

Issues of Vehicle Digital Forensics

Dagmar Kopencova
University of Finance and
Administration
Department of Criminalistics and
Forensic Science
Prague 10, Czech Republic
dagmar.kopencova@seznam.cz

Roman Rak
University of Finance and
Administration
Department of Criminalistics and
Forensic Science
Prague 10, Czech Republic
roman.rak@seznam.cz

Abstract — Modern vehicles are equipped with a large number of electronic devices. These devices generate, transmit, process and store digital data. Human transformation from digital data creates digital information that can be used for many purposes. Thus, forensic experts, security experts, police officers and investigators can use this information to clarify a traffic accident, the behavior of a vehicle and its crew before, during and after an accident or other incident or security event under investigation. In-vehicle data is stored in different devices, in different data formats, and is generally not internationally standardized. Similarly, some tools for analyzing this data for forensic purposes within the European Union are not standardized. These facts make it difficult to use digital data and information obtained from it for forensic purposes. The paper deals with sources, classification, characteristics and uses of digital information in vehicles for forensic purposes from various perspectives.

Index Terms—Digital Evidence. Electronic Control Unit. Event Data Recorder. Safety, Safety management, Vehicle Digital Forensics, Vehicles.

I. INTRODUCTION

Today, the development of the automotive industry is associated with the phenomena of electromobility, autonomous vehicles, digitisation and telematics. New vehicles contain a large number of electronic control units which process and preserve digital data on the vehicle's activity and its occupants, including communication with the external environment. This data can also be used for forensic purposes, as described in this paper. Attention is also paid to current trends, problem areas and safety risks.

The present-day development, advancement and operation of vehicles is inseparably linked with the introduction of electronic devices and digitisation. As a result of this trend, vehicles process, transmit and save a large quantity of operational data and data connected with the activities of the vehicle's occupants. This trend has a sharply rising character, especially in connection with the development of electric engines and an effort to create and put into operation entirely autonomous vehicles that do not require the active involvement

of a driver in order to reach their established destination. Electronic processes are carried out in the vehicles themselves, which, in addition, also communicate with other vehicles and traffic and telematics infrastructure. Data from a number of devices, which are a part of the vehicle or which connect to the vehicle (mobile phones, tablets and computers of its occupants, etc.), are saved to a cloud environment.

From the perspective of forensic disciplines and criminalistics, every modern vehicle creates a large quantity of digital evidence. On average, a contemporary, newly manufactured passenger car contains more than 75 electronic control units which store over 150 million lines of source codes of support programs and which generate over 25 GB of data [2] for every hour for which the vehicle is in operation!

II. VEHICLE AS A SUBJECT OF FORENSIC INVESTIGATION

Vehicles can be involved in accidents (or other negative events) and may subsequently be subject to a forensic investigation. They can also be an instrument (means) for committing or a target for criminal acts or other events or activities with a negative impact on safety (other than in the context of road traffic). In the first case, forensic and traffic engineers or forensic experts in the field of construction, maintenance and operation of vehicles or related fields are involved in clarifying the course of events and their consequences. In the latter case, the vehicle is of interest to criminalistics units and other security-oriented institutions which deal with a variety of criminal activities and guarantee general security as such at various levels [1], [3].

In any case, every modern vehicle today turns out an enormous volume of data/information which can provide digital evidence that help to explain the course of negative events and their consequences.

III. VEHICLE AS A SOURCE OF DIGITAL DATA

Every modern vehicle contains a range of devices which generate, process, transmit or store digital data in various formats, which can be used as digital evidence to help in forensic investigations of incidents.

Typical data sources of digital evidence are:

- Black boxes (Event Data Recorders – EDR)
- Telematics and information systems (telematics and infotainment systems)
- Electronic Control Units -ECU
- eCALL units
- Key fobs
- Dash cams (front and rear)
- Aftermarket technologies

IV. BLACK BOXES (EVENT DATA RECORDERS -EDR)

Black boxes are the most widely used source of digital data (evidence) during forensic investigations of traffic accidents. They have been well-known in professional practice since the 1990s [1], when they were first used in the USA. Also known as Event Data Recorders (EDR), they are activated at the “moment” that a vehicle heads for a collision (traffic accident) [24], [23]. The EDR records events 5 seconds before the traffic accident and subsequently records and stores data over the course of the entire event; this data can then be analysed [11], [13]. Predetermined relevant data for accident analysis are sent to the EDR from an Electronic Control Unit (ECU) located inside the vehicle in a specified format and specified time sequences [16].

