# Cybercrime in Automotive Security in the 21th Century

***Milan Marcinek***
*ORCID: n/a*
*Academy of the Police Force in Bratislava, Slovakia*

***Abstract.*** *Intelligent transportation systems introduce smart technology to civil transportation infrastructure. Modern services depend on the use of information technology systems. Cybersecurity plays an important role in the ongoing development of information technology. Enhancing cybersecurity and protecting critical information infrastructures are essential to each national security. Nowadays, vehicles are equipped with electronic security systems that automatically call the emergency service operator in case of an accident. This safety system combines different technology in order to ensure vehicle safety. When you are unconscious, the system informs the rescuers where the accident happened. They arrive at the scene of the accident within a few minutes. The introduction of this system in vehicles results from Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 on type-approval requirements for the deployment of the 112 on-board eCall system and amending Directive 2007/46/EC. Nevertheless, there is concern that this could expose connected cars with their passengers to potential risks from online threats. Scientific development for the security of our vehicles has also raised the possibility of misuse of vehicle data. It is seen that e-threats have become the leading threats in the further deployment of e-services in the society of the 21st century.*

**DOI: 10.5604/01.3001.0014.6694**
**http://dx.doi.org/10.5604/01.3001.0014.6694**

**Keywords: cybercrime, cybersecurity, crime, eCall, driver, electronic device, GPS, road, vehicle, driver, injury, safety, security**

## Introduction

The Internet has become one of the fastest-growing areas of the modern world. The demand for connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment[1]. The fact that the 2010 United Nations General Assembly resolution on cybersecurity addresses cybercrime as the major challenge underlines this. Making the Internet safer protects the users, which has become crucial to the development of new services in government policy. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, it includes the adoption of appropriate

[1] Cybercrime often has an international dimension. The term cybercrime defines a range of offences, not only traditional computer crime. It also covers offences with any relation to networks and also single computer systems. It is activity in which computers or networks are targets of criminal activities.

legislation against the misuse of the intelligent transport system for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this responsibility required coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.

Cybersecurity strategies help to reduce the risk of cybercrime. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. The World Summit on the Information Society recognised the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime.

The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas:

- Legal measures — focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.
- Technical and procedural measures — focuses on key measures to promote the adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards.
- Organisational structures — focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems.
- Capacity building — focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda.
- International cooperation — focuses on international cooperation, dialogue and coordination in dealing with cyberthreats[2].

As it seems, a comprehensive approach against cybercrime is needed. Considering only the technical measures, any crimes cannot be prevented. International cooperation, such as international dialogues, cooperation and coordination in dealing with possible future cyberthreats in this area is also crucial. Sufficient legislation and a legal framework is an essential part of each cybersecurity strategy.

## eCall System

Among the intelligent transport systems, eCall consists of information and communication technology located either in a vehicle or transport infrastructure. It serves to optimise and manage road transport, increase road safety and continuity,

[2] *Electronic source:* www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html, *accessed:* 2.05.2019.

improve the management and maintenance of roads, improve public transport services and reduce the negative impact on the environment. It provides transmission, collecting, processing and exchange of information among service providers, traffic information providers and transport infrastructure users.[3] The eCall system is a European initiative intended to bring rapid assistance to motorists involved in a collision anywhere in the European Union. The eCall system is mandatory in all new cars within the EU after April 2018.

The concept of eCall was presented in 1999 by European civil servant Luc Tytgat, at the launching of the Galileo project, by the European Commission. The year before, 170 experts met in Brussels, invited by the Commission, to analyse the European dependence on the American GPS system, and also to gather civilian applications/propositions.[4] As it seems, these plans aim at the mandatory introduction of eCall across the EU. In general, all new models of passenger cars and light commercial vehicles will be equipped with the eCall system as well as the necessary infrastructure in order to properly receive and process eCall. Data obtained through eCall enable rescue services to provide assistance to drivers and passengers faster.

The European Commission introduced eCall, a groundbreaking initiative intended to bring rapid and automatic assistance to motorists involved in incidents anywhere in the European Union. Industry coalitions such as ERTICO, Europe's Intelligent Transportation System organisation, European Member States and ITS industry leaders around the globe are working hard to develop and deploy new technologies and strategies to meet the eCall challenge. To meet the challenge of developing a Pan-European eCall program, ERTICO and its member organisations supported the EU-funded Harmonised eCall European Pilot programmes, also known as HeERO.

The HeERO 1, HeERO 2 and iHeERO programmes began in 2011 and will continue. They contain interoperable eCall programs in all participating EU regions, which are synchronised across country and network borders. Due to HeERO, eCall has been successfully pre-deployed in several regions according to European Norms using 112 as the pan-European PSAP emergency call number. A 112-based emergency call relies on an automatically established two-way emergency call to a Public Safety Answering Point (PSAP) call centre immediately following an incident or after manual activation. The Cinterion Machine-to-Machine (M2M) module solution reliably sends the collected MSD to a PSAP via cellular networks. In addition, the module establishes an automatic hands-free voice call so PSAP staff can gather additional information from the involved passengers. The call helps determine what emergency services are needed so early responders arrive at the scene of an incident fully informed and prepared to help as needed.[5]

[3] Marcinek M, Simulation of crisis situations of the national and international crisis management system as a support for crisis managers' education, [in:] Nehody s hromadným postihnutím osôb. International Congress. Žilina, 2011, pp. 33–35.

[4] Marcinek M, Linka tiesňového volania eCall v podmienkach Slovenskej republiky. The emergency line eCall in the Slovak Republic, [in:] Bezpečnostné fórum 2015. I. Zväzok: zborník vedeckých prác. Banská Bystrica, 2015, pp. 161–165.

[5] The European Commission estimates that eCall is expected to reduce emergency response times by 50% in rural areas and 40% in urban areas.

eCall works on an upgraded Europe-wide interoperable PSAP infrastructure, and is installed or embedded in M2M communication devices in all vehicles. In the event of a serious road incident, the In-Vehicle Equipment (IVE) must be able to automatically dial 112 and reliably communicate incident details over wireless networks.

These details are collectively defined as the minimum set of data (MSD) and include:

- time of the incident,
- cause of activation,
- GPS coordinates, and
- VIN.[6]

eCall can also be activated manually. The mobile network operator (MNO) identifies that the 112 call is an eCall from the 'eCall flag' inserted by the vehicle's communications module. The MNO handles the eCall like any other 112 call and routes the call to the most appropriate emergency response centre — Public Safety Answering Point (PSAP). The PSAP operator will receive both the voice call and the MSD. The information provided by the MSD will be decoded and displayed on the PSAP operator screen. At the same time, the operator will be able to hear what is happening in the vehicle and talk with the occupants of the vehicle if possible. This will help the operator ascertain which emergency services are needed at the accident scene (ambulance, fire, police) and rapidly dispatch the alert and all relevant information to the right service(s). The European standards do not specify whether eCall is provided by using an embedded network access device (GSM module) or using nomadic or portable equipment, i.e. mobile phone, however, in the pan European eCall operating requirements, it is defined that:

- the solution is robust and will normally survive a crash;
- the quality of service of the in-vehicle equipment, including communications equipment, is reliable.[7]

## Data Protection in-Vehicle Systems

On 26 November 2012, the European Commission produced a draft Regulation regarding the 'harmonised provision for an interoperable EU-wide eCall' to take place by 1 October 2015.[8] Some EU countries initiated a discussion regarding the impact eCall would have on privacy and data protection. Moreover, other discussions dealt with mandatory installation of Event Data Recorders (EDR). This gadget is known as a black box, and especially in the context of aircraft, as a flight

[6] Marcinek M, Euro-NCAP a simulácie nárazov automobilov — crashtesty, [in:] Rozvoj teórie bezpečnostných rizík a tvorba krízových scenárov [elektronický zdroj]. Zborník z konferencie s medzinárodnou účasťou, ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave, 5.12.2013. Akadémia Policajného zboru v Bratislave. Bratislava, 2014, pp. 210–214.

