2012-09

Towards an automatic enforcement for speeding: enhanced model and ITS realization

Fuentes, José María de

Institution of Engineering and Technology (IET)

IET Intelligent Transport Systems, Sept. 2012, vol. 6, issue 3, pp. 270-281
http://hdl.handle.net/10016/14412

Towards an automatic enforcement for speeding: enhanced model and intelligent transportation systems realisation

J.M. de Fuentes A.I. González-Tablas J.L. Hernández-Ardieta A. Ribagorda

Computer Science Department, University Carlos III of Madrid Av. Universidad, 30, Leganes 28911, Spain
E-mail: jfuentes@inf.uc3m.es

Abstract: An adequate enforcement process is essential to make road traffic fines effective. Automatising such process is intended to provide such effectiveness. However, current enforcement practices do not achieve this goal, as they usually have weaknesses regarding the reliable identification of the offender, the immediacy of feedback after the violation and the completeness of offence description. Intelligent Transportation Systems (ITSs) technologies may be introduced to contribute to these issues. To enable such integration, a complete model of this process must be built. Based on the VERA2 model and the Spanish traffic legislation, in this work an enhanced model is proposed that identifies the stakeholders, the process entities, the data at stake and their interchanges. Its suitability to represent current enforcement systems (particularly the Spanish ESTRADA and the French CSA) is evaluated. Furthermore, based on this model, the integration of the ITS-related technologies is analysed, as well as their suitability compared with current approaches.

1 Introduction

Legislation determines which actions are allowed within a jurisdiction and those that should be punished. In order to ensure fairness, specific enforcement processes have been established in each country. Such a process starts when an illegal action is observed and lasts until the punishment is established. Its realisation must preserve its efficacy, trying to avoid the repetition of such a behaviour. This factor is critical in road traffic enforcement processes, as offences may put road safety at risk.

The European Commission has pointed out the need for offences 'to be notified and sanctions to be executed within a short time period' [1]. In this regard, European research projects such as Enhanced Safety Coming from Appropriate Police Enforcement (ESCAPE) have highlighted the benefits of automatising this process [2]. Different attempts in this direction have been recently made by European countries. For example, the French Contrôle et Sanction Automatisée (CSA) [3] and the Spanish EStación de TRAmitación de Denuncias Automatizada (ESTRADA) systems automatically register the offence and prepare the fine notification [4]. In a complementary approach, the Video Enforcement for Road Authorities (VERA) series of projects focused on cross-border enforcement, that is, to ensure that an offence committed by a foreign driver is punished in the country of residence. As a part of its results, VERA2 has proposed an enforcement process model consisting of a set of flowcharts and a data dictionary [5].

Despite the expected benefits of automated processes, current enforcement practices have three main weaknesses. First, a reliable identification of both driver and vehicle has not been satisfactorily achieved so far [2]. Second, an immediate feedback of the fine is not provided when the offence is detected by automated devices like radars [2]. Third, the offence description usually relies on a single data source (e.g. radar, policemen), which does not ensure that the offence is fully described [6]. At the same time, the driver does not have a similar data source to defend himself from the accusation, leading to an unfair situation.

Our approach. Intelligent transportation systems (ITSs) technologies may be integrated in the enforcement process to contribute towards solving the identified problems. Prior to that integration, it is necessary to have a complete model of the process. The VERA2 flowchart constitutes a basic model, as it details 'what' has to be done. However, it does not specify 'how' to perform each step nor the involved data. On the other hand, although the same project has proposed a data dictionary, it is focused on cross-border enforcement (e.g. the enforcement of punishment on foreign offenders) [5]. It covers the data elements that may be sent between countries for delegating the enforcement. Thus, it does not contain all the elements produced in each process phase that is addressed in a single country. In this situation, the VERA2 model is not enough to clarify how to integrate the ITS techniques in this process.

Our contribution. The contribution of this paper is two-fold. First, several enhancements of the VERA2 model are proposed. In particular, based on the results of the mentioned project and on Spanish legislation, the stakeholders of this process, its participant entities, the data at stake and the data exchanges are identified. The suitability of such an enhanced

model to represent current systems (particularly, ESTRADA and CSA) is discussed. Second, based on this model, the integration of the ITS-related technologies is analysed, as well as their suitability compared with current approaches.

Scope. The focus of this work is on speeding enforcement, as it is the offence that has the worst effect on the road injury problem [7]. Moreover, as most European countries apply civil or administrative sanctions for light traffic offences, and given that speeding is usually considered as such unless the speed difference is remarkable, this enforcement variant is the one modelled in this work [8].

The paper is organised as follows. Section 2 gives the background on the VERA2 speeding enforcement model, current enforcement systems and the ITS technologies. Section 3 describes the proposed enhanced model based on VERA2. Section 4 evaluates the suitability of the model to represent current systems. Based on the model, the integration of the ITS technologies in this context is analysed in Section 5. Section 6 describes the related work. Finally, Section 7 shows the main lessons learned and future work.

2 Background

This section introduces the current model built in the VERA2 project (Section 2.1), the Spanish and French enforcement systems and their problems (Section 2.2) and the relevant ITS-related technologies (Section 2.3).

2.1 VERA2 speeding enforcement model

The enforcement process starts when an illegal action is detected and finishes when punishment is established. In between, several steps take place (see Fig. 1). Countries like Spain group them into four phases – starting, preliminary investigation, resolution and appealing. Such a division will be employed to describe the process.

1. *Starting:* The enforcement process starts with the detection of the illegal action. Supporting evidence is collected and sent to the concerned authorities for evaluation. If the authorities consider the action as an offence, a fine notification is issued and sent to the vehicle owner. To retrieve the owner information, the vehicle number plate is analysed. In case it is a foreign vehicle, its corresponding national database or EUCARIS (European car and driving licence information system [https://www.eucaris.net/, accessed January 2012]) is contacted.
2. *Preliminary investigation:* There are two actions that may be performed by the offender in this phase. First, the owner can nominate another person as the offending driver. Then, the notification is sent to this person. It must be noted that these notifications may be ignored by its receiver and, in some cases, re-sending them is allowed. In case that the notification is finally not ignored, the second action is to contest the fine. As a result, if the fine is cancelled, this decision is sent to the offender.

