SCIENCE & MILITARY

No 1 | Volume 17 | 2022

SCIENCE & MILITARY

The rationale for publishing this periodical by the Armed Forces Academy of General Milan Rastislav Štefánik is to enable the authors to publish their articles focused on particular scientific issues in the following areas: Military science, Natural Sciences, Engineering and Technology.

Original scientific articles will be published twice a year.

Editorial Board

Published by: Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic. IČO 37 910 337. Registered No: EV 2061/08. ISSN 1336-8885 (print). ISSN 2453-7632 (on-line).

Printed by: Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic. Order forms should be returned to the editorial office. Published biannually.

The subscription rate for one year is 7,30 €.

The journal Science & Military is included in following multiple databases: EBSCO. ProQuest Central: PQ Science Journals; PQ Military Collection; PQ Computing; PQ Telecommunications; Illustrata: Technology; Forthcoming Technology Research Database (TRD) full text packages.

Address of the editorial office

SCIENCE & MILITARY

Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Phone: +421-960-423065 Fax: +421- 044-55 222 47 E-mail: redakcia@aos.sk http://sm.aos.sk

DOI: https://doi.org/10.52651/sam.j.2022.1

SCIENCE & MILITARY

No 1 | Volume 17 | 2022

Dear readers,

Scientific communication is one of the essential prerequisites for global progress. Following Mark Walport, who once said that "science is not finished until it is communicated", the Science & Military's editorial board has been using the Digital Object Identifier (DOI) system since 2021 in order to promote the journal and its contents. The DOI system promotes authors' publications in the scientific world, encourages academic communication and contributes to sharing and spreading of knowledge and expertise. Today, the Science & Military is an open access journal supporting the Budapest Open Access Initiative (BOAI). The main objective of the open access movement is to provide free scientific information available to as many readers as possible. That is why the Science & Military journal is accessible online for free. Its readers can read, copy, print, download, refer to and use full texts of research papers for any legitimate purposes without the publisher's or authors' prior consent as long as they cite their sources. Open licenses, which provide online access, allow authors to retain their copyright. The Science & Military uses the Creative Commons - Attribution 4.0 license. By submitting their papers, authors grant their consent to the CC BY-ND 4.0 license.

Dear readers, let me briefly present the contents of this issue.

The first among the peer-reviewed articles in this issue is the article titled ***"Dependence of Military Bridge Length and Parameters Defining its Manufacturing Costs"*** *written by Peter Mako. This article explains graphical and functional dependence between the bridge length and the basic parameters which define manufacturing costs of the bridges.*

Among the articles in this issue, you can find the paper written by Andrej Fedák and Jozef Štulrajter titled ***"Evasion of Antivirus with the Help of Packers".*** *The article presents a very interesting and current topic of malware detection and provides an initial insight into the complex subject of antivirus protection. In this article, the internal components of AV programs and well-known packing techniques are riefly explained while, in addition, they are tested against each other.*

The following article written by Pavol Lukášik, Vladimír Kadlub and Jindřich Stehlík titled ***"Searching for the Causes of Abnormally Fast Degradation of Engine Oil in a Diesel Combustion Engine"*** *deals with the possible causes of some undesirable processes of engine oil degradation. The authors present the importance of engine oil analysis, giving a specific example. The presented research shows that a significant factor influencing the degradation of motor oil is, among other things, the time aspect. Furthermore, according to the authors, in the case of regular addition of additives to fuel, intensive cleaning processes can occur, which can affect the degradation of engine oil.*

In another paper titled ***"The Human Interface Device (HID) Attack on Android Lock Screen Non-Biometric Protections and Its Computational Complexity"****, the authors Sebastián Potocký and Jozef Štulrajter describe the hardware and software requirements for implementing a HID attack. The article contains examples of three non-biometric types of lock screen protection for an Android smartphone and their computational complexity. The paper also presents an overview of the time complexity of all types of Android lock screen protection.*

Military operations in the 21st century will be characterized by an increasing degree of command and control automation as well as the autonomy of robotic systems. The series of articles concludes with the paper titled ***"The Impact of Technological Changes on the Development of Military Leaders"*** *written by Jan Nohel, Zdeněk Flasar, Milan Podhorec and Bryan Pakula, in which the authors deal with possible directions of leadership development in future military operations. The authors describe the principles of leading people and the functions of leaders-commanders needed to perform these tasks.*

*The final article by Péter Boda and Tibor Kovács titled "****Methods for Determining the Risk Factors for Road Transit in Hungary"*** *presents and evaluates some of the procedures that can help to reduce the risk factors of road transport and reduce the severity of unexpected consequences.*

Dear readers, on my behalf and on the behalf of the editorial board, I would like to express my gratitude for your support and interest. I firmly believe that this issue will provide you with interesting information and inspiring ideas that will enrich your knowledge.

Brig. Gen. (ret.) Assoc. Prof. Eng. Boris ĎURKECH, CSc.
Chairman of the Editorial Board

Reviewers

Assoc. Prof. Dipl. Eng. Lubomír **BELAN**, PhD.	Armed Forces Academy of General M. R. Štefánik, Lipt. Mikuláš, SK
Brig.Gen.(ret.) Assoc Prof. Dipl. Eng. Boris **ĎURKECH**, PhD.	Armed Forces Academy of General M. R. Štefánik, Lipt. Mikuláš, SK
Col. (GS) Assoc. Prof. Dipl. Eng. Petr **FRANTIŠ**, Ph.D.	University of Defence, Brno, CZ
Col. Prof. Klára **SIPOS KECSKEMÉTHY**, PhD.	National University of Public Service, Budapest, HU
Assoc. Prof. Dipl. Eng. Jaroslav **ODROBIŇÁK**, PhD.	University of Žilina, SK
Assoc. Prof. Dipl. Eng. Marie **SEJKOROVÁ**, Ph.D.	University of Pardubice, CZ
Assoc. Prof. Dipl. Eng. Jiří **ŠTOLLER**, Ph.D.	University of Defence, Brno, CZ

DOI: https://doi.org/10.52651/sam.a.2022.1.5-13

DEPENDENCE OF MILITARY BRIDGE LENGTH AND PARAMETERS DEFINING ITS MANUFACTURING COSTS

Peter MAKO

Abstract: Knowledge of dependence between the length of the bridge and parameters which are defining the costs for its production can be extraordinary valuable for making decisions during planning, procurement or any other inhouse processes of manufacturers of this equipment. This article is expressing graphical and functional dependence between the bridge length and the basic parameters which are defining manufacturing costs of the bridges. Presented functions allow to predict parameters defining manufacturing costs for bridges which are out of the scope of this article also.

Keywords: Bridge; STANAG 2021; Bridge length; Static analysis; AM-50; Dependence.

1 SLOVAK ARMED FORCES BRIDGE EQUIPMENT

At the moment Slovak Armed Forces are using several types of bridging equipment. Mostly they are equipped with assault bridging systems and support bridging systems. Assault bridging systems are represented by wheeled vehicles AM-50 and PM-55. Tracked assault bridