Supplier Cybersecurity Risk Assessment Methodology

Albena Tzoneva and Borislav Stoyanov

Chernorizets Hrabar Free University of Varna, Varna 9007, Bulgaria

albenatz@gmail.com, borislav.stoyanov@vfu.bg

Abstract. Supplier cybersecurity risk has increased significantly with the galloping introduction of new mobility trends in vehicle technologies and the emergence of fast to market providers of electrical components hardware. The risk for OEMs (Original Equipment Manufacturer) is compounded based on the tiered structure of the automotive supply chain. The global nature of the supply chain additionally exacerbates the issue due to local state policies and requirements. Lack of common standards further elevates the risk level. The demand for supplier risk assessment springs from the automotive manufacturers mission to provide safe and secure transportation. Their responsibility in safeguarding personal data and human lives is the utmost driver behind making supplier decisions. The demand lies in the fundamental cybersecurity industry asks for a reliable tool to assess risk level and make well-grounded business decisions.

The objective of this paper is to provide a methodology for assessing third party cybersecurity risk on a component, sub-system, system, and enterprise levels. This methodology will deliver the following improvements: assess status with a live, reconfigurable model; provide the dollar amount for a particular risk level; feed into common requirements and set future product requirements; define company policies; -develop risk mitigation strategies; generate synergies between connected vehicle ecosystems and smart cities, and provide flexibility for a modular approach with interdependencies between modules.

Keywords: Risk, Automotive, Cybersecurity.

1 Supplier risk assessment demand

The demand for supplier risk assessment springs from the automotive manufacturers mission to provide safe and secure transportation. Their responsibility in safeguarding personal data and human lives is the utmost driver behind making supplier decisions. The demand lies in the following fundamental cybersecurity industry asks.

A reliable tool to assess risk level and make well-grounded business decisions is in great demand by top level executives. High level management is responsible for the safety and security of customers. Strategic decisions can be facilitated by a risk assessment at the initiation of a project. Whether to produce a product or

provide a service in house vs. outsourcing can be justified by assessing the risk and implications to the company. Corporate financial losses can be detrimental if this responsibility is not fulfilled. Company image may be destroyed leading to devaluation of the company stock and possible bankruptcy. Lawsuits may debilitate operations and the bottom line with millions of dollars spent on litigation.

A risk assessment tool would play a significant role in preventing implications on a national level. If products are a part of a system which is the case with connected vehicles, effects could be far reaching and of a large proportion. They can easily propagate to a national disaster. A risk assessment tool can serve as a competitive advantage. A proof of lesser risk exposure would bring more customers and contracts. It will help OEMs build a reliable supplier base that allows for in time delivery and quick to market execution. An assessment tool would indicate what measures are lacking and where budget allocation needs to go. Mitigating risk has a price and budget allocation decisions need to be founded on data. New mobility ecosystem brings significant complexity. Building a successful depth in defense strategy against cyber security threats requires tools to assess vulnerabilities and provide security status of the whole ecosystem tree. Building the future smart cities will be reliant on methods and tools already proven in assessing risk in the connected vehicle ecosystem.

1.1 Mobility landscape

The automotive industry will be facing sweeping changes. Vast shifts will be necessary to enable the new mobility ecosystem. It has already incorporated many efficiencies afforded by the internet and computation.

Navigant Research predicts that 75% of vehicles sold in 2035 will have some sort of autonomous capability [1]. ADAS systems (Advanced driver assistance systems) are already taking stage in numerous vehicles, paving the way for fully autonomous driving. The cars are becoming multifunction interactive platforms, opening avenues to the interconnected world. For example, technology like the space-astronaut robot Kirobo, developed by the University of Tokyo, Robo Garage, and Toyota, could provide both automated driving and interactive communication in the personal transportation systems of the future [2].