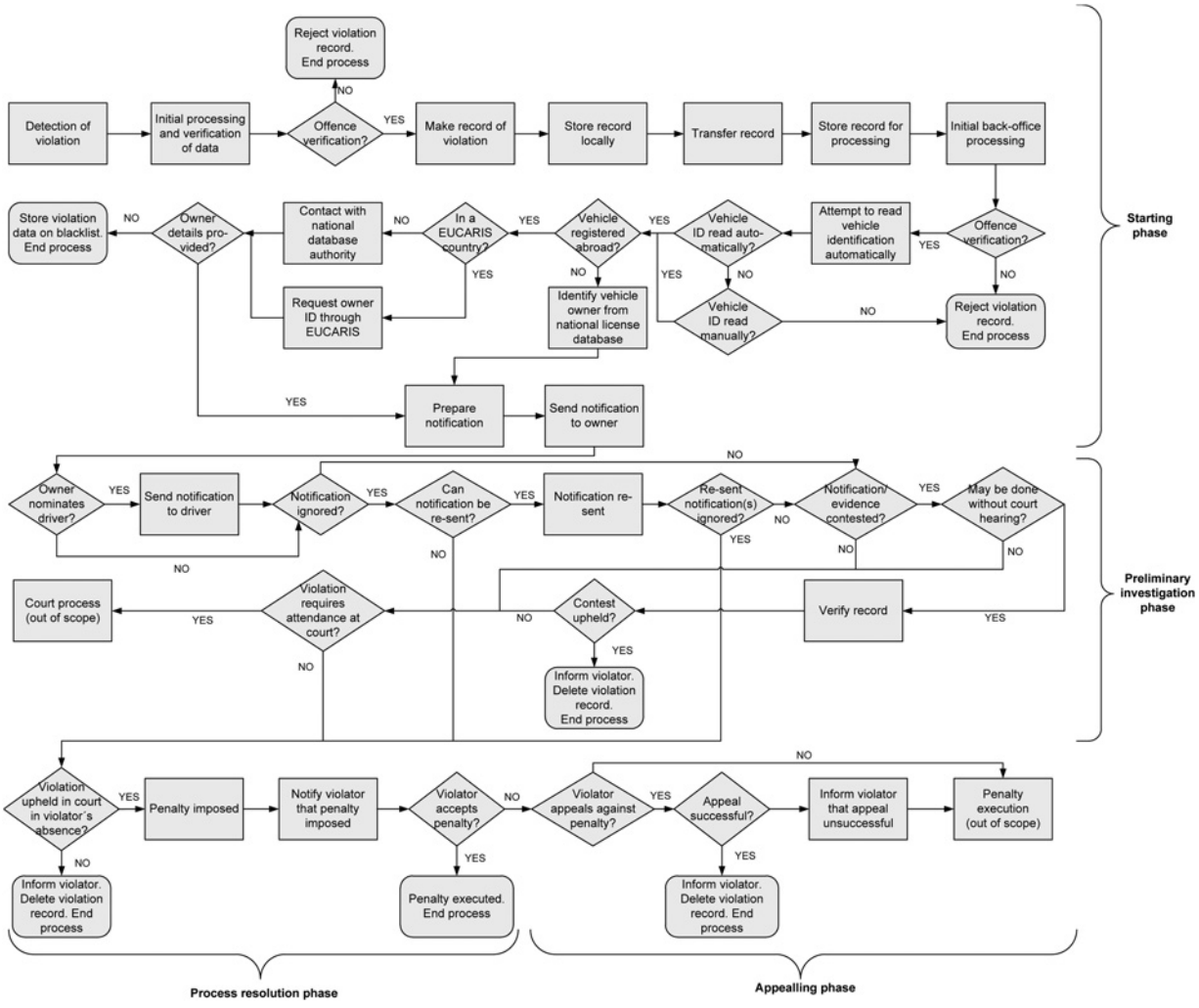

Fig. 1 *VERA2 process model, based on the material provided at [5]. Usual process phases have been marked*

3. *Resolution:* If the previous phase has not cancelled the fine, an independent revision of the whole process is conducted. It verifies whether the process development respects of the law and thus if the offence is upheld. In any case, the revision result is notified to the offender.
4. *Appealing*: After receiving such a notification, if the penalty is imposed the offender may accept or appeal against it. In the latter case, the offender creates a document expressing the reasons to proceed, and sends it to the authorities for evaluation. The result of this process is notified to the sender. In case the appeal has not removed the fine, the penalty is executed.

2.2 Overview of current enforcement systems. Case studies: Spanish ESTRADA and French CSA

Most enforcement systems in developed countries have automatised some of their steps. However, such automated devices are usually only employed in the Starting phase. Systems like ESTRADA [4] or CSA [3] are good representatives of this enforcement trend. Both are composed of fixed and mobile speed cameras connected to a central processing office. Here, the number plate is extracted from the pictures, and the vehicle holder is identified by retrieving this information from the official register. The fine notification is prepared to be sent by post to the vehicle holder. All these steps are performed automatically.

Beyond this point, there are some slight differences between both systems. In the Spanish case, a recent revision of the traffic law has allowed sending this notification by electronic mail [9]. The notification receiver may also receive a short text message in her mobile phone indicating that such a notification has been sent. The French case does not provide this option. Moreover, the French system requires the vehicle holder to pay the fine before identifying the real driver in the Preliminary investigation phase [10].

According to [2, 6], current automated systems face three main problems:

1. *Lack of reliable and immediate offender identification:* Automated devices such as cameras have to protect the drivers' privacy. Thus, graphic evidences (i.e. pictures or videos) usually only show the vehicle's rear [11]. This method has three drawbacks. First, the offending vehicle might be erroneously identified, as the effectiveness of current automatic number plate recognition (ANPR) systems is not complete, but around 90% [12]. This rate may be even lower for foreign offenders owing to singularities on their number plates. Second, the process is delayed as the owner has to perform the mentioned identification. For example, Spanish legislation provides up to 15 days for this purpose, added to the time to deliver the notification. Third, it can lead to identification fraud. This is especially relevant in countries where sanctions have an effect on the driving licence (i.e. demerit points, licence withdrawal).
2. *Notification delays:* Notifications introduce a delay in the process composed of three factors: the time to prepare the notification ($t_{\text{prepare-notif}}$), to send it ($t_{\text{send-notif}}$) and to access to it by the receiver ($t_{\text{access-notif}}$). Recent estimations in Spain showed that such delay was 45 days for postal notification and 12 days for electronic notification [13]. Manual notifications are usually performed in a few minutes, as they only require filling up a form. Even if such notifications are the most immediate ones, they may only be applied to a short proportion of offences owing to the limitation of human resources. Therefore for most offences its notification arrives after several days, which decreases its educational purpose [2].
3. *Unfairness: incomplete offence description and lack of witnesses:* Nowadays, automated surveillance devices (such as cameras) or even police agents are the main data sources employed to describe the offence. They observe the situation from a single point outside the vehicle. However, sensorial errors (for devices) as well as perception limitations or even psychological factors (for persons) may offer inaccurate offence descriptions, thus leading to unfair punishment. This situation may not be encountered by drivers, as usually there are no witnesses to support their claims [6].