[7] The most reliable solution is a fully embedded system with an embedded GSM module, embedded SIM, and the ability to manage the devices over the air.

[8] European Union, Draft Regulation No. 305/2013. *Electronic source:* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0305&from=EN, *accessed:* 14.11.2019.

data recorder. In the car, the term may be similar to the term with a camera. Nonetheless, there really is a black car box that records your every move. It contains important information about the course of the journey, when we use a flight accident as an example, which can reveal what has happened. Truthfully, EDR has existed in cars for a longer time. It served mainly as a source of information for airbags in order to activate them. Consequently, the unit improved and began to collect a lot of other information. Nowadays, we can learn not only vehicle's speed and location, but also the pedal positions and the position of the steering wheel. As an example, in the United States, there is mandatory deployment of EDR units for cars. Some manufacturers have already put EDR into their cars in Europe. Certainly, the companies do not discuss this integrated mystery. The problem with EDR is also how to access the data. This requires not only special hardware and software, but also real knowledge of the issue.[9]

EDR is probably installed in most modern cars. The data are collected only for automakers to help them improve the vehicles. It is also essential to explain the important distinction between eCall and EDR. While the eCall system may not record the location of the car constantly, EDR does have that capability. There are concerns that the EDR's ability to gather extensive data can and will be misused, as:

- the data could be accessed by hackers to track an individual's location.
- insurance companies can use this to promote personalised insurance quotes by recording how individuals drive.
- police forces have already started using eCall systems to track suspicious motorists.

The European Commission has stated that the purpose of eCall is to help mitigate the consequences of serious road accidents across the EU.[10] Both systems are, however, similar to each other.

Naturally, there are differences between eCall and EDR. The eCall system has been designed to send in-vehicle emergency calls using the EU emergency telephone number: 112. EDR is fitted in vehicles when they are manufactured. The eCall system may be installed after that. EDR can also not be switched off once it is installed in the vehicle. It is important to note that technology similar to eCall can already be purchased by individuals if they wish to voluntarily install it in their vehicle. The European Commission has stated that the MSD includes the exact location of the crash, time and vehicle description.[11]

According to a report by the European Telecommunications Standards Institute, the MSD also includes the driving direction resulting from accurate satellite-based data.[12] This data is necessary in order to enable the emergency services to assess

[9] In some US states, EDR data may be used to investigate an accident in a court, some of which may be used without the consent of the owner of the vehicle. In Europe, however, such a possibility does not yet exist, even though this theme is becoming more widely discussed.

[10] The European Commission, eCall: automated emergency call for road accidents mandatory in cars from 2015. *Electronic source:* http://ec.europa.eu/commission_2010-2014/kallas/headlines/news/2013/06/ecall_en.htm, *accessed:* 15.09.2019.

[11] European Commission. *Electronic source:* http://www.imobilitysupport.eu/ecall/, *accessed:* 15.09.2019.

[12] ETSI, What is eCall? *Electronic source:* www.ietf.org/proceedings/87/slides/slides-87-ecrit-1.ppt, *accessed:* 15.09.2019.

the seriousness of the accident. Additionally, the report states that the EDR will record for 20 seconds before the accident and 10 seconds after. The European Commission has not made any remarks regarding what recording will take place before and after an event. The opinions say that it is unclear whether or not this data will be included in the MSD as standard. If the MSD does include data before and after the incident, this means that the EDR is not passive. In order to obtain data prior to the incident, the EDR must be recording and erasing continuously. As the EDR has the ability to record the vehicle's exact location, if it is hacked, detailed information about the driver's location and journey details would then be available.[13]

The information in the MSD lets the emergency services know the exact location of the vehicle.[14] The European Commission has called for eCall devices to be fitted in all new types of passenger and light commercial vehicles, such as small vans, with the Commission estimating that '2033 will see full penetration of the technology.'[15]

As a result, the use of EDR and eCall will become a mandatory part of vehicles, as, once it has been installed drivers, will be unable to remove the technology. EDR can also not be switched off once they have been installed in the vehicle.