Single-purpose black boxes are primarily intended for accident analysis. They are not suitable, however, for forensic investigation of various acts of fraud, manipulation of the identifier of the VIN [17] stored in the vehicle in digital form, odometer fraud (rolling back the number of kilometres travelled) and detecting other vehicle activities (including automated activities), as well as the conduct of the vehicle's occupants and their communications with the environment outside of the accident event. A number of events outside of the accident have an extremely varied course and nature, and are often useful for forensic purposes during running investigations of serious criminal acts. This information or data are found elsewhere than in the black box.

V. TELEMATICS AND USER-ORIENTED INFORMATION SYSTEMS (TELEMATICS AND INFOTAINMENT SYSTEMS)

The term “**telematics**” is derived from the words “*telecommunication*” and “*informatics*”. Telecommunications involve wire and wireless transfers of data between individual components of a vehicle, between different vehicles, and potentially external components and traffic infrastructure. The term informatics can be simply defined as a method of processing and storing data, including transmitted data. The terms “telematics” (just like the term “infotainment”) therefore expresses an ability to generate, send, receive and process data. The term “**infotainment**” is a combination of the words [8] “*information*” and “*entertainment*”. The word originated in the USA, primarily with the advancement of cable television as a type of news, where the choice of topics and their processing is intended to evoke emotions and to entertain. In the original sense of the word, infotainment was perceived as an insufficiently serious source of news.



Fig. 1 Driver's seat of a modern vehicle. Skoda Kamiq. Photo: Roman Rak

The term infotainment was first introduced into the automotive industry and vehicle design in connection with the arrival of mobile phones and with video, CD/DVD players, screens (tablets) for entertaining occupants (usually children), particularly in the rear seats, and later with the use of touchless tablets on the central panel of the dashboard. The aim is to provide the occupants with the simplest, user-friendly information environment closely related to (and sometimes triggered by) the car's location, and to enable them to control information and entertainment systems (radio broadcasts), to communicate with the environment (mobile phone control), to search for information on the internet, and to orient themselves in space (navigation systems). Today, infotainment systems can be controlled by touch screens, controls on the steering wheel, or by human voices. Data can be transmitted through various communication protocols and interfaces, such as Bluetooth, WiFi, USB devices, SD data cards, etc.

Infotainment systems in vehicles are an excellent source for analysing the geographical movement of a vehicle (routes travelled, favourite routes, frequently visited destinations, etc.) and telecommunications activities of the vehicles occupants (phone calls, text messaging, internet activity, social network activity, and so on) [14]. The combination of these activities in terms of time and place of implementation gives a qualitatively new idea of the course and consequences of such events [18].



Fig. 2 Driver's seat of a modern vehicle. Mercedes G series. Photo: Roman Rak

VI. ELECTRONIC CONTROL UNIT - ECU

An electronic control unit (ECU) is a digital microcontroller which controls activities and operations in a vehicle. Modern vehicles usually have more than 75 ECUs [12], [19] which manage and control partial key processes and “operations” in the vehicle. Every ECU is responsible for controlling certain specific processes, such as the status of engine, gearbox and airbag activity, fuel levels, the overall vehicle status, the number of closed doors and fastened seatbelts, etc [9], [10].

ECUs are closely connected to the vehicle's telematics and ensure data transmission and exchange. Data connectivity is ensured by various data protocols and standards, e.g. LIN (*Local Interconnect Network*), CAN (*Controller Area Network*), MOST (*Media Oriented Systems Transports*), FlexRay, WiFi, Bluetooth, etc.



Fig. 3 Example of an infotainment panel. Skoda Kamiq. Photo: Roman Rak

Access to control and management units (to their data) inside a vehicle is provided by an external interface called OBD-II (*On-Board Diagnostics*), which makes it possible to connect to individual ECUs and to obtain required data or information.