Today we get a preview of the challenges that mobility management will pose to enterprises and infrastructure. Ride hailing companies orchestrate networks connecting those offering the service with the ones requiring it. New business model solutions such as Uber, Lyft, and Maven, have come to gain significant market share. They put to test the traditional vehicle ownership and provide alternatives for congested urban areas.

As autonomous vehicles are gaining ground, companies will further widen the integrated set of mobility options and services they are offering. They will

connect the self-driving cars with other modes of transportation to provide customers with improved services of seamless intermodal transportation. They will strive to ensure easy access, smooth payment process and rich entertainment experience. The mobility system will have to provide customers with trip planning, route adjustment, seamless connectivity to infrastructure and vendors. Social networks would take on an expanded role by suggesting customer preferences to make the journey most pleasurable. These functionalities will have to be handled by sophisticated electronic components and software applications.

Technology is the driving force behind this wide scope change. Technology companies will have to adapt to creating and operating larger and more complex information networks. Artificial intelligence and deep learning [3] will minimize human error and facilitate management of huge amounts of data. These companies will enable new environments and create the landscape of new digital communities. The security aspect of the software these companies will provide is of paramount importance for their viability. Security must be embedded in every stage of the product development process both in hardware devices and the software algorithms. Suppliers are facing a dynamic, fast shift to fully digital connectivity with seamless flow of data between cars, infrastructure, and mobile devices.

The connected vehicle ecosystem will bring the greatest challenges to cybersecurity specialists. Today the deepest fears and concerns for cyberattacks are related to in-vehicle systems. These concerns would most likely not be the prevalent ones we head into the autonomous future. The extent of economic and human life damages if a malicious attack were successful on connected vehicles could be of catastrophic proportion. The connected world of computing is prevalent in our modern society with connected vehicles as part of this ecosystem. Connectivity between devices and wearables, IoT sensors, smartphones, tablets, laptops, personal robotics, smart cars, and smart cities has become the new paradigm. Connected world research firm GSMA estimates that 100% of cars will be connected to a cellular network by 2025 [2].

Connected cars are storming into our everyday life loaded with new technologies and devices that perform the new functions. It brings along computing demand challenges. The devices already installed in the car and the infrastructure around are becoming platforms for enhanced safety features, advertising, entertainment, and social networking. They also become attack vectors for malicious intruders and need to be protected.

1.2 Mobility management

Supplier sourcing of materials and parts, building customized automobiles, integration with insurance, regulatory, and financial services, will require enhanced

level component intelligent systems for connectivity and data exchange. With it come the challenges of securing the data flow, protecting the information, and not allowing malicious disruptions.

Content component suppliers, service providers, advertisers, entertainment, and social media industries will use this new forum to reach the customers and provide customized services that are immersive and interactive. The in-vehicle transit experience will bring new challenges and opportunities. Automobile sensors and personal devices will be transferring greater and greater data loads. Their data collection will be producing information about customer experiences and directing targeted advertising and service options.

Supplier community will be providing components to meet the automotive as well as infrastructure demands. Intermodal transportation will be made possible by integrated computer technology systems. As society is moving to a more integrated set of mobility services, the digital infrastructure supporting the physical infrastructure will have a critical role. Roads, waterways, bridges, parking structures will again take their vital part in this interconnected environment. Cloud computing, Internet of Things, Operating systems, and Cybersecurity are growing in importance and will be of paramount significance for the safety and security of people.

Cybersecurity and electronic device suppliers will be challenged with the scope and complexity of these systems. The magnitude of these changes requires adequate foresight and preparation to ensure the systems are protected for integrity, confidentiality, and availability. The security risk would involve large systems and can spread at higher speed than ever. The consequences can be detrimental and encompass not just individuals but states and the global community.

Technology companies are the top contributors of patents in the automotive space and not the automotive companies themselves. With the acceleration in automated driving technologies, several automotive companies have entered into joint ventures with technology companies to develop self-driving cars like General Motors and Cruise, Ford, and Argo AI. BMW and Daimler formed a partnership to develop autonomous vehicles.

