THE CATEGORIZATION AND INFORMATION TECHNOLOGY SECURITY OF AUTOMATED VEHICLES

Attila Albini*, Dániel Tokody and Zoltán Rajnai

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.4
Regular article

Received: 23rd March 2018.
Accepted: 31st August 2018.

ABSTRACT

In addition to mechanical changes automation plays an increasingly important role in the evolution of vehicles. The development of autonomous automobiles is the driving force behind the evolution of the information technology (IT) infrastructure in vehicles. Self-reliance requires more and more automation. Enhanced level of automation requires increased operational reliability. This will also resulting an increased level of safety in the cyberspace of vehicles. Endangering cyberspace can also come from a threat of natural and human origin. IT security is the protection against threats of natural origin. It includes protection against natural and technological impacts. For these reasons, it is important to increase IT security in the IT infrastructure of vehicles. This article examines IT security increasing system building technologies from the aspect of the overall IT infrastructure of vehicles. These technologies enable faster processing, increased availability and greater flexibility. The study requires the creation of a new vehicle automation categorization. Technologies are examined according to these new categories and the functional layers of the general IT infrastructure.

KEY WORDS

IT infrastructure, IT security, increase, technology, vehicle

CLASSIFICATION

ACM: C.0, K.6.5
JEL: O39, R41

*Corresponding author, η: attila.albini@gmail.com; +3630 526 7757;
OE-BDI office, Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

For a long time, technological progress was a top priority in vehicle development. Shortly afterwards solutions appeared that affected the integrity of the consignment. This becomes more important for the transport of special items, living things, humans and dangerous materials. The following viewpoints were to enhance the comfort and driving experience. Later the environmental impact of vehicles became detectable. As a further problem, the amount of raw materials used to produce fuel is finite. Alternative solutions for fuel, engines and power transmission have appeared to maintain the environment and technology. The electronics and ICT (info-communication technology) help the development of sustainable technologies [1, 2]. However the human factor is the biggest risk in the safety of vehicles. This risk is equally visible in the design, manufacturing, maintenance, driving of the vehicle and in the organization of the traffic. Sustainability requires the risks be treated. Automation reduces the human factor [2, 3]. The use of electronic and information technologies is the basis of automation. The use of ICT makes the question of cyber security important. IT security contains the protection of cyberspace against natural impacts and technological failures [4, 5].

This article explores IT security enhancing technologies from the aspect of IT infrastructure according to the vehicle automation and the automation of traffic organization. The analysis of IT security enhancing technologies follow the logic of the solutions used in the construction of ICT clouds. These technologies enable faster processing, increased availability and greater flexibility. The examination reveals that it is worth introducing wider categorization of vehicles and traffic management systems. Therefore, the study also proposes a new categorization. The IT security increasing technologies are analyzed according to these new categories and the IT infrastructure layers.

TECHNOLOGIES THAT INCREASE INFORMATION TECHNOLOGY SECURITY

The need for increasing IT security has gradually emerged in the development of information technology. This primarily means independent operation from natural and technological impacts. Secondly it means that the management of resources is flexible. The cloud systems have developed along a similar criteria system. Thus, analysis of building technologies used in clouds can help in the examination.

The first major problem of IT systems was to shorten the processing response time. The answer was the grid technology. Later on to increase the availability became the main consideration. The solution is the cluster technology. Virtualization is the answer to the problem of flexible resource grouping. System protection against major impacts has led to the emergence of the disaster-tolerant solutions based on the split technology [4].

The purpose of grid technology is to shorten processing time. Performing tasks is autocratic. Multiple processing points perform a particular task at a time. Each processing point only performs a subtask that assigned by the controller component. If a processing point error occurs, the subtask is redistributed to another processing point. There is no need for fast communication between the components. Heterogeneous devices can be included in the system [4].

Cluster technology aims to increase availability. Performing tasks is based on a democratic principle. There are several processing points but one task is performed by only one processing point. If a processing point error occurs, another processing point takes over its role. The change of role is very fast and is based on a joint decision of the processing points. This mechanism only works with fast communication. This technology requires homogeneous processing points [4].

The primary purpose of virtualization is to ensure regrouping of resources. To achieve this possibility the resources of the virtualized structure layer are covered and are presented only in the required quantity and quality to the upper layer. This will ensure that the system resources are distributed flexibly. The goal of split technology is replicating consistent system states to long distance. This will allow the system to restart in a remote place in case of a critical impact [4].

Cloud systems could be created by using these technologies. These technologies serve to increase IT security. So the IT security of IT infrastructures should be considered in accordance to the principles of these technologies.