Access to control and management units (to their data) inside a vehicle is provided by an external interface called OBD-II (*On-Board Diagnostics*), which makes it possible to connect to individual ECUs and to obtain required data or information.

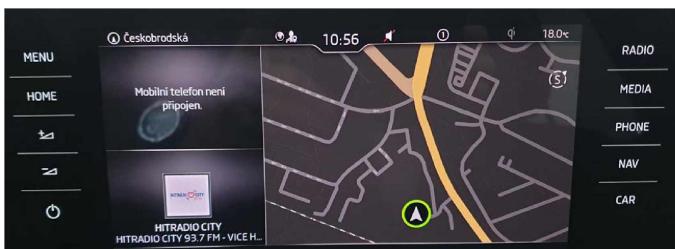


Fig. 4 Example of an infotainment panel - navigation. Skoda Kamiq. Photo: Roman Rak

Vehicle data is usually obtained through OBD connectors from ECUs or through a black box (EDR); this includes physical extraction of data. Data from such devices frequently have diverse, non-uniform and non-standard content across individual motor vehicle manufacturers.

VII. ECALL UNITS

An eCALL unit is a device which is designed to call emergency services in the event of a car crash or an emergency involving an occupant of a vehicle. This technology has been used since 1 April 2018 in all new homologated vehicles in the European Union, including vehicles imported from outside Europe intended for the European market.

The energy-independent units with high resistance and long life are activated automatically (thanks to special sensors which register an impact of the vehicle or expansion of the airbags), or can be activated manually from the front seats. Next, the closest operating centre of emergency phone line 112 is located, and data describing the location of the incident, the circumstances and the basic characteristics of the vehicle is transmitted by telematics systems. The following data is

transmitted: part of the incident, the coordinates of the vehicle's location, the direction of travel, the VIN identifier, the vehicle category, the type of fuel, the number of fastened seatbelts (i.e. the number of persons wearing a seatbelt), an indication of how the unit was activated (manually or automatically) and various other information on the credibility of the incident [22]. This data is displayed at the emergency line operating centre and serves primarily for organising and carrying out rescue operations. However, the sent data can also subsequently be used for forensics and other security tasks for investigating fraud (e.g. changes to the vehicle's identity, faking a traffic accident, and so on).



Fig. 5 Demonstration of manual activation of the eCALL system. At the push of a button, the vehicle sends not only its location but also other information about the accident, including technical and other characteristics of the particular vehicle, to the nearest rescue center. This data can be used for the following forensic activities. Photo: Roman Rak

VIII. KEY FOBS

Key fobs (smart keys) to modern vehicles are another source of valuable information of forensics investigations. They serve as an external storage device for selected important vehicle data. Key fobs contain a globally recognised unique identifier (*Vehicle Identification Number – VIN* [17]), a key transponder ID number, time data stamps indicating the last time that the key was used, the status of the odometer (counter of distance travelled by the vehicle) corresponding to the time stamp, the number of paired keys to the vehicle, the amount of fuel in the tank, other paired data as of the time that the key to the vehicle was last used, and more. Data from key fobs for unlocking a vehicle can generally be read by authorised service centres or specialised forensics instruments.



Fig. 6 Key of Jeep Compass. Use the keys to digitally identify the vehicle. Important vehicle characteristics are also stored in the vehicle keys. Photo: Roman Rak

IX. DASH CAMS (FRONT AND REAR)

Vehicles are equipped with cameras that capture and record movement and events occurring in front of and behind the vehicle in the form of digital time loop recordings. These video sequences are a welcome source of information when investigating traffic accidents. They provide visual information on the scene around the vehicle and the conduct of other road users. Recordings can clarify the conduct of certain road users (so-called brake tests, tailgating, failure to give way, improper driving in parallel lanes, dangerous overtaking, running a red light, passing over a level crossing when the warning signals are activated, and so on).