Suppliers on the other hand are forming a unique network of highly specialized providers. The complex requirements and ever shifting market demand force these companies to go fast and invent new ways to make features functional. Highest demand suppliers are in the following areas: Biometrics, ADAS and Autonomous, Infotainment, and Telematics.

1.3 IoT (Internet of Things)

IoT would multiply the effect of a malicious intrusion to a devastating widespread catastrophe. IoT is adding to the complexity of the problem. Communications

over the wireless medium pose security threats that are yet to be fully understood. With the advent of sophisticated cognitive radios, wireless devices, drones, small satellites, driverless cars, and wireless healthcare devices, security threats to wireless mobile communications systems are rapidly increasing. As 5G and other newly developed systems are deployed, a new wave of protective methods and policies are needed. The level of complexity of wireless systems creates a wider attach surface with multiple potential points of failure. A workshop was held by the Networking and Information Technology Research and Development (NITRD) Program's Wireless Spectrum Research and Development (WSRD) Interagency Working Group (IWG), which is co-chaired by the National Science Foundation (NSF) and the National Telecommunications and Information Administration (NTIA) - Security from a Wireless Spectrum Perspective: Technology Innovation and Policy Research Needs, on September 13, 2018, in Washington, DC [4]. The goal was to create connections and contacts between Federal agencies and between public and academic specialists to talk about wireless mobile devices cybersecurity. There were thirty-five workshop participants who represented stakeholders with a vested interest in the topic of research.

The damage magnitude inflicted on the connected ecosystem is much greater than if it were localized to one individual vehicle of the ecosystem. The lure of penetrating the ecosystem is ever so high which makes targeting human weaknesses more prevalent. Social engineering methods could potentially be exploited for easier entry into the car system during diagnostics or OTA (Over the Air) updates. Consequences then would be spread among the wider fleet. The work force performing these tasks would be a lucrative group for malicious hackers to study them and employ methods to beguile them.

Another challenge of significant magnitude is the lack of knowledge and insufficient training of employees and personal users with these new challenging components and technologies. Social engineering techniques such as shoulder surfing, impersonation, false alarm, just to name a few, can occur in a shared vehicle. This vehicle, if penetrated, can become a node spreading malware or extracting personal information. It can become the originator of a system wide havoc and malfunction.

The connected world of computing is prevalent in our modern society with connected vehicles as part of this ecosystem. Connectivity between devices and wearables, IoT sensors, smartphones, tablets, laptops, personal robotics, smart cars, and smart cities has become the new paradigm. The devices already installed in the car and the infrastructure around are becoming platforms for enhanced safety features, advertising, entertainment, and social networking. They also become attack vectors for malicious intruders and need to be protected.

A complex web of suppliers, manufacturers, and service providers has emerged due to the interconnection of IoT systems and infrastructure. IoT is an

intricate and dynamic ecosystem. It includes numerous hardware components and systems in various electric architecture layouts. As more and more features are being introduced to meet customer demands, the complexity of these systems has escalated to an unprecedented level.

IoT supply chain has a paramount influence on security. The SCRM (supply chain risk management) for the information and communication technology is essential in conquering the challenges stemming from the IoT wide-spread dominance. Although it does act as a useful guideline, it may not be sufficient to tackle the more complex nature of IoT networks and the associated supply chain [5].

The various ownership and decentralized control are another point of concern. A network administrator over the complete device ecosystem does not exist and therefore there is limited control over the network. The administrators may not even have a complete understanding of all the connected devices and their inter-operability.