GENERAL INFORMATION TECHNOLOGY INFRASTRUCTURE

The modeling of the general IT infrastructure should be built on philosophical basis for the sake of uniform analysis. The proposed aspects are the structural and functional division of the infrastructure. Infrastructure layers can be identified on the basis of structural layers, which is consistent with human abstraction levels. Functional divisions can be defined by identifying the equivalence with the abstract categories of human thinking [6].

Structural layers can be considered as the vertical segments of the system. The bottom layer is the fundamental layer. It contains the energy resource management. This layer corresponds to the natural energy environment of man. The second layer is the hardware layer, which generates the physical IT resources. This layer is analogous to man's material environment. Next layer is the virtual layer. This generates the logical IT resources and corresponds to human modeling. The operation layer is the implementation of the main features. This layer corresponds to the operating layer of the model. The management layer is the top layer, which provides the operation of the system in time [6].

Horizontal division may be the functional division. These are information paradigm elements based on abstract categories. These should be supplemented with components that express change. Elements of the horizontal structure include storage, transformation, transmission, statogenesis (non-organizational changes) and morphogenesis (organizational changes) [6].

AUTOMATION LEVELS OF VEHICLES

Classification of vehicle automation is currently based on the automation of the vehicle's driving function [3]. Because of the impact of IT security technologies, it is important to take into account all related components of the system and their problems. Therefore the categorization used so far is not enough. To identify new categories the abstract categories can help: thing, property, relation. In the aspect of vehicles these are the technical functions of the vehicle, the storage function of the vehicle and the movement of the vehicle. An expanded interpretation of the relation category requires the inclusion of the aspect of transport organizing. It corresponds to the control of the transporting. An example sentence for checking: “the vehicles took the consignments to the destination within the planned time”. In the criteria system of examination *the vehicle* is equivalent with the technical compliance, *consignment* is equivalent with the storage, *took* with the move, *destination* and *in time* with the time management and routing. Problems associated with the aspects are: storage, maintenance, driving, routing. The levels to be found for each problem can be the following:

- category S (storage) – (i) objects, (ii) living things and special objects, (iii) humans, (iv) hazardous material,
- category M (maintenance) – (i) traditional maintenance, that neither detects errors nor periodic maintenance automated. (ii) controlled maintenance, where proactive monitoring is performed but repair management and periodic maintenance are not automated,

(iii) with the exception of periodic maintenance the vehicle manages the errors automatically, (iv) fully automated, where the vehicle manages errors and periodic maintenance automatically,

- category D (driving) – (i) traditional driving. (ii) controlled driving, in which case a supervisor can take over the driving. (iii) fully automatic driving. (iv) convoy driving, where vehicles close to each other synchronize their movements,
- category R (routing) – (i) conventional static routing, (ii) dynamic on-line routing, (iii) dynamic routing with centralized control, (iv) dynamic central and community routing at the same time.

The new classification of automated vehicles can be defined by the SMDR categorization system. For example, the SMDR-3232 marking means that the vehicle delivers humans, has controlled maintenance, automated driving and dynamic routing. Table 1 shows the categorization.

Table 1. New categorization of automated vehicles.

Categories	**Category S**	**Category M**	**Category D**	**Category R**
Abstract category	Property	Thing	Relation	Control
Aspect of vehicle	Storage in vehicle	Technical operation	Moving the vehicle	Traffic control
Problem	**Storage**	**Maintenance**	**Driving**	**Routing**
Level 1	Objects	Traditional maintenance	Traditional driving	Static routing
Level 2	Creatures, special objects	Controlled maintenance	Controlled driving	Dynamic routing
Level 3	Humans	Periodic maintenance	Automatic driving	Central routing
Level 4	Hazardous material	Automatic maintenance	Convoy driving	Community routing

TECHNOLOGIES IN INFORMATION TECHNOLOGY INFRASTRUCTURE

IT security increasing technologies in the IT infrastructure of vehicles should be examined by the layers and the new categories.

It is worth minimizing the risk of all threats in the energy layer from S2, M3, D3, R3 levels. At least in vibration, water intrusion and thermal protection. In the power supply at least the cluster technology principle should be applied.

With regard to hardware devices the local processing should be ensured above M2 and D2 levels. Not self-contained sensor and actuator units should be used, but gridded processing units. This reduces the amount of data being transferred. In addition the big data effect occurs later in the central unit. This solution also allows for the redundant storage of data. This principle is in line with the principles of increasing the technical security of IoT devices [2]. For the internal communication of the vehicle on D3 and R3 levels the cluster principle should be used. For the external communication on D4 and R4 levels the gridded cluster principle should be used.