X. AFTERMARKET TECHNOLOGIES

Other digital (usually recording) devices can be installed in a vehicle. These relatively often include **journey logs** in so-called fleet vehicles (company vehicles used either entirely for business purposes, or for combined purposes – business/private). The operators of such vehicles are provided with real-time information on the movement and other activities of the vehicles. The aim is to reduce paperwork (manually filling in a logbook), to optimise operation costs, to streamline vehicle movement logic, to provide information on the current status of the vehicle, and to prevent fuel theft and abuse of the vehicle for private purposes, etc.).

Devices of this type obtain information not only from their own navigation systems, but often from the vehicle's ECUs. A specific feature of such devices is intensive telematics operation, where monitored characteristics are transmitted to the vehicle operator and then stored in the operator's own information systems or in a cloud (virtual) environment. This fact heavily affects (in a certain sense of the word, significantly complicates) forensic methods [5] of obtaining such data which is not stored and preserved in the vehicle's equipment, but in third party systems, to which it is then necessary to acquire authorised access.

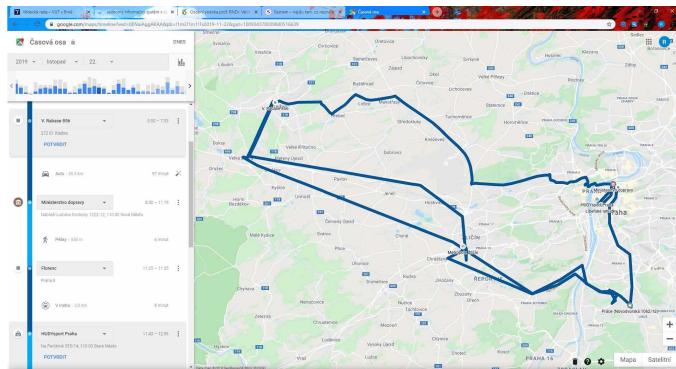


Fig. 7 Information about the movement of the vehicle and its crew can be obtained not only from embedded navigation systems in the vehicle, but also from third-party manufacturers' applications. It is sufficient for the user to have activated the Google services in their mobile and allowed sending GPS coordinates.

Data from telematics applications like journey logs can be derived from applications intended for insurance companies. Data from selected vehicle ECUs are then transmitted to remote data repositories (clouds) and various characteristics of the

vehicle's operation are assessed. These include the nature of the driver's driving style (e.g. an aggressive type – speeding, abrupt braking, intensive braking [15] and so on). The amount of the vehicle's insurance premiums then depends on these parameters.

XI. FORENSIC USE OF DIGITAL EVIDENCE

In forensics practice (engineering and criminalistics), it is possible to use digital data (evidence) for determining, analysing, clarifying, etc. the following:

- the vehicle's identity (*Vehicle Identification Number* and serial numbers of individual vehicle components)
- the driver's conduct while driving and operating the vehicle (e.g. defensive versus aggressive driving)
- the behaviour of the vehicle and/or driver over the course of an accident, and the cause and consequences of the accident
- activity around the vehicle
- (un)justified ((un)authorized) interventions into the vehicle's technology (e.g. rolling back the number of kilometres travelled)
- (un)authorised exchanges of vehicle components
- use of telecommunications by the vehicle's occupants - their "digital activity" inside the vehicle
- the vehicle's geographical location
- the economy of the vehicle's operation

In the future, we can expect much greater vehicle autonomy, coupled with very strong information support and telecommunications with all objects involved in driving and road logistics, including artificial intelligence elements. Vehicles will use their "experience", learn, and exchange information with other vehicles (v2v - Vehicle to Vehicle), traffic infrastructure (v2i – Vehicle to Infrastructure), parking spaces, etc. It will subsequently be entirely possible and essential to use much of this information for forensics work.

XII. PROBLEM AREA TO BE RESOLVED

The automotive industry is one of the most intensively developing fields. Commercial pressure is enormous, and manufacturers and individual brand names strive to outdo each other in their ranges. Anything that is new and innovative quickly finds customers, meaning that things that prove successful for one brand will usually appear in one form or another in other brands. With changes occurring at an extremely rapid pace, time intervals between individual changes are very short and constantly decreasing.

Trends in electromobility and vehicle autonomy are clear to see. In practice, however, this results in certain paradoxes in terms of security, and in substantial threats [4]. The highly dynamic nature of development and production often overtakes safety practice, especially as regards vehicle information and telecommunications systems [6]. In many cases, manufacturers pay insufficient attention to these concerns.