The IoT ecosystem and its security is significantly different from the established ICS (information and communication systems). There are many different parties participating in a system with no regulations. Services are mainly interconnected thus opening the door for multitude of specific applications. There is no industry standard to use a particular protocol for the IoT ecosystem. This complicates successfully embedding security as part of the code. The connectivity nature of the IoT creates security challenges and new attack vectors. There are some significant differences between IoT systems and the established information systems. The IoT devices interact with the physical world by using actuation functionality as opposed to conventional mobile and computing systems. Consequences, compared to ICT systems, may be detrimental to human safety, make equipment inoperable, or cause operational interruptions. The complete access and management functionalities may not be built into the IoT devices [5]. These devices are mainly constructed as low power and with limited data processing capabilities. The security and privacy specifications for operating IoT devices may differ significantly from the mainstream ICT systems in the way they handle authentication and access control security.

2 Problem statement – supplier cybersecurity issues

Risks in the automotive software supply chain as well as those associated with hardware components have escalated with the fast advent of autonomous mobility and the new connectivity paradigm. Automotive manufacturers procure electronic components from a supply chain of hundreds of vendors. The most pronounced risk of all is whether the tier supplier has built-in cybersecurity protection appropriately into their products. When OEMs put together the specifications, the level of the requirements is generic enough so that suppliers can innovate. In addition, not all constraints are known and understood at the time the supplier

is brought on board. When innovation and new concept development is taking place, requirements are generated on the go. That makes it hard to align with overall industry recommendations and procedures as it is not always possible to follow those. It is even harder to capture those requirements as lessons learnt after the product development phase. Competitive pressures further complicate any sharing or communization between suppliers. In addition, the timeframe of getting a component to market is incredibly compressed and does not follow normal mature product progression.

Assessing the compound risk of various supply chain vendors is one of the pressing and compelling challenges with automotive component and software providers. Best practice for suppliers to minimize risk would be to follow a structured approach according to industry recommendations. Cybersecurity must be embedded in the product development life cycle from the very initiation. That is not always the case and there is no consistency among suppliers in doing that. The complexity comes from the large number of tiered suppliers and compressed timing.

A Study of Automotive Industry Cybersecurity Practices, Supply Chain and Third-Party Component Challenges was performed jointly commissioned by SAE (Society of Automotive Engineers) and Synopsys [6]. Seventy-three (73%) percent of respondents are very concerned about the cybersecurity posture of automotive technologies supplied by third parties (Fig 1). Sixty-eight (68%) percent are also very concerned about the cybersecurity posture of the industry as a whole. Only forty-four (44%) percent say their organizations impose cybersecurity requirements for products provided by upstream suppliers [6].

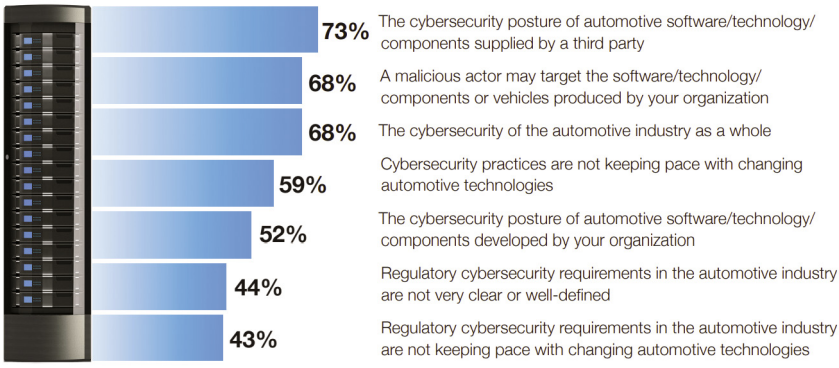

Fig. 1. SAE, Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices [6].

Secure coding training has not been brought up in priority. Only thirty-three (33%) percent of participants state that their companies train developers to practice secure coding. The disparate manner in which new technology devices are

developed opens suppliers to vulnerabilities. Quality issues and cybersecurity attack vectors are often the result of the integration of 3rd party components, software, and applications.

