs could be used to compensate for the increased bargaining power given to them. In case customers must buy the

subscription, M(V)NOs would be able to maintain customer ownership, and could bundle the C-ITS connectivity provision with subscriptions for handsets and other services (e.g., audio-visual content provided through the external HMI).

If MNOs deploy MEC architectures they could also bundle connectivity services with MEC services, for instance offering them to data exchange platforms (discussed in the next section), likely via intermediary cloud hosting providers. Therefore, MNOs can find multiple revenue sources from C-ITS services by providing connectivity (including network slices), complementary services, and MEC hosting.

Furthermore, since these complementary services strongly rely on real-time traffic, vehicle and user data, service providers will need constant access to it. Therefore, the question of what data are open and accessible and what remain under control of private parties becomes relevant. To address this issue, the following section discusses the unclear value network roles of data aggregation, exchange and governance.

### 3.3 Data Exchange and Governance

Both to address the challenges of monetizing C-ITS and encouraging coordination, a main aspect is data sharing. To evaluate options regarding the governance and exchange of data, we first analysed existing and proposed regulations. Next, we reviewed extant literature about data platforms for traffic-related use cases. In addition, we organised an internal consultation with a subset of nine of our project partners, including central C-ITS stakeholders such as telecommunications, automotive and research organizations. While not representative, it provided valuable insights about their views and preferences with regard to data sharing and governance options.

Regarding mandatory data sharing, legal ground is found under the ITS Directive 2010/40/EU and the delegated regulations that supplement it. These supplementing regulations—DR 2017/1926, DR 885/2013, DR 2015/962, and DR 886/2013—have a different scope in terms of the data types covered, but overall it can be concluded that: (i) Member States are to set up National Access Points (NAPs), where (ii) at least the most ‘fundamental’ safety-related data shall be accessible for exchange and reuse; moreover, that (iii) such access must be provided under fair, standardised and non-discriminatory terms; (iv) that such data sharing must be timely and meet quality requirements; and finally, (iv) that the role of assessing compliance with these rules falls under an independent national (or supranational) body. In addition, recent documents (European Parliament, 2018; European Commission, 2019) confirm this approach.

However, while we can assume that prospective regulation will mandate the sharing of safety-related data, the question still remains on how much data (if any), and in what terms, is made accessible with regard to other, less ‘fundamental’ data types.

In order to develop a profitable business model, it may also be necessary to allow the access and reuse of data by third parties beyond the ‘fundamental’ safety types, for example to enhance predictive maintenance, travel advice or insurance services. The surveyed project partners agreed with the basic premise that offering profitable C-ITS services will require the sharing of in-vehicle proprietary data among different stakeholders, although the specific data types would depend on each service. However, as also identified elsewhere (e.g., see C-ITS Platform, 2016; Vantomme, 2018), a business requirement by OEMs is to receive a fair return for sharing the in-vehicle data they own. This is also in line with our previous point about the sale of data being an alternative revenue source for OEMs to monetize their investments in OBUs.

We distinguish between three different types of relevant data, namely traffic, in-vehicle (e.g., location, speed) and user data (e.g., driving behaviour). In-vehicle and user data are gathered by OBUs and HMI devices, subsequently sent to proprietary servers, and shared on the basis of bilateral market agreements subject to market pricing. Moreover, while Belgian NAPs offer open access to aggregated traffic data, they consist of rather static databases, plus they do not include all the above data types. Therefore, we expect the relevant sharing that enables complementary services to be done through other, alternative data platforms.

Data platforms are access points, or digital interfaces, where data are made available to third parties. The C-ITS Platform (2016; 2017) project identified several types of relevant data platforms for C-ITS, differing in terms of location and ownership. Regarding location, they can be distinguished based on whether they are external to the vehicle (i.e. off-board) or in-vehicle (i.e. on-board). Regarding ownership, the platforms may be proprietary to the party who gathers data, or alternatively be owned and operated by a neutral entity, such as a public entity, a public-private partnership or a private entity controlled by a consortium of C-ITS stakeholders.