2.3 Overview of the ITS technologies

In an ITS context, vehicles can connect with each other and also with a set of ITS service providers (see Fig. 2). To perform such a connection, they are equipped with a transponder called on-board unit (OBU). Such a device may establish connections under different technologies, such as vehicular ad-hoc networks (VANETs), satellite connections and so on. Thanks to such connectivity, vehicles share some data, such as their perceptions and driving status. To prepare these messages and process the incoming ones, a computational device is employed. Such a device also processes the data coming from in-vehicle sensors (GPS, motion sensor etc.) that register the vehicle's own status and its surroundings [14]. To protect these messages, a cryptographic module hardware security module (HSM) is employed. The HSM also securely manages the electronic vehicle identifier (EVI), a credential that enables the electronic identification of the vehicle. To avoid a vehicle from being tracked, other identification alternatives (such as short-lived credentials) have been proposed [15]. The driver may also be electronically identified through a driver credentials reader, which may use the electronic identity card or even the electronic driving license according to ISO 18013 [16]. To interact with the aforementioned devices, vehicles have a human-machine interface.

3 Enhanced road traffic administrative enforcement model for speeding offences

Based on the VERA2 model introduced in Section 2, several enhancements to this model related to the identification of enforcement entities, stakeholders, data structures and interchanges are proposed herein. In order to derive them, the system that realises the enforcement process is considered. Section 3.1 presents the methodology employed to derive the enhancements. Section 3.2 describes the refinements made in the VERA2 process model. Section 3.3 introduces the stakeholders that interact with the system to establish the appropriate fine. The legislation establishes several data structures to be present at each part of the process. Section 3.4 presents such data structures, which will be managed by the enforcement entities (Section 3.5). The main data interchanges that happen during the process are depicted in Fig. 3, whereas Appendix 1 specifies all of them in detail.

3.1 Methodology

In order to identify the proposed enhancements, two sources of information have been analysed: the VERA2 flowchart [5] and the Spanish traffic law [9]. As a result, some refinements of the VERA2 flowchart have been introduced. Afterwards,

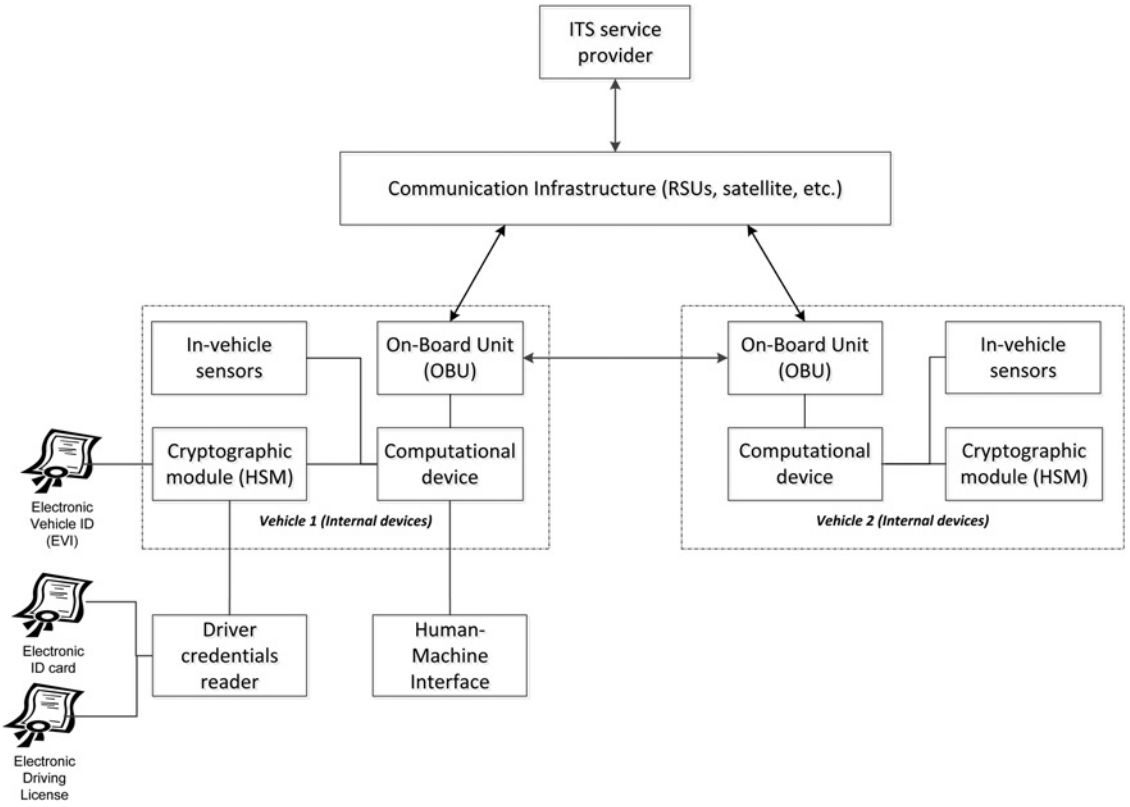

Fig. 2 *Main components of an ITS scenario*

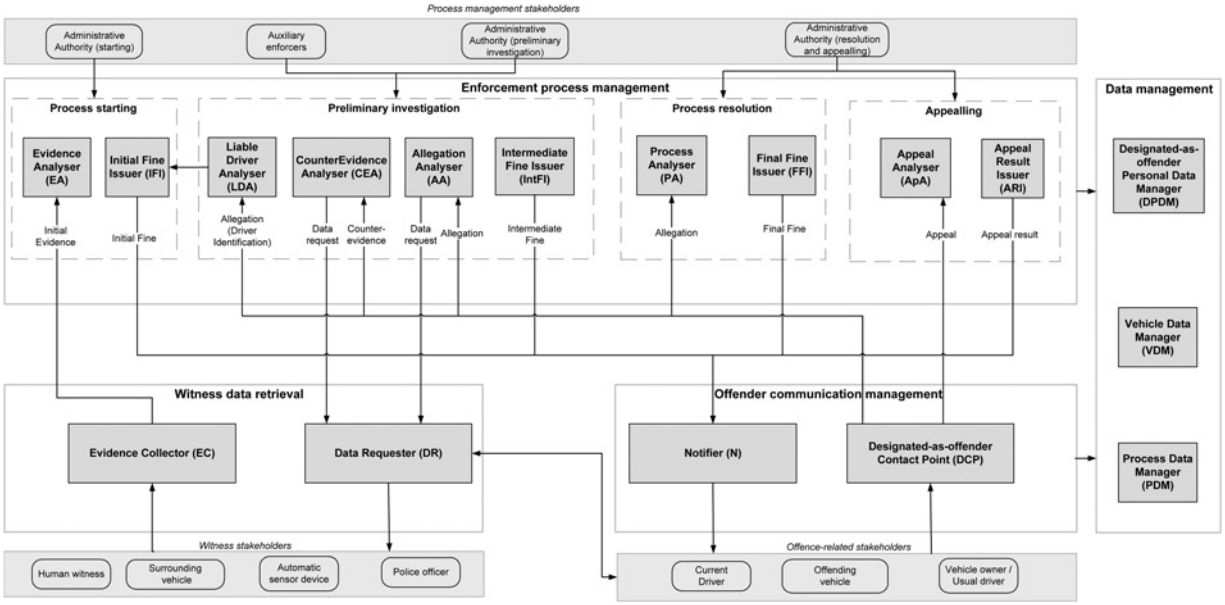

Fig. 3 *Proposed enforcement system model*

the flowchart steps have been grouped whenever they form a conceptual set of operations that may be addressed by an enforcement entity. Each of these groups (and thus, enforcement entities) has been given a name, leading to an initial set of entities.