Modern trends of **information and communications technology** also find a use in the automotive industry. The result is a logical integration of ECUs and their CAN buses, as

well as infotainment systems inside a vehicle (which contain a considerable quantity of sensitive data) with the external environment by way of internet interfaces to remote data repositories and to various remote third-party applications. The vehicle becomes a part of the Internet of Things (IoT) [21], [7].



Fig. 8 A digital dashboard is capable of displaying much more information than traditional analogue dashboards. Drivers can set up several appearances and choose the one that suits them best. Dashboard of an Audi. Photo: Roman Rak

In the case of insufficient **security measures**, the opposite path can therefore be used to access the data and functionalities of a vehicle: to use the internet to gain unauthorised control of individual ECUs inside the vehicle. In recent years, various scientific conferences [12] have demonstrated ways in which hackers can gradually gain control of vehicle systems all the way to steering the vehicle, operating the brakes, etc.

Standardising new technologies in practice is a tough nut to crack. When innovating, it is not necessarily possible to know exactly how things will turn out, what the consequences might be and whether innovations become established in practice. As a result, different manufacturers or groups of manufacturers achieve their goals after a time by various means, technologies or their own data standards. In practice, it is therefore no easy task to carry out diagnostics, to examine the content of black boxes, to monitor various processes or to read data from ECUs across all brand names. From the perspective of diagnostics by independent service centres, government institutions (technical and emissions control stations, checks for unauthorised interference with systems, etc.) and forensics institutions, every manufacturer or group of manufacturers uses its own technology, readers, etc. Therefore, if any institutions wish to work with all brand names, they must obtain multiple devices which are only compatible with the systems of certain brand names. Universal instruments essentially do not exist, which increases not only costs, but also demands for technical equipment and software, expert knowledge, ongoing training, etc.

Standardisation of processes within the EU is progressing very slowly. The adoption of a standard for eCALL technology alone took over 8 years, and the first requests or ideas for transmitting information from a stricken vehicle to rescue operation centres are more than 30 years old.

XIII. CONCLUSIONS

The examination of digital data relating to the operation of motor vehicles (*Vehicle Digital Forensics*) is one of the widest fields of digital data (evidence) analysis, which is typically referred to as *Digital Forensics* or *Computer Forensics*. Today, examining data and digital evidence ensuing from the use of computers, mobile phones and other components of equipped

processing units is a relatively stable field which has gone through a somewhat difficult history.

Vehicle Digital Forensics is a field that is just emerging and is still waiting to be put into extensive use. Key issues are the standardisation of data interfaces, recording units and in-vehicle data storage on the one hand, and their use and application in forensic activities on the other. There will undoubtedly be a need for affordable, sufficiently general and certified forensic technologies that will be relatively easy to use in forensic investigations, as well as adequate forensic methods and methodologies. These activities will be closely associated with the training of entirely new kinds of specialists, forensic engineers and forensic workplaces [20], whose subject matter will be highly multidimensional.