Common concerns about on-board platforms relative to off-board ones involve their being more expensive to develop and requiring more time to be implemented, while relative concerns about off-board platforms include their ability to support all real-time use cases (C-ITS Platform, 2016; McCarthy et al.,

2017). Similarly, proprietary platforms triggered concerns of impaired competition and innovation in terms of services, while OEMs argue that proprietary solutions could offer reduced time to market (C-ITS Platform, 2016; McCarthy et al., 2017). In any case, it is estimated that providing access to in-vehicle data would bring higher socio-economic benefits from the enabling of added services than the costs of implementing any of these data platform architectures (McCarthy et al., 2017).

Most of the consulted project partners expressed a preference for the data governance role being done by a third party, and among these the average feeling was of being “somewhat more comfortable” with that party being a public entity. Nevertheless, in spite of a slight majority also preferring the data exchange being done through a public agency’s platform, there was no consensus in this regard.

In conclusion, based on our understanding of the value network, monetization challenges, the relevant regulations and data platform types, and our project partners’ preferences, we argue in favour of a specific data platform and data sharing arrangement, which would provide clarity to the unclear, bottleneck value network roles of ‘data aggregation and exchange’ and ‘data governance’.

We argue that the closest fit—in the context of the CONCORDA project—would be a neutral marketplace platform. This server would aggregate vehicle, traffic, and travel-related user data from multiple proprietary servers and offer a standardised interface for third parties (such as connectivity and information service providers, OEMs and public authorities) to access the data and gather it for reuse in their own servers and the NAPs of different countries. It would be owned by a consortium of public and/or private C-ITS stakeholders, thereby being neutral to any specific entity, and it would be operated independently. In addition, it would be located off-board of vehicles, but close to them at the edge of the telecommunications network, i.e., in MEC servers. As mentioned before, this would address the issues of latency of C-ITS messages and of privacy of personal data. Privacy is another issue to take into account, since based on the General Data Protection Regulation 2016/679 (GDPR), C-ITS messages contain personal data, hence its processing for commercial exploitation requires the consent of the data subject (FIA, 2017; Art 29 DP WP, 2017).

Data subject to commercial interest would be subject to market pricing and exchanged for a fee, with defined access price ceilings. Compared to ad hoc bilateral agreements, by giving access to a broader pool of potential service providers, we argue

such a sharing arrangement would increase efficiency, competition and service innovation. Furthermore, this platform could finance its operational costs through transaction fees, possibly complemented by public subsidies and private sponsorship as well.

This arrangement would have to be complemented by rules that mandate open sharing of more than safety-fundamental traffic and in-vehicle data based on fair and non-discriminatory terms, and would be subject to user consent. The consulted project partners differed in their views regarding how to enforce such sharing. While their answers indicate clear support for certain explicit rules around data sharing, the preferred extent of regulation depends on the objective of such rules. Most answered that rules should be established to ensure data are shared in a standardised manner; however, establishing rules to ensure data are made available unaggregated or with a minimum quality was not a majority opinion.

## 4 CONCLUSIONS

C-ITS safety-related use cases are expected to bring high societal value by contributing to reduce road accidents. However, creating this value relies on a series of investments in infrastructure and in-vehicle equipment, which in turn will depend on the ability of private actors to monetize them. We argue that the following aspects make this monetization challenging: (i) the lack of stakeholder involvement and coordination within the overall ecosystem, (ii) the costs of deploying equipment and infrastructure, (iii) the lack of a standalone business case for C-ITS safety service delivery, and (iv) the issue of data exchange and governance models. Therefore, to help enable the creation of value from C-ITS safety services and overcome this investment problem, we provide several suggestions.

First, stakeholder coordination and involvement must be encouraged. Coordination is an increased challenge in an ever-expanding mobility ecosystem with complex value networks. In this paper, we plot the overall C-ITS value network, its bottleneck roles that will have to be fulfilled, and its interactions in terms of financial and liability flows. Such involvement depends on each role’s specific business requirements (in the form of the discussed interactions and monetization strategies) being covered. For policymakers, encouraging involvement and coordination means the use of regulatory actions to guide deployment and competition (e.g.,



mandating on-board units in vehicles and the sharing of certain data).

Second, coordinating the timing of initial investments is key to overcome the ‘chicken and egg’ problem of investing in the infrastructure and equipment necessary to set up the system. We argue that public entities should lead initial investments in roadside infrastructure to signal their commitment in subsequent deployments and, in turn, acquire credible commitments by more risk-averse actors.