## Conclusions

The simple definition of cyber crime is 'crimes directed at a computer or a computer system'. The nature of cyber crime, however, is far more complex. It may appear from different sources. However, one thing remains the same. It is data, not the system that is its target. Investigating crimes against data means we have to investigate the crime scene: the computer system. That is the place where we collect the evidence of the crime against the data. To find a starting point, though, it may be difficult compared to other forms of crime, i.e. burglary, murder, theft etc. Moreover, we may find that there are few good clues to start with. There may be no obvious signs. Another aspect of cybercrime is that nobody wants to admit that it has happened to them. Statistically, computer criminals have less than a 1% chance of being caught, prosecuted, and convicted of their deeds. That does not mean that we cannot fight against this crime effectively. It only means that we have to work smarter and harder. Cyber crime can result in confidential information

[13] According to an article in The Sunday Times, this type of data has already been used by the police to track motorists. It states that some INTERPOL members are using the eCall system for surveillance operations.

[14] Confusingly, there appears to be differing statistics available from the European Commission on how effective eCall could be. One estimate notes that when fully deployed, eCall could save up to 2,500 lives a year, ease the severity of road injuries and reduce congestion due to speeding up emergency response times by 40% in urban areas and 50% in the countryside. However, an alternative European Commission estimate is that eCall could save up to 747 lives each year once fully deployed and that emergency response times in urban areas will increase by 60%.

[15] European Scrutiny Committee, Twelfth Report of Session 2013–14. *Electronic source:* http://www.publications.parliament.uk/pa/cm201314/cmselect/cmeuleg/83-xii/8310.htm, *accessed:* 13.08.2019.

being compromised; affecting the price of the victim's publicly traded shares. It can be an attack on a corporation's marketing information, causing misinformation to be communicated to the sales force. Misinformation is an element of intelligence that has application in the business world. It consists of altering or creating information to give a false impression about a target's activities, financial situation, or future plans.

Safety has become a top interest for both new-car manufacturers and customers. Car manufacturers have been developing technology to help prevent accidents and significantly reduce the risk of injury and death in the event that you are involved in a collision. It is important that your vehicle can provide you with maximum protection in an accident. How safe a car is can be determined by a number of factors. Following the measures foreseen in the Transport White Paper 2001, the situation of road safety has improved. Road fatalities have declined by more than 19 % since 2013 in the EU.

However, with thousands of deaths and millions injured, roads remain the least safe mode of transport. New vehicle technology offers potential benefits, but the driver is a critical factor, especially among teens and older drivers. Vehicle safety features have become a part of almost every car model. Car manufacturers have integrated different safety system units in order to provide occupant protection. There are also systems for theft protection. One single unit is installed with some improvisations in order to make it impossible for the thieves to disable these systems. Furthermore, new visions plan new technologies that would reduce the deaths and injuries caused by road accidents. One of the goals is to integrate advanced technology into cars to prevent driving accidents caused by alcohol. Sensors in the car's seats and gearshift will detect alcohol through the driver's perspiration and prevent the vehicle from being driven. Additionally, a camera will watch the driver's eyes. If it detects signs of drowsiness or drunkenness, the car will issue a voice alert to the driver and tighten the seat belt as a wake-up call. While this futuristic concept car may not be hitting the highways just yet, it is interesting to see what future will bring in car security systems in order to prevent external threats on the roads.

Finally, no connected computer system is 100% guaranteed secure in terms of invulnerability and the integrity of the data it holds. Some of the risk can be balanced by allocating security resources to where it is needed most at any given period. Identifying the motivating factors behind cyber-attacks can prove an effective toll in countering cyber-crime. For the automotive sector, such motives might include, i.e. access to online automotive apps and services that contain banking records, general personal identification data as social media usernames and passwords, insurance and tax data useful for identity theft or international travel permits etc. These motives may also include illegal access to intellectual property, sabotage or degrading of vehicle and connected system performance, terrorism with disabling vehicles as part of an attack, and vehicle identification re-assignment in the case of stolen cars. A series of events should be proposed to identify these common challenges and threats in the modern automotive industry and cybersecurity's issues in transport. However, these events should provide an environment to encourage mutual cooperation and research within the industry in order to provide safety, security and innovation in the 21st century.