REFERENCES

- [1] P. Augustin, P., R. Odler, The mission of the police in a democratic state in the context of globalization. In: Securitologia: scientific journal, semiannual, No. 2., 2013, ISSN 1898-4509. Vol. 18, Nr. 2 pp. 55-64.
- [2] E. A. Bates, Digital Vehicle Forensics [online, cit, 2019-11-17], <https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf>
- [3] M. Felcan, Implementation of European Union legislation and regulations on road safety standards of the Slovak Republic In: Road Safety: conference proceedings, 24. - 26. 9. 2008, Hotel SITNO, Vyhne, Kosice: Steelcomp, spol. s r. o., 2008, ISBN 978-80-232-0292-2. - pp. 122-132.
- [4] M. Felcan, D. Kopencova, Objects and systems - Basic analytical security features. Proceedings of the 14th International Symposium of 14 March, 2019 in international Security expo Bratislava 2019, Academy of Police Force in Bratislava, Bratislava, pp. 212, ISBN 978-80-8054-795-0, pp. 41-55
- [5] T. Hajdukova. Research Methodology, In: Application of Scientific Methods to Cases from Police Practice. ISBN 978-80-8054-766-0 (2018), pp. 8-35.
- [6] V. Holubiczszy Security of information systems - human factor. Proceedings of the 14th International Symposium of 14 March, 2019 in international Security expo Bratislava 2019, Academy of Police Force in Bratislava, Bratislava, pp. 212, pp. 177-187, ISBN 978-80-8054-795-0
- [7] L. S. Junaid, F., B. Heena, I. K. Asif, , T. Claudio: Towards Seamless and Secure Integration of Cloud Computing With Internet of Things, International Journal of Digital Crime and Forensics, vol. 11, issue 3, 2019, pp. 1-22, ISSN: 1941-6210, DOI: 10.4018/IJDCF
- [8] R. Jurecki, M. Poliak, M. Jaskiewicz, Young Adult Drivers: Simulated behavior in a car-following situation. Promet-Traffic & Transportation Volume: 29, Issue 4, pp. 381-390, 2017, DOI: 10.7307/ptt.v29i4.2305
- [9] P. Kolitschova, P. Kerbic, R. Rak, R, Forensic and technical aspects of vehicle identification labels 11th International Scientific and Technical Conference on Automotive Safety, Casta Papernicka, Slovakia, Apr 18-20, 2018. Proceedings Paper IEEE Xplore, INSPEC Accession Number: 17823676, DOI: 10.1109/AUTOSAFE.2018.8373340.
- [10] E. Kolla, J. Ondruš, P. Vertal. Reconstruction of traffic situations from digital video-recording using method of volumetric kinetic mapping. The Archives of Automotive Engineering – Archiwum Motoryzacji. 2019;84(2):147-170. doi:10.14669/AM.VOL84.ART11.
- [11] I. Makarova, K. Shubenkova, P. Buyvol, V. Mavrin, I. Giniyatullin, K. Magdin. Safety Features of the Transport System in the Transition to Industry 4.0. The Archives of Automotive Engineering – Archiwum Motoryzacji. 2019;86(4):79-99. doi:10.14669/AM.VOL86.ART6.
- [12] H. Mansor, K. Markantonakis, R. Nakram, R. N. Mayes, K. Gurulian, I.: Log your car: The non-invasive vehicle forensics. 2016 IEEE International Conference Trustcom/BigDataSE/ISPA, Trust, Security and Privacy in Computing and Communications, [online, cit, 2019-11-26], <https://ieeexplore.ieee.org/document/7847047/authors#authors>
- [13] M. Moravcik, M. Jaskiewicz, Boosting car safety in the EU. 11th International Scientific and Technical Conference on Automotive Safety. Location: Casta Papernicka, Slovakia, Date: Apr. 18-20, 2018. WOS:000435296000013.