The flowchart does not detail the stakeholders that participate in each step in the process. For this purpose, Spanish traffic law has been analysed to extract this information. These stakeholders have enabled a classification of the aforementioned enforcement entities based on the relationship between such entities and the stakeholders (see Fig. 3).

Finally, the legislation has also been analysed to determine the data at stake in each enforcement entity, along with their data interchanges. A new block of enforcement entities was identified to store these data.

3.2 Refinements of the VERA2 process model

Four refinements are performed on the VERA2 process model. The first one aims to extend this process to enforcement actions performed by police patrols. Thus, the person identified as the offender (called Designated-as-offender

role, from now on) in the Starting phase may not only be the owner, but also the driver. Related to this point, the second refinement is that the legislation enables the owner to nominate another person as the usual driver. Therefore the nominated person will receive the fine notification at first, instead of the owner.

The third refinement is to specify the ways to contest the fine in the Preliminary investigation. Thus, there may be allegations and counterevidences. Allegations enable us to take another view of the offence context, trying to decrease its severity. For example, medical emergencies may be considered as an alleviating factor for speeding. Regarding counterevidence, it is a piece of verifiable data describing the facts. As an example, a counterevidence could show that the vehicle speedometer did not reach illegal speed. It may be built by the authorities after a proposal from the offender or by its own initiative. For example, it may consist of checking whether the radar was properly calibrated.

The fourth refinement is related to the notification of the Intermediate fine. Such notification happens only once the fine has been contested and this action has not been upheld because of data or facts unknown to the offender. Moreover, only in this case the offender is in a position of defence by sending new allegations at the beginning of the Resolution phase.

3.3 Stakeholders

There are three groups of stakeholders in this process. The first one contains the participants related to process management (Fig. 3, upper part). These are the administrative authorities and the auxiliary law enforcers that support their work.

The second group (Fig. 3, lower left corner) contains the participants that have been witnesses to the offence, but are not the offender. According to Spanish law, three types of witnesses may report an offence – persons, automated sensor devices or police officers [9]. Moreover, technically enabled vehicles could also become electronic witnesses.

The third group (Fig. 3, lower right corner) is composed of the entities directly related to the offence. Apart from the offending vehicle, it may be any entity that has the Designated-as-offender role (recall Section 3.2).

3.4 Data at stake

In this section the data structures involved in this process are described (see Table 1), detailing their composing data elements based on Spanish legislation [9]. For the sake of uniformity, the catalogue of information elements provided by the VERA2 dictionary is used whenever possible [5]. In Table 1, the element identifiers from that dictionary are marked in parenthesis (where *n/a* indicates that this data item is not in the dictionary).

In the Starting phase, two structures exist – the initial evidence and the initial fine. The 'initial evidence' is the first description of the violation, whereas the 'initial fine' is the first evaluation of the aforementioned violation conducted by the authorities.

There are three data structures in the Preliminary investigation, namely the 'allegation', the 'counterevidence' and the 'intermediate fine'. The allegation contains the alleged element and the motivation. A very similar structure is used by counterevidence, where only the allegation content is substituted by the evidence data. In this case, it may contain a testimony, a graphical proof (i.e. picture or video) or any probatory element. Regarding the intermediate fine, it is a revision of the initial fine based on the previous data elements. Thus, it is formed by the assessment of the counterevidence and allegations at stake and the revised fine amount.

In the Process resolution, apart from the aforementioned allegations, only the 'final fine' is managed. The main difference between this structure and the previous one is that it establishes the definitive fine, showing its motivation. It also details the legal basis for posterior appeals by the offender.

Finally, the Appealing phase manages the 'appeal' and its 'result'. Although the appeal has a different legal status, its contents are the same as the allegations phase, except for the vehicle data. On the other hand, the appeal result mainly describes the appeal assessment by the authorities and the remaining legal actions that may be taken by the offender.

3.5 Enforcement entities

The entities that compose the enforcement system are organised in four blocks, namely Witness data retrieval, Offender communication management, Data management and Enforcement process management. Given below is a description of each block:

1. *Witness data retrieval:* This block gathers the two entities (Evidence collector and Data requester) who communicate with the witness stakeholders. The evidence collector gathers the initial evidence, delivers it to the appropriate entity in the Process management group, and registers it within the Data management block. The data requester retrieves additional information from the stakeholders. It may be required by the authorities to contrast a given allegation or counterevidence. It may also enable the offence-related stakeholders to contact witnesses to retrieve information for a later counterevidence.
2. *Offender communication management:* The two entities (Notifier and Designated-as-offender contact point) that enable communication with the offence-related stakeholders are placed here. The Notifier performs the legal notification of every fine (initial, intermediate, final) and resolution (appeal resolution). The Designated-as-offender contact point allows these stakeholders to introduce allegations, counterevidences and appeals.
3. *Data management:* This block is formed by three entities that manage all the process-related data. First, the Designated-as-offender personal data manager gathers all the personal data (including the driving licence information) related to the Designated-as-offender. Second, the vehicle data are managed in the Vehicle data manager. These two entities may be implemented using national registers or the EUCARIS database. Third, the Process data manager stores the data exchanged with stakeholders, thus ensuring process traceability.
4. *Enforcement process management:* This block is divided into four groups, each one called as the phase which it refers to. The Starting group contains two entities. First, the Evidence analyser completes the offender personal data and vehicle description (if not contained within the initial evidence) and scrutinises the evidence authenticity and its reliability. In case this evidence is determined to be valid, the Initial fine issuer establishes the initial fine considering the described facts and the legislation in force.

The Preliminary investigation group is formed by four entities – the Liable driver analyser, the Counterevidence analyser, the Allegation analyser and the Intermediate fine

Table 1 Data structures on each process phase

Process phase	Data structure	Information elements
starting	initial evidence	vehicle data: identifier [e.g. number plate (65 004)], make and model (65 007, 65 008), type (65 005) offender data, if known: name (200, 201), postal address (218–222), identifier type and number (216, 217), driving licence type (n/a) offence description: speed limit (65 101), recorded speed (65 102, 65 103), place (304–310) and time (311–313) witness data, which may be one of: camera reference number (65 001), recording device (65 104, 65 105), person name (200, 201) and postal address (218–222) or police officer identifier (n/a)
	initial fine	initial evidence, infraction data: infringed rule (300, 301, 314, 315), fine amount (700–703), demerit points cost (n/a) authority issuing the fine: name and identifier (101,102), legal basis that enables the Authority (n/a) legal process reference: identification number (505), date and time (n/a) payment: amount already paid and remaining amount (704–706), legal consequences of partial payment (n/a) legal period and procedure to present allegations and counterevidences (n/a). Offender postal address (218–222)
preliminary investigation	allegation	offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) legal process reference: identification number (505) Vehicle data: number plate (65 004), make and model (65 007, 65 008) allegation: alleged element(s) (n/a), motivation (n/a), allegation time (n/a) and place (n/a) receiving authority: name and identifier (101,102)
	counterevidence	offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) legal process reference: identification number (505) vehicle data: number plate (65 004), make and model (65 007, 65 008) evidence data, which may be in form of: Testimony: person name (n/a) and postal address (n/a), testimony content (n/a). Graphical proof: picture or video (n/a). Probatory element: content (n/a) Counterevidence time (n/a) and place (n/a) receiving authority: name and identifier (101,102)
	intermediate fine	authority issuing the fine: name and identifier (101,102), legal basis that enables the Authority (n/a) offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) vehicle data: number plate (65 004), make and model (65 007, 65 008) legal process reference: identification number (505) considered facts: description (n/a), relevance (n/a) proposed fine revised amount (n/a). Date and time (n/a). Legal period and procedure to present allegations (n/a)
resolution	allegation	same contents as in the preliminary investigation
	final fine	authority issuing the fine: name and identifier (101,102), legal basis that enables the authority (n/a) offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) vehicle data: number plate (65004), make and model (65 007, 65 008) legal process reference: identification number (505) considered facts: description (n/a), relevance (n/a) definitive infraction data: infringed rule (300, 301, 314, 315), fine amount (700–703), demerit points cost (n/a) payment issues: amount already paid and remaining amount (704–706), legal consequences of partial payment (n/a). Legal period and procedure to present appeals (n/a). Date and time (n/a)
appealling	appeal	offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) legal process reference: identification number (505) appealling content: appealed elements (n/a), motivation (n/a) Receiving Authority: name and identifier (101,102). Date and time (n/a)
	appeal result	offender data: name (200, 201), postal address (218–222), identifier type and number (216, 217) legal process reference: identification number (505) resolution content: appeal result (n/a), motivation (n/a) issuing authority: name and identifier (101,102), legal basis that enables the Authority (n/a). Legal provision on the potential actions by the offender (n/a). Date and time (n/a)

issuer. The Liable driver analyser receives the allegations that identify another person as the offending driver. This entity verifies the plausibility of such identification trying to decrease the chance of fraud. The remaining allegations are evaluated by the Allegation analyser, who establishes their authenticity and their relevance in the process. The Counterevidence analyser operates in the same way over the counterevidence. Based on their evaluation results, the Intermediate fine issuer confirms, revokes or decreases the initial fine.

Process resolution contains the Process analyser and the Final fine issuer. The former revises process development and determines if the legal framework has been respected. Excessive delays or unreliable data elements are examples of illegal process executions. Moreover, it evaluates the allegations sent after the Intermediate fine. Using these analysis results, the Final fine issuer establishes the final fine. Although the task performed by this entity is quite similar to that of the Intermediate fine issuer, they must be independent entities to mitigate the threat of collusion.

Finally, in the Appealing group the Appeal analyser determines the relevance of a given appeal and, based on such assessment, the Appeal result issuer definitively confirms or cancels the fine.

4 Model suitability validation against current representative enforcement systems

The model proposed in this work must be suitable to represent current enforcement systems. In this section this property is validated against the Spanish and French enforcement systems already introduced in Section 2.2.

For this purpose, the entities identified in this model have been matched with the different functional parts of each system (Table 2). The granularity of the matching is related to that of the functional description. Thus, the ESTRADA description enables specifying which module of the whole system is in charge of a set of operations. On the contrary, the CSA description only establishes which operations are carried out in the national processing centre (referred to as CACIR, Centre Automatisé de Constatation des Infractions Routières) and those that are performed by other entities.

In general words, almost all functionalities have been identified in the proposed model. There are two exceptions – the Data requester task was not explicitly detailed in the studied systems and the Appealing phase is out of the scope of the CSA. As a result, the suitability of these parts of the proposed model is not completely contrasted.

4.1 Model suitability to the Spanish ESTRADA

The Evidence collector is found in two different entities of the Spanish traffic agency (called DGT) that are related to radar and surveillance cameras management. The Notifier operations are performed by regular mail (managed by the Spanish postal company) or by electronic mail managed by the electronic notification module of the DGT's data processing centre (DPC). The Designated-as-offender contact point is performed in module M2 of the ESTRADA processing centre.

With respect to the process management entities, they are placed in different modules of the ESTRADA centre except from the different fine issuance entities (Initial, Intermediate and Final fine issuers), which are placed in the Enforcement process module of the DGT's DPC.

Table 2 Model suitability validation against ESTRADA and CSA

Model entity	CSA	ESTRADA
evidence collector	pictures received and decoded in the National Processing Centre (CACIR)	radar management system and Picture server of the Spanish Traffic Authority
data requester	not explicitly detailed	not explicitly detailed
notifier	regular mail sent by the national postal system (La poste)	regular (certified) mail; Electronic mail (Electronic notification module in the Data Processing Centre of the Spanish Traffic Authority)
designated-as-offender contact point	regular mail to National Processing Centre	ESTRADA M2 module (Paper-based documentation received and classified)
evidence analyser	offender data retrieved by the National Processing Centre	ESTRADA M1 module (Owner data retrieval)
initial fine issuer	automated process under the supervision of the Public Prosecutor Officer	enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
liable driver analyser	analysed by the National Processing Centre	ESTRADA M3 module (Citizen-given data processing)
counterevidence analyser, allegation analyser	the Public prosecutor analyses the material provided by the *Designated-as-offender*	ESTRADA M3 module (Citizen-given data processing), although the processing of counterevidences is not explicited
intermediate fine issuer	the Public prosecutor creates this fine	enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
process analyser	the case is heard by a Police court in case that the previous allegation/counterevidence has not suspended the fine	ESTRADA M3 module (Citizen-given data processing)
final fine issuer	the Police court issues this final fine	enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
appeal analyser	out of the scope of CSA	ESTRADA M3 module (Citizen-given data processing) and Appeal and allegation system in the Data Processing Centre of the Spanish Traffic Authority
appeal result issuer	out of the scope of CSA	appeal and allegation system in the Data Processing Centre of the Spanish Traffic Authority
designated-as-offender personal data manager	national driving licence database; EUCARIS	Spanish driver and offenders register; EUCARIS
vehicle data manager	national number plate database; EUCARIS	Spanish vehicle register; EUCARIS
process data manager	held within the National Processing Centre	ESTRADA M2 module (Envelope removal, classification, digitalization, storage) and Document Manager of the Data Processing Centre of the Spanish Traffic Authority

The data management entities are placed in different modules. The Designated-as-offender personal data manager is performed by the Spanish driver and offender register, whereas the Vehicle data manager is on the national vehicle register, both placed in the aforementioned DPC. In both cases, they may also be realised by the EUCARIS database. Regarding the process data management, it is jointly addressed by the ESTRADA module M2 and the Document manager of the DPC.