Third, we discuss the challenge of monetizing on-board units, telecommunications infrastructure and (edge) cloud deployments, and provide some strategic options available to different actors. For instance, regulation may allow connectivity service providers to maintain direct access to end customers instead of mandating that a connectivity subscription be included in the vehicle. Moreover, enabling to monetize C-ITS safety services will be contingent on enhancing value propositions through bundling complementary services, which can incentivise the uptake of the key service provision role. Bundling allows to cross-subsidise across a firm’s service portfolio, and leverage economies of scope. Importantly, enabling these complementary services will require the sharing of data.

Last, to encourage the rich sharing of data, we argue in favour of a data marketplace platform owned by a neutral entity—for instance a public or consortium entity—as the best fitting option for the Belgian context. To capture value from C-ITS safety use cases, vehicle and traffic data with commercial interest will need to be shared among multiple actors in real-time. In this marketplace, such data would be timely exchanged and traded in a standardised manner. Complementarily, national access points would contribute to the bottleneck data aggregation and exchange role for less time- and commercially-sensitive datasets, sharing them in a more open manner. In addition, regulation would ensure access to these data and sharing, thus contributing to the ‘data governance’ value network role.

Finally, further research is needed in order to provide more comprehensive guidance. Several aspects can be addressed, such as which specific data types are covered by the proposed sharing arrangements, and what specific regulation in terms of access pricing would be optimal. In addition, further research could also extend the present work to other C-ITS use cases.

## REFERENCES

Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A. & Flinck,

- H. (2018). Network slicing & softwarization: A survey on principles, enabling technologies & solutions. *IEEE Communications Surveys & Tutorials*, 20(3), 2429-2453.
- Ai, Y., Peng, M., & Zhang, K. (2018). Edge computing technologies for Internet of Things: A primer. *Digital Communications and Networks*, 4(2), 77-86.
- Article 29 Data Protection Working Party (2017). Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
- Beck, M. T., Werner, M., Feld, S., & Schimper, S. (2014). Mobile edge computing: A taxonomy. In *Proc. of the Sixth International Conference on Advances in Future Internet*, 48-55.
- Chang, H., Hari, A., Mukherjee, S., & Lakshman, T. V. (2014). Bringing the cloud to the edge. In *2014 IEEE Conf. on Computer Communications Workshops*, 346-351.
- C-ITS Platform (2016). Final report. Retrieved from [https://ec.europa.eu/transport/themes/its/c-its\\_en](https://ec.europa.eu/transport/themes/its/c-its_en).
- C-ITS Platform (2017). Final report Phase II. Retrieved from [https://ec.europa.eu/transport/themes/its/c-its\\_en](https://ec.europa.eu/transport/themes/its/c-its_en).
- European Commission (2016). A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. Brussels: COM(2016) 766 final.
- European Commission (2019). Commission Delegated Regulation (EU) .../... of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. Brussels: C(2019) 1789 final.
- European Parliament (2018). Report on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)). Committee on Transport and Tourism.
- FIA (2017). What EU legislation says about car data: Legal Memorandum on connected vehicles and data.
- Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile edge computing—A key technology towards 5G. *ETSI white paper*, 11, 1-16.
- Knieps, G. (2019). Internet of Things, big data and the economics of networked vehicles. *Telecommunications Policy*, 43(2), 171-181.
- Lang, N., von Szczepanski, K., & Wurzer, C. (2019). The Emerging Art of Ecosystem Management. Boston Consulting Group.
- McCarthy, M., Seidl, M., Mohan, S., Hopkin, J., Stevens, A., & Ognissanto, F. (2017). Access to in-vehicle data and resources: Final report. European Commission.
- NGMN Alliance (2015). 5G White Paper. A Deliverable by the NGMN Alliance, version 1.0.
- Sabella, D., Vaillant, A., Kuure, P., Rauschenbach, U., & Giust, F. (2016). Mobile-edge computing architecture: The role of MEC in the Internet of Things. *IEEE Consumer Electronics Magazine*, 5(4), 84-91.
- Satyanarayanan, M. (2017). The emergence of edge computing. *Computer*, 50(1), 30-39.
- Vantomme, J. (2018). Data sharing and re-use: Perspective from the vehicle manufacturers. ACEA BITS – Brussels Internet & Telecom Seminars.