Survey results also revealed the supplier's exposure to risk. Nineteen (19%) percent of respondents said they did not perform sufficient security testing during the creation of requirements and the design phase, and only twenty-eight (28%) percent said that development and testing was rigorously enforced [6]. It is notable that testing and validation are performed too late in the process. For the majority of participants, testing happens after product is released, which can incur massive increase cost to the organization. The goal should be to enable suppliers in their security and vulnerability process improvements and do that from the initiation of a product development cycle. If we enabled suppliers to improve cyber security testing and vulnerability management early through the supply chain, we would get a much better result [6].

Cybersecurity should not be looked upon as a burdensome overhead and addressed at the end of the product cycle. Instead, it should become a constituent in every stage of the engineering process creation and be a guiding principle for every department that is involved. Automotive companies can employ numerous solutions from other industries by following their example of best practices and standards implementation. This rigorous approach to cybersecurity is vital to achieve enhanced safety while ensuring security, quality, and rapid time to market [6], [7], [8], [9], [10].

3 Supplier risk assessment methodology composition

The base methodology used is the FAIR (Factor Analysis of Information Risk) approach. It provides a solid foundation for risk assessment and quantification of results and a bottom-up approach of managing risk and operational supplier readiness [11]. The methodology comprises of steps that allow mapping the attributes on a component level, sub-system level, and finally on a system or enterprise level. This approach addresses supplier issues and leads to the development of policies and procedures to control the risks.

A risk assessment methodology is essential in defining the weaknesses in the supplier process. The issues laid out can be addressed and mitigated by a concerted effort by the most prominent industry suppliers to implement stringent common processes in the early phases of product development. It will include collaboratively working with suppliers to identify and classify the weaknesses in the engineering design, define security requirements along with the technical requirements, and institute policies. In Fig. 2, it is schematically shown how can be chosen to procure several components based on their security posture and competitive characteristics.

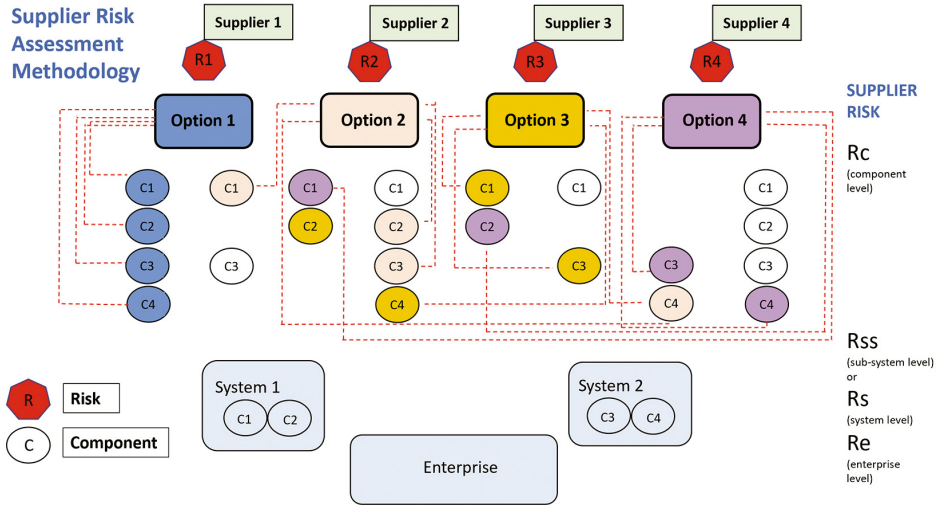

Fig. 2. Supplier choice to procure components based on cybersecurity posture.

The risk assessment building blocks consist of establishing the strategic and procedural approach of a supplier to cybersecurity. It should comprehend process steps such as forming a cross functional team, identifying risks and their attributes, filtering, assessing, prioritizing risks, analyzing results, and constructing an actionable mitigation strategy. As the company Vector laid it out, the V model is now in wide use among the automotive communities. The V model calls for a coordinated process between functional safety and cybersecurity. Starting with item definition, then threat and risk assessment in both fields, followed by defining of the cybersecurity and safety goals, concept, and requirements. The next stage starts with verification on a component level, then on a system level, followed by validation, pen testing, approval for release, and finally production, maintenance, and decommissioning.