When processing data it is worth introducing virtualized service management. From a logical point of view it is necessary to separate the handling of the physical parameters and the parameters of the logic functions required for the operation of the vehicle. The relationships and dependencies of these two layers must be determined. This follows the principle of virtualized grid-cluster. Usage of this technology is recommended above the M2 and D2 levels. In addition it must be ensured that a given parameter can be defined in at least two different ways to ensure the redundant calculating.

The functions of the vehicle must be implemented in the operational layer. Artificial intelligence items should be used to make decisions because they can contain heuristic elements [7] and provide a quick method [8-10]. In category S it is necessary to allow the use of split technology for convenience and possible legal compliance. This will allow storing convenience functions and the law specific parameters in a vehicle-independent location. It makes the initial parameterization of the vehicles simple [5].

From R3 level, it is strongly recommended to use all that technologies in traffic management centers which help increase availability, ensure system integrity and data consistency. It is also recommended to use full scale management and disaster tolerant solutions.

CONCLUSIONS

The development of the ICT systems is becoming increasingly important in the development of vehicles. The level of automation is growing steadily [1-2]. Sustainability also requires increased security. Increasing security also requires increased security of IT infrastructure. This is a part of IT security [5]. In the case of vehicles, this primarily means safety against natural impacts and technological failures. Furthermore it means shorter processing time and more flexibility. The requirements of the IT cloud systems are similar. So the principle of inquiry is the same as principle of examining IT cloud building technologies [4-5].

The current definition of automation levels does not match the scope of the examination [3], so a new and more extensive automation categorization has been created. New categories are defined on the basis of abstract categories of human thinking and supplemented with statogenesis. These correspond to storage (S), maintenance (M), driving (D) and routing (R) problems. This was the basis for SMDR categorization. Each subcategory has four levels, depending on the degree of automation.

IT security increasing technologies in the IT infrastructure of vehicles have been examined in the layers of infrastructure [6] and the new categories. Proposals have been made to apply the principles of cloud building technologies and to use artificial intelligence [7-10]. It was found that the technologies used to enhance the features of vehicle systems functions is the same as the technologies used to increase the technical security of IoT devices [2]. Further expectation is that systems of traffic management centers created in the future should be like IT clouds.

ACKNOWLEDGEMENTS

The research presented in this article was carried out as part of the EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

REFERENCES

[1] Mester, G.; Pletl, S.; Pajor, G. and Jeges, Z.: *Flexible Planetary Gear Drives in Robotics*. Proceedings of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation. San Diego, pp.646-649, 1992, http://dx.doi.org/10.1109/IECON.1992.254556,

[2] Wolz, U.: *The required technologies for Automotive towards 2020*. The 20th Asia and South Pacific Design Automation Conference. IEEE, Chiba, p.1, 2015, http://dx.doi.org/10.1109/ASPDAC.2015.7058916,

[3] SAE International: *Automated Driving – Levels of driving automation are defined in new SAE International standard J3016*. https://cdn.oemoffhighway.com/files/base/acbm/ooh/document/2016/03/automated_driving.pdf, accessed 20th March 2018,

[4] Albini, A. and Rajnai, Z.: *Felhőelméleti fenntarthatóság adaptálása humán rendszerekre – Adapting cloud computing sustainability to human systems*. In Hungarian. Lépések a fenntarthatóság felé **22**(3), 17-19., 2017,

[5] Kovács, Z.: *Cloud Security in Terms of the Law Enforcement Agencies*. Hadmérnök **7**(1), 144-156, 2012,

[6] Albini, A.; Tokody, D. and Papp, J.: *IT Infrastruktúra Informatikai Biztonsági Aspektusai – IT Security Aspects of IT Infrastructure*. In Hungarian. Bánki Reports **1**(1), 11-16, 2018,

[7] Rotar, C. and Iantovics, L.B.: *Directed Evolution – A New Metaheuristic For Optimization*. Journal of Artificial Intelligence and Soft Computing Research 7(3), 183-200, 2017, http://dx.doi.org/10.1515/jaiscr-2017-0013,

[8] Rodic, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*. In: Pap, E., ed.: Intelligent Systems: Models and Applications. Topics in Intelligent Engineering and Informatics **3**. Springer Verlag, Berlin & Heidelberg, pp.115-134, 2013, http://dx.doi.org/10.1007/978-3-642-33959-2_7,

[9] Brassai, S.T.; Iantovics, L.B. and Enachescu, C.: *Optimization of Robotic Mobile Agent Navigation*. Studies in Informatics and Control **21**(4), 403-412, 2012, http://dx.doi.org/10.24846/v21i4y201206,

[10] Mester, G. and Rodic, A.: *Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments*. International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010.