## References


1. Commission Staff Working Paper, Impact Assessment, Accompanying the document, Commission Recommendation on support for an EU-wide eCall service in electronic communication networks for thetransmission of in-vehicle emergency calls based on 112 ('eCalls'). Brussels, 8.9 2011.
2. eCall — saving lives through in-vehicle communication technology, General fact sheet 49. European Commission, October 2011.
3. *Electronic source:* ec.europa.eu/information_society/activities/esafety/ecallstandards
4. *Electronic source:* http://ec.europa.eu/commission_2010-2014/kallas/headlines/news/2013/06/ecall_en.htm
5. *Electronic source:* http://ec.europa.eu/transport/road_safety/projects/doc/veronica2_final_report.pdf
6. *Electronic source:* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52009DC0434
7. *Electronic source:* www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf
8. *Electronic source:*www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf
9. Environment and E-Application Department, ITU Telecommunication Development Bureau., September, 2012
10. ETS 185 — Convention on Cybercrime Environment and E-Application Department, ITU Telecommunication Development Bureau, September, 2012.
11. Gercke M, Understanding cybercrime: phenomena, challenges and legal response, Understanding cybercrime: phenomena, challenges and legal response,
12. Marcinek M, Dworzecki J, General Vehicle Safety Systems overview: chapter I, [in:] Safety Engineering: Selected Aspects.New York: Iglobal Writer Inc., Pro Pomerania Foundation Poland, 2014.
13. Marcinek M, Dworzecki J, Technical Aspects of use of Selected Specialist Equipment Intended for Road-Side Rescuing, 1. Edition. New York: Iglobal Writer Inc., Pro Pomerania Foundation Poland, 2015.
14. Marcinek M, Euro-NCAP a simulácie nárazov automobilov — crashtesty, [in:] Rozvoj teórie bezpečnostných rizík a tvorba krízových scenárov [elektronický zdroj]. Zborník z konferencie s medzinárodnou účasťou, ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave, 5.12.2013. Akadémia Policajného zboru v Bratislave. Bratislava, 2014.
15. Marcinek M, Linka tiesňového volania eCall v podmienkach Slovenskej republiky. The emergency line eCall in the Slovak Republic, [in:] Bezpečnostné fórum 2015. I. Zväzok: zborník vedeckých prác. Banská Bystrica, 2015.
16. Marcinek M, Simulation of crisis situations of the national and international crisis management as a support for crisis managers' education, [in:] Nehody s hromadným postihnutím osôb. International Congress. Žilina, 2011.
17. The EU legislation in the Directive 2012/36/EU.

***About the Author***

***Milan Marcinek**, Ing, PhD. has been a lecturer at the Department of Public Administration and Crisis Management at the Police Academy in Bratislava since 2009. He has been the author and coauthor of several academic publications, exercises books, studies, articles and research projects in Slovakia and abroad. He has over 20-year experience in the field of security and protection. He is a holder of various certificates and attestations as a specialist and crisis manager in Slovakia and abroad. E-mail:*

***Streszczenie.** Inteligentne systemy transportowe wdrażają inteligentną technologię do infrastruktury transportu cywilnego. Nowoczesne usługi są uzależnione od wykorzystania systemów informatycznych. Bezpieczeństwo cybernetyczne odgrywa ważną rolę w ciągłym rozwoju technologii informatycznych. Wzmocnienie bezpieczeństwa cybernetycznego i ochrona krytycznej infrastruktury informatycznej mają zasadnicze znaczenie dla bezpieczeństwa każdego kraju. Obecnie pojazdy są wyposażone w elektroniczne systemy zabezpieczeń, które w razie wypadku automatycznie wzywają operatora pogotowia ratunkowego. Ten system bezpieczeństwa łączy w sobie różne technologie w celu zapewnienia bezpieczeństwa pojazdu. W przypadku utraty przytomności, system informuje ratowników o miejscu wypadku. Docierają oni na miejsce wypadku w ciągu kilku minut. Wprowadzenie tego systemu w pojazdach wynika z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/758 z dnia 29 kwietnia 2015 r. w sprawie wymogów dotyczących homologacji w odniesieniu do wdrożenia pokładowego systemu eCall 112 i zmieniającego dyrektywę 2007/46/WE. Niemniej jednak istnieje obawa, że takie powiązanie samochodów z ich użytkownikami może narazić ich na ryzyko związane z zagrożeniami internetowymi. Postęp technologiczny w zakresie bezpieczeństwa naszych pojazdów spowodował pojawienie się możliwości niewłaściwego wykorzystania danych dotyczących pojazdów. Zagrożenia elektroniczne stały się głównymi zagrożeniami podczas wdrażania e-usług w przestrzeni społecznej XXI wieku.*