A cybersecurity assessment methodology should verify there is a management process in place to ensure cybersecurity is part of the fabric of the product development cycle. It should acknowledge if there is a cybersecurity development team, plans developed, requirements followed, tests performed, reports produced. This approach proves a structured cybersecurity plan in place and acknowledges the degree of cybersecurity achieved by the supplier.

Suppliers should demonstrate their continuous cybersecurity activities such as cybersecurity monitoring, event assessment, and vulnerability analysis throughout the products development phases, starting with the concept phase, then the product development phase, followed by cybersecurity validation, production, and operations maintenance, all the way to decommissioning.

The methodology acknowledges a systemic Threat and Risk Assessment (TARA) activities of the supplier. They should include asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, risk determination, and mitigation strategy. This approach is part of the new standard ISO/SAE 21434. Assigning a risk value and attack feasibility rating should be at the basis of the cybersecurity supplier assessment as recommended by this standard. CAL is the risk value of CAL1 through CAL4, Attack Feasibility Rating would range from Very Low to High, resulting in an impact rating of Negligible, Moderate, Major, or Severe. Adequate process measures need to be in place to respond to those risks to ensure minimizing the time, financial and image damage to the organization.

The proposed methodology assigns dollar value to the supplier risk level and facilitates executive ranks in making adequate investment decisions. The dollar value can be calculated on the basis of tangible and intangible factors. Lost time of production or delivery is one factor that can be quantified. This factor can be assigned dollar amount based on historical quality standards adherence data for the company. On a functional level, Monte Carlo analysis can be utilized to simulate attack vectors and the loss function of those attacks.

The risk assessment methodology relies on historical data, yet breaches are not 100% predictable. Malicious agents continuously change their practices and come up with new ways to attack. Depth in defense, employing several measures and adhering to a rigorous process is the best approach to successful cybersecurity management. Functional safety, cybersecurity, and homologation aspects demonstrated in a risk assessment model would be a proof of supplier process maturity and consequently be reflected in the supplier cybersecurity rating.

Cybersecurity risk should not be looked at in isolation. Recommendations from the latest draft of ISO/SAE 21434 standard, along with ISO 26262, ISO 21448, and SAE J3061 need to be reflected in the assessment process. On an enterprise level, a high- level risk map needs to be created to outline the threat landscape. This approach should include identification and analysis of the sources of attack and plotting them on the map of acceptable and unacceptable risks. The risk map needs to be looked at holistically, comprehending external events along with cybersecurity threats and their interdependencies. In the recent years, cybersecurity threats have moved from acceptable risk to high-risk quadrant of the risk scale. This calls for enforced measures to detect and mitigate risks. On an organizational level, management needs to determine the tolerable level of risks they are willing to take. This proposed methodology will facilitate converting the level of risk into the dollar amount a company can tolerate and establish a risk curve of loss exceedance. This curve will reflect the risk suppliers are bringing to the organization from outside. Risk should be estimated as a compound value, either complementary or independent, depending on the characteristics of the

organization. Some intangible values can also be considered as part of the overall risk. Trust, established between a company and a supplier, can participate in the equation as a Trust Value. On an enterprise level, the Loss Exceedance probability would translate into a dollar amount that senior management can determine if tolerable or not.

The compound risk can also be estimated by breaking down the cybersecurity services into four main areas to further establish where the greatest vulnerability impact may lie. These areas are Edge Security like secure gateways, Vehicle Computer Security of systems and connectivity, Access and Communication Security like authentication, or Services Security like threat intelligence and emergency responses. These areas can be separately rated and allocated a security risk. This approach can help an organization enhance processes and mitigation strategies for a particular security partition as well as focus more resources to it.

4 Conclusion

The proposed risk assessment methodology addresses the burning issues associated with supply chain management of cybersecurity risk. The automotive industry is going through a dramatic change on its way of embracing automated driving, IoT, cloud data, and artificial intelligence. The new paradigms require in depth analysis of risk. The multilayer supply chain exhibits complex issues stemming from various levels of technological development, internal procedures and processes, market demands, and cost structure. OEMs will need to make informed decisions on which suppliers to bring on board and how reliable these suppliers are to deliver just in time quality products.

The innovative approach of the proposed risk assessment methodology allows OEMs to calculate compound cybersecurity risk at all tiers, then assess this compound risk as part of the overall enterprise risk. Its significance lies in its applicability to industry demands. Requirements are derived from the very initiation of the product development process. These requirements are then embedded in the risk assessment tool and tracked periodically throughout the life of the product.

The challenges associated with this methodology lie in the quality of the historic risk data used for assessment, the truthfulness of supplier disclosure, and the unpredictability of future threats. These three aspects need to be further explored, analyzed, and structured as a reliable basis for evaluation.

Industry level awareness of the importance of cybersecurity posture are laying the ground for supplier inclusiveness. It is in the interest of individual vendors to demonstrate cybersecurity posture in order to be considered by OEMs. Failure of responsibility, although generally allotted to OEMs, has on many occasions been attributed to an individual supplier, leading to an image detriment as well as

severe consequences such as bankruptcy. Brining suppliers to a common level of cybersecurity requirements and disclosure is of paramount importance for both OEM and supplier product acceptance and organizational longevity. Guided by the common goal of ensuring customer safety and security, OEMs and suppliers can address cybersecurity issues as a coalition, embracing a common risk assessment methodology as the one proposed in this paper.

The value of this proposal can be summarized as providing a unique methodology that evaluates risk of a supplier tier tree. The methodology is essential in defining the weaknesses in the supplier process. It offers a structure that can be applied to suppliers on a global scale. OEMs can require the same set of requirements and procedures when quoting a commodity to several suppliers. Awareness of the potential financial impact on the organization is a foundation for sound business decisions.

References

1. Navigant Research, http://smarttransport.solutions/2018/05/29/consumer-impacts/he Automobile, last accessed 2021/03/30.
2. Swan, M.: Connected Car: Quantified Self Becomes Quantified Car. Journal of Sensor and Actuator Networks 4(1), 2-29 (2015).
3. Tsankova, P., Momcheva, G.: Sentiment detection with FedMD: Federated learning via model distillation. In: Dimitrov, V., Georgiev, V. (eds.) ISGT 2020, CEUR Workshop Proceedings, vol. 2656, pp. 236–247 (2020).
4. EInfochips Homepage, https://www.einfochips.com/blog/role-of-edge-computing-in-connected-and-autonomous-vehicles/, last accessed 2021/03/30.
5. Farooq, M. and Zhu, Q.: IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. arXiv:1908.07828v1 [cs.CR], (2019).
6. SAE Homepage, https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf, last accessed 2021/03/30.
7. Spasova, V.: Software Quality ISO Standards. In: 4th International Proceedings on International Congress Mechanical Engineering Technologies MT'04, pp. 1–6. Scientific Notices of the Scientific and Technical Union of Mechanical Engineering: Collection of Reports, Sofia, Bulgaria (2004).
8. Bakardjieva, T., Gercheva, G.: Knowledge management and e-learning - An agent-based approach. World Academy of Science, Engineering and Technology 76, 663–666 (2011).
9. Spasova, V.: Standards for Quality Management in the Software Business, University Publishing House of VFU "Chernorizets Hrabar", Varna, Bulgaria (2019).
10. Gradinarova, B., Bakardjieva, T., Gradinarova, M.: Some aspects of application of software agents in information retrieval in virtual-based educational environments. IFIP International Federation for Information Processing 210, 315–319 (2006).
11. Jones, J.: An introduction to factor analysis of information risk (FAIR). Norwich Journal of Information Assurance 2(1), 67 (2006).