- [14] M. Odlerova, M. Information technology and operative-search activity. In: Act on police corps: Application on practice. Pilsen: Ales Cenek, s.r.o., ISBN 978-80-7380-682-8, pp. 196-217, 2017
- [15] K. Pavlica, R. Kaiser, E. Jarošová, E. Balanced Leadership: Managerial Skills Dynamics. Prague: Management Press, 2015. ISBN 978-80-7261-289.
- [16] P. Posuniak, M. Jaskiewicz, F. Kowalski, F. Dąbrowski, Child restraint systems: problems related to the safety of children transported in booster seats (without integral safety belts). 11th International Scientific and Technical Conference on Automotive Safety. Location: Casta Papiernicka, Slovakia, Date: Apr. 18-20, 2018. WOS:000435296000058
- [17] R. Rak, P. Kolitschova. Forensic and manufacturer aspects of VIN production and location on motor vehicles. The Archives of Automotive Engineering – Archiwum Motoryzacji. 2018;82(4):131-142. doi:10.14669/AM.VOL82.ART10.
- [18] J. Reitspis, L. Gaspierik, K. Boc, M. Felcan. Policing in the Slovak Republic: The Organization and Current Problems of Police Work, In: Handbook on Policing in Central and Eastern Europe. - New York: Springer Science Business Media, 2013. - ISBN 978-1-4614-6719-9. - pp. 239-261
- [19] O. Stopka. Approach technique of specifying a proper autonomous cart type for its service in the logistics center. The Archives of Automotive Engineering – Archiwum Motoryzacji. 2019;84(2):23-31. doi:10.14669/AM.VOL84.ART2.
- [20] F. Vlach, Evaluation of Cooperation between Educational Institutions of the Armed Forces. New trends in police training III. International conference. Holesov: Higher Police School and Secondary Police School of the Ministry of the Interior in Holesov, 2018, pp. 121–124. ISBN 978-80-7616-008-8.
- [21] H. Xinchao, L. Zihan, L. Wei, L. Hongmei, X. Shijun. Fast and Effective Copy-Move Detection of Digital Audio Based on Auto Segment. International Journal of Digital Crime and Forensics, vol. 11, issue 2, 2019, pp. 47-62, ISSN: 1941-6210, DOI: 10.4018/IJDCF
- [22] R. Zrubak, R. Rak, Project eCALL – Car in Emergency Situation. 7th Scientific International Conference Crisis Management: Environmental Protection of Population – Conference Proceedings. Edited by Horak, R.; Juricek, L.; Schwarz, R. pp. 251-258, 2012. Proceedings paper.
- [23] J. Wicher Reconstruction of the collision of many cars considered as the system of material points. The Archives of Automotive Engineering – Archiwum Motoryzacji. 2019; 83(1):123-131. doi:10.14669/AM.VOL83.ART9.
- [24] Event data Recorders (US National Highway Traffic Safety Administration regulation) (NHTSA), 2018 edition, updated as of May 29, 2018, The Law Library, printed by Amazon, ISBN 9781729754900



Dagmar Kopencova (F'67) was born in Hranice na Morave, Czech Republic, in 1967. She graduated from the Vocational School of Electrical Engineering in Valasské Mezirici and from the combined study of Local Economy in Lipník nad Bečvou, - Electrical Engineering for Electronic Devices. She received her bachelor's degree in Security Services from the Police Academy in Prague, Czech Republic in 1997. She completed her master's degree in the same field in 2012 at the Police Academy of the Slovak Republic in Bratislava in 2001. Here she passed a rigorous legal examination. Title PhD. she received in 2019 at the Police Academy in Prague in the field of Security Management and Criminology.

She worked for a significant part of her professional career as an investigator at the Office of Investigation for the Czech Republic on organized crime, then in the nationwide departments of the National Drug Headquarters and the Corruption and Financial Crime Unit. Here she dealt with the detection and investigation of particularly serious, organized crime. From 2005 to 2016, she worked as a lecturer at the

Higher and Secondary Police School of the Ministry of the Interior in Prague.

JUDr. Dagmar Kopencova, PhD. she is also commander of search and rescue dog unit at the fire department and cooperates with the national forces of the integrated rescue system. She is the author of several dozen professional works and co-author of several books.



R. Rak (M'62) was born at Kladno, Czechoslovakia. After graduating from a science-based grammer school, he studied at the Moscow Energy Institute, Russia. He received the MSc. in the field of nuclear machinery and energy equipment, 1988. His PhD. he finished 2001 in forensic engineering at Technical University Brno, Institut of Forensic Engineering, Czech Republic. He was habilitated by an associate professor (2002) in the field of personal and property protection at the Academy of the Slovak Police Forces, Bratislava. He was inaugurated by a professor in the same field, 2016.

In 1990-2001 he worked as a police officer in the services of the Ministry of the Interior in the field of Vehicle Crime and Police Informatics. During the period 2002-2015, he lectured at the Police Academies in Prague and Bratislava, Czech and Slovak Republic. His professional interests include Criminalistics and Forensic Science, Theoretical Aspects of Forensic Identification and Trace Theory, Digital Footprints, Identification of People, Vehicles, Writing, Automotive, Computer Crime, Biometric Identification, Criminalistic Informatics, Criminalistics, Criminalistic Documentation.

Prof. Roman Rak is the author or co-author of more than 20 scientific monographs and academic textbooks. He is the award recipient of the Czech Republic's Minister of the Interior for the development of national security.