***Zusammenfassung.** Intelligente Transportsysteme implementieren intelligente Technologie in die zivile Verkehrsinfrastruktur. Moderne Dienstleistungen sind auf den Einsatz von Informationssystemen angewiesen. Cybersicherheit spielt eine wichtige Rolle bei der kontinuierlichen Weiterentwicklung der Informationstechnologien. Die Stärkung der Cybersicherheit und der Schutz kritischer Informationsinfrastrukturen sind für die Sicherheit eines jeden Landes unerlässlich. Derzeit sind die Fahrzeuge mit elektronischen Sicherheitssystemen ausgestattet, die im Falle eines Unfalls automatisch den Notdienstbetreiber anrufen. Dieses Sicherheitssystem kombiniert verschiedene Technologien, um die Fahrzeugsicherheit zu gewährleisten. Im Falle einer Bewusstlosigkeit informiert das System die Retter über den Unfallort. Sie treffen innerhalb weniger Minuten an der Unfallstelle ein. Die Einführung dieses Systems in Fahrzeugen ergibt sich aus der Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über die Typgenehmigungsanforderungen für die Umsetzung des bordeigenen eCall112-Systems und zur Änderung der Richtlinie 2007/46/EG (im Folgenden „Verordnung (EU) 2015/758'). Es besteht jedoch die Befürchtung, dass eine solche Verbindung zwischen Autos und ihren Nutzern die Risiken im Zusammenhang mit Internet-Bedrohungen aussetzen könnte. Der technologische Fortschritt in der Sicherheit unserer Fahrzeuge hat dazu geführt, dass ein Missbrauch von Fahrzeugdaten möglich ist. Im Gegensatz dazu sind elektronische Bedrohungen bei der Einführung von E-Services in der Gesellschaft des 21. Jahrhunderts zu einer großen Gefahr geworden.*

***Резюме.** Интеллектуальные транспортные системы внедряют интеллектуальные технологии в гражданскую транспортную инфраструктуру. Современные услуги зависят от использования информационных систем. Кибербезопасность играет важную роль в постоянном развитии информационных технологий. Укрепление кибербезопасности и защита важнейшей информационной инфраструктуры имеют огромное значение для безопасности каждой страны. Сегодня автотранспорт оборудован электронными системами безопасности, которые автоматически в случае возниконвения ДТП вызывают диспетчера скорой помощи. Эта система безопасности объединяет различные технологии для обеспечения безопасности транспортного средства. В случае потери сознания, система информирует о месте аварии спасателей, которые прибывают на место происшествия в течение нескольких минут. Внедрение этой системы в транспортных средствах является результатом принятия Европейским парламентом*

*и Советом Регламента (ЕС) 2015/758 от 29 апреля 2015 года о стандартах сертификации для установки бортовой системы eCall 112 и о внесении поправок в Директиву 2007/46/ЕС. Тем не менее, существует опасение, что это может привести к тому, что данные о автомобилях и их владельцах будут подвергаться потенциальным рискам, связанным с онлайновыми угрозами. Научные разработки в области безопасности наших автомобилей также предполагают возможность незаконного использования данных о транспортном средстве. Оказывается, что э-угрозы стали ведущими видами опасности при внедрении э-услуг в общественном пространстве 21 века.*