4.2 Model suitability to the French CSA

In this system, evidence collection and analysis are performed by the national processing centre (called CACIR). On the other hand, communication with the offender is performed exclusively by regular post, managed by the national French postal company. The initial fine issuance is also addressed by the CACIR, supervised by the Public prosecutor officer.

Beyond the Starting phase, the remaining enforcement process is conducted manually. In particular, the preliminary investigation is performed by the Public prosecutor, whereas the Process resolution is performed by a police court.

Regarding data management, both the Designated-as-offender and Vehicle data management are performed in national databases or the EUCARIS database. Finally, the Process data management entity functions in the CACIR processing centre.

5 ITS-based enhancements on enforcement systems: integration in the proposed model and analysis

This section focuses on how the ITS-related technologies may contribute to solving the problems of current enforcement systems described in Section 2.2. Table 3 summarises the comparison between current practices and the envisioned ITS-enhanced practices. Such a table also details the entities in the model that are affected by each approach. Note that none of the proposed algorithms (see Appendix 1) should be changed to implement the ITS-based improvements.

5.1 Improvements on offender identification

ITS-related identification techniques for vehicles (EVI) and also for its driver (Electronic identification card or Electronic Driving License), enable a more immediate electronic offender identification. An automatic remote verification may be performed using the Driver credentials reader, as envisioned by TISPOL [https://cleopatra.tispol.org/cleopatra/europe/general/technology/identifying-and-fining-owner-vehicle/identifying-and-fining-owner, accessed January 2012].

1. *Integration in the proposed model:* Apart from the Offending vehicle (which should be ITS-enabled, as described in Section 2.3), only automatic sensor devices are affected as they should perform the electronic authentication protocol. The remaining entities (starting from the Evidence Collector) are not aware of this issue as the 'initial evidence' structure was already prepared to contain the real offender identification.
2. *Comparison with current approaches:* As opposed to cameras, the ITS techniques allow the driver to be identified in a shorter time. With cameras it is the vehicle owner who identifies the real offender, and this action may take several days. Instead, the ITS techniques require a few seconds or minutes depending on the availability of resources. This improvement takes less time if this identification is performed by police patrols, as it only requires time to physically check the credentials and fill up a form. Concerning the incurred costs, deploying and maintaining the ITS infrastructure (e.g. set of Road-Side Units) requires a significant investment, which is assumed to be higher than the current costs. However, extensive cost-benefit analysis has concluded the long-term suitability of the ITS developments [17].

A key factor in this comparison is the global effectiveness of each approach, that is, the amount of detected offences in which the offender is reliably identified. Such effectiveness is potentially low for cameras owing to identification errors or fraud. Police patrols are moderately effective, because even if they reliably identify the offender, they can only operate at specific places and times. The ITS-based solutions enable a continuous reliable authentication of offenders wherever they are installed. Although there exists the chance for the driver to steal another person's credential, biometric approaches may contribute to this issue. Therefore this approach is highly effective if deployed on a wide scale.

5.2 Improvements on notification delays

ITS communication technologies are suitable for sending timely notifications to the offender through the offender's vehicle. Even if the speed of this transmission is subject to the availability of the network and computational resources, the message may be delivered either during the journey or, if required, using periodic resilient connections (i.e. gas stations). Moreover, the vehicular human-machine interface may present the notification in real time without causing a distraction.

1. *Integration in the proposed model:* The notification improvements only affect the Offending vehicle (which should be ITS-enabled, as described in Section 2.3) and the Notifier. The first one should be ready to receive (and present to the driver) the notification message. The Notifier encapsulates the mechanism to deliver such a message to the appropriate stakeholder. Thus, any future variation on this mechanism would be confined to this entity.
2. *Comparison with current approaches:* Thanks to the ITS technologies, the driver may be aware of the punishment during the same trip in which the offence was committed. In this regard, they outperform traditional surveillance cameras and are similar to police enforcement. It must be noted that the ITS technologies may only contribute to reducing two of the three delay factors ($t_{\text{send-notif}}$ and $t_{\text{access-notif}}$) to the order of minutes. To achieve improvement it is also necessary to reach a negligible $t_{\text{prepare-notif}}$, which requires an adequate background processing infrastructure.

The improvement on overall speed also has an impact on cost analysis. Thus, even if the cost of the ITS infrastructure is again significant, the process duration is reduced and therefore the cost of the bureaucracy is decreased. On the other hand, this novel notification method is more reliable than the postal method, where outdated information may cause notification loss. Therefore it is considered as reliable as current electronic or manual alternatives.

5.3 Improvements on offence description

In-vehicle sensors and the data shared through VANETs may help in offence description. Thus, sensors may give a complementary description of the situation from inside

Table 3 Current enforcement systems vs. ITS-enhanced ones. comparison on approaches in problematical issues

Problem	Type of system	Realisation	Time taken	Cost	Reliability/ robustness	Implementing entities
offender identification	current	vehicle keeper nominates the offending driver (postal)	$t_{\text{send-notif}}$ (postal) + 15 days	postal parcel	false driver nomination	vehicle owner + Designated-as-offender contact point
		vehicle keeper nominates the offending driver (electronic)	$t_{\text{send-notif}}$ (electronic) + 15 days	electronic transmission		
		police patrols stop the offending car	approximately 5–10 min (check credentials)	human resources, car patrol	depends on the ability to identify persons and the chance to counterfeit documents	police officer
	ITS-enhanced	electronic authentication protocol between infrastructure and vehicle. Use of National e-ID cards and Electronic Driving License	minutes (Depends on the availability of devices and network.)	use of RSUs	chance to use other person (e.g. co-pilot) credentials, reduced by biometry	automatic sensor devices + offending ITS-enabled vehicle
notification delay	current	postal notification	45 days [13]	postal parcel	outdated info may cause data losses	notifier + vehicle owner/current driver
		electronic notification	12 days [13]	use of inf. systems	high (but subject to availability of Inf. Systems)	notifier + vehicle owner/current driver
		police patrols stop the offending car	aprox. 15 min (fill up the form)	human resources, car patrol	high/full	police officer
	ITS-enhanced	electronic notification protocol directed to the offending vehicle. Use of OBU and HSM	minutes (Depends on the availability of devices and network.)	use of RSUs	high, as vehicles will be almost permanently connected and resilient connection is periodically available (end of journey, gas stations, etc.)	notifier + offending ITS-enabled vehicle
offence description	current	human witnesses	minutes	time consumption (witness declaration)	psychological factors, limits of perception, may affect the reliability. Lack of additional proofs	human witness
		cameras/radars	immediate	use of such devices	automatic number plate recognition has an efficiency of 90%. Weather conditions and daylight affect to their reliability	automatic sensor device
		policemen	aprox. 15 min (fill up the form)	human resources, car patrol	limits of perception may affect the reliability	police officer
	ITS-enhanced	use of in-vehicle sensors contrasted with aggregated data electronically shared between vehicles (e.g. VANET beacons)	seconds (Depends on the availability of devices and network.)	use of receiving devices by the authority (RSUs,...)	sensorial errors are possible, but their impact may be limited, as several viewpoints (i.e. surrounding vehicles) may be available	data requester + surrounding ITS-enabled vehicle

the vehicle [18]. Even if sensorial errors may happen, several surrounding vehicles may be contacted to gather their viewpoint, thus clarifying the situation.

1. *Integration in the proposed model:* The use of vehicular sensorial data may be implemented through the interaction between the Surrounding vehicles (which will offer

information using the ITS equipment) and the Data requester (who will gather it).

2. *Comparison with current approaches:* The costs of the ITS-based improvements are again greatly higher than those required for the operation of current systems. However, they enable having data currently not available, which is a significant benefit. Moreover, such data will be available a few seconds after the offence, at any place where two or more vehicles coincide. This may also help victims of offenders to rapidly report them. This fact opens the door to continuous road monitoring (as opposed to current spot-based surveillance) which promotes a permanent compliance with traffic rules. However, the same reason dictates that the ITS techniques must integrate privacy protection mechanisms [15].

6 Related work

The improvement of the road traffic enforcement process has received several contributions. The main precedents are presented below.

The ESCAPE project analysed the process at a European level and identified its effects, measures, needs and future [2]. The enforcement weaknesses pointed out by this project, as well as its suggestions to introduce new technologies, were the starting point of this work.

The European architecture on the ITS provides support for the enforcement process, particularly for the Starting phase [19]. Even if it introduces interactions with the vehicle to obtain some data, the problems considered herein are not addressed in the current version of this architecture.

The fully automatic integrated road control (FAIR) project aimed to improve enforcement by using different surveillance technologies [20]. The integration of the ITS-related technologies proposed in this work is beyond what was envisioned in this project. In fact, giving an immediate feedback to the offender is a future research issue of FAIR.

The efficiency and effectiveness of the enforcement process was the focus of the police enforcement policy and programmes on european roads (PEPPER) project [21]. This project pointed out that the ITSs could improve the enforcement process, although there were several legal, technical and operative issues that should be addressed first. Our proposal aims to offer a better understanding of the process, laying the basis for the integration of the ITS-related technologies.

7 Conclusions and future work

Current road traffic administrative enforcement practices suffer from several drawbacks that affect their effectiveness. Thus, the lack of a reliable automated driver and vehicle identification, the absence of immediate feedback after the violation and the usually limited amount of data to describe an offence are remarkable.

ITS technologies may contribute to these issues. However, it is necessary to have a complete understanding of the enforcement process before integrating such technologies. The VERA2 speeding enforcement process model lays the basis for this issue, but it is not precise enough to clarify how to integrate the ITS technologies. For this purpose, in this work such a model has been enhanced by identifying the stakeholders, the entities and their data interchanges that are produced within such a process. It has been shown that the model captures the key parts of the automated process system in both the Spanish and French cases. Based on this enhanced model, the integration of the ITS technologies has been described. The potential of such an ITS integration has been compared with current enforcement approaches.

Based on the proposed model, future research work should be focused on building an architecture and the corresponding mechanisms that integrate the ITS-related technologies identified herein. Specifically, the electronic vehicle-driver joint authentication will require an adequate privacy-compliant functional framework. On the other hand, the notification protocol should fulfil its underlying legal requirements. Finally, the reliability of vehicle-based data sources to describe an offence should be assessed considering real vehicular devices and communication networks.

8 Acknowledgment

This work was partially supported by the Ministerio de Ciencia e Innovacion of Spain, project E-SAVE, under grant no. TIN2009-13461. The authors wish to thank the anonymous reviewers for their comments that helped in improving this work.

9 References

1 European Commission: 'Respecting the rules. better road safety enforcement in the European Union. A consultation paper', 2004
2 Mäkinen, T., Zaidel, D., Andersson, G., *et al.*: 'Traffic enforcement in Europe: effects, measures, needs and future. Final report', ESCAPE Project, 2003
3 Chevreuil, M., Canel, A.: 'Development of automated traffic enforcement systems in France', Available online at: http://road-network-operations.piarc.org/
4 Toriello, A.: 'Nuevos conceptos en la gestión de denuncias del tráfico: El centro de tratamiento de denuncias automatizadas', IX Spanish ITS Congress, 2009. (in Spanish). Available online at: http://www.worlditsdirectory.com/
5 VERA2 (Video Enforcement for Road Authorities 2) project: 'Deliverable D3-1. Common data exchange format and demonstrator', 2004
6 Delaney, A., Ward, H., Cameron, M., *et al.*: 'Controversies and speed cameras: lessons learnt internationally', *J. Public Health Policy*, 2005, **26**, (4), pp. 404–418
7 World Health Organization (WHO): 'World report on road traffic injury prevention', 2004
8 European Commission: 'Comparative study of road traffic rules and corresponding enforcement actions in the member states of the EU', 2003
9 Spanish Government: 'Ley 18–2009, por la que se modifica el texto articulado de la Ley sobre Trafico, Circulacion de Vehiculos a Motor y Seguridad Vial'. Spanish National Bulletin, no. 283, 2009 (in Spanish)
10 European Commission: 'Best practices in road safety – Handbook for measures at the country level', 2010
11 Police Enforcement Policy and Programmes on European Roads (PEPPER) project: 'Deliverable 10: Implications of innovative technology for the key areas in traffic safety: speed, drink driving and restraint systems', 2008
12 Keilthy, L.: 'ANPR System Performance', Parking Trend International, June 2008. Available online at: http://www.parkingandtraffic.co.uk/Measuring%20ANPR%20System%20Performance.pdf
13 de Leon, L.c.: 'La rapidez del centro Estrada causa las protestas de los "quitamultas", (in Spanish)
14 Wolf, M.: 'Security engineering for vehicular IT systems' (Vieweg + Teubner Research, 2009, 1st edn.)
15 Hubaux, J.-P., Capkun, S., Luo, J.: 'The security and privacy of smart vehicles', *IEEE Secur. Priv.*, 2004, **2**, (3), pp. 49–55
16 ISO 18013: 'ISO-compliant driving licence – Part 1: Physical characteristics and basic data set', 2005
17 Bunch, J., *et al.*: 'Intelligent transportation systems benefits, costs, deployment, and lessons learned desk reference: 2011 update' (US Department of Transportation, 2011)
18 Lo, N., Tsai, H.: 'Illusion attack on VANET applications – a message plausibility problem'. Proc. IEEE Globecom Workshops, 2007, pp. 1–8
19 Jesty, P.: 'Extend FRAMEwork architecture for cooperative systems. Version 1.0', Available online at: http://www.frame-online.net

20 Fully Automated Integrated Road control (FAIR) project: 'Deliverable 2: integrated enforcement architecture', 2006
21 Police Enforcement Policy and Programmes on European Roads (PEPPER) project: 'Deliverable 17: Final Report', 2008
22 Spanish Government: 'Real Decreto 818/2009 por el que se aprueba el Reglamento General de Conductores', Spanish National Bulletin, n. 138, 2009 (in Spanish)

10 Appendix 1

10.1 Appendix 1: data interchanges specification

begin
Any witness stakeholder → Evidence collector (EC): *initial evidence* (Traffic environment detection)
EC → Process data manager (PDM), Evidence Analyser (EA): initial evidence (Initial evidence transfer) if *the offence is not reported by a police officer* then
EA → Vehicle Data Manager (VDM): Vehicle identifier (e.g. number plate, EVI) (Vehicle and owner/usual driver data request)
VDM → EA: Vehicle data, owner or usual driver identifier (Owner or usual driver data response)
EA → Designated-as-offender personal data manager (DPDM): Owner or usual driver identifier (Personal data completion request)
DPDM → EA: Owner or usual driver personal data: name, address, type of driving licence. Offending record(s): infringed rule(s), demerit points credit. (Personal data completion response)
EA → Initial Fine Issuer (IFI): initial evidence, Vehicle data, Offending record(s), Owner/usual driver personal data, evidence analysis result (Initial evidence verification result)
else
EA → DPDM: Offender identifier (Personal data completion request)
DPDM → EA: Offending record(s): infringed rule(s), demerit points credit. (Personal data completion response)
EA → Initial Fine Issuer (IFI): initial evidence, Offending record(s), evidence analysis result (Initial evidence verification result)
IFI → Notifier → PDM, Offence-related stakeholder: *Initial fine* (Fine notification)

Algorithm 1: Process starting

begin
 # Allegation identifying another person as the offending driver
if *the vehicle owner or usual driver was identified as the designated-as-offender and that person is not the offending driver*
then
Vehicle owner/usual driver → Designated-as-offender contact point (DCP) → Liable Driver Analyser (LDA): Allegation identifying the offending driver (Offender identification request)
 # The following action only happens if the LDA determines that it is a plausible identification. Otherwise, criminal law may be applied
LDA → Initial Fine Issuer: Offending driver personal data (Offender identification transfer)
GO TO else case in Starting algorithm
 # Counterevidence creation and transfer. This part should be repeated if multiple counterevidence is involved
Any offence-related stakeholder → Data Requester (DR) → Selected witness stakeholder:
Offender data: Designated-as-offender identifier or vehicle number plate,
Offence characterisation: date, time, place.
Requested counterevidence description: type (testimony, graphical proof, probatory element), witness stakeholder identifier (Counterevidence data request)
Selected witness stakeholder → DR → Offence-related stakeholder: Requested counterevidence data, witness stakeholder identifier, time of evidence (Counterevidence data retrieval)
Offence-related stakeholder → Designated-as-offender Contact Point (DCP) → Process Data Manager (PDM), CounterEvidence Analyser (CEA): *Counterevidence* (Counterevidence transfer)
 # Allegations are autonomously created by the offence-related stakeholder. They are also transferred for evaluation
Offence-related stakeholder → DCP → PDM, Allegation Analyser (AA): *Allegation* (Allegation transfer)
 # Counterevidence/allegation analysis. First part: additional data retrieval (if needed)
CEA/AA → DR → Selected witness stakeholder: Additional data request: Offence subject (one of: offence context, offender behaviour or road traffic status), offence context (place, date, time, offender vehicle identification), witness stakeholder identifier. (Additional test for contrasting the counterevid. and alleg. (request))
Affected witness stakeholder → DR → PDM, CEA / AA: Additional data response: Witness stakeholder identifier, requested data, time of response. (Additional test for contrasting the counterevid. and alleg. (result))
 # Counterevidence/allegation analysis. Second part: assessment. Intermediate fine issuance
CEA/AA → Intermediate Fine Issuer (IntFI): Counterevidence(s), allegation(s), additional requested data, evaluation result of these elements and their legal relevance (Assessment result transfer)
 # This notification only happens if additional data retrieval was needed
IntFI → Notifier → PDM, Offence-related stakeholder: *Intermediate fine* (Intermediate fine notification)

Algorithm 2: Preliminary investigation

begin
if *the Intermediate fine was notified to the offender (see Algorithm 2)* then Offence-related stakeholder → Designated-as-offender **Contact Point (DCP) → Process Data Manager (PDM), Process Analyser (PA):** *Allegation* (Allegation transfer)
PA → PDM: Legal process identifier (Process data retrieval (request))
PDM → PA: *Initial fine, intermediate fine, allegation(s), counterevidence(s)*, Additional data retrieved in the preliminary investigation. (Process data retrieval (response))
PA → Final Fine Issuer (FFI): Process revision, including recent allegations (if any) and assessment of their relevance in the process (Allegation evaluation)
FFI → PDM, Notifier → Offence-related stakeholder: *Final fine* (Final resolution notification)
if the offence is considered as serious then

 # According to the Spanish legislation, it must be annotated in the Designated-as-offender personal data manager in case that is considered a serious (i.e. not minor) offence [22].
FFI → Designated-as-offender personal data manager (DPM): Offender identifier, legal process identifier, infringed rule, demerit points credit (Offence record annotation)

Algorithm 3: Process resolution

begin
Offence-related stakeholder → Designated-as-offender Contact Point (DCP) → Process Data Manager (PDM), Appeal Analyser (ApA): *Appeal* (Appeal transfer)
ApA → PDM: Legal process identifier (Process data retrieval request)
PDM → ApA: *Initial fine, intermediate fine, final fine, allegation(s), counterevidence(s)*, Additional data retrieved in the preliminary investigation. (Process data retrieval response)
ApA → Appeal Result Issuer (ARI): Appeal, Appeal assessment: reasoned appeal relevance evaluation. (Appeal evaluation transfer)
ARI → Notifier, PDM → Offence-related stakeholder: *Appeal result* (Appeal resolution notification)

Algorithm 4: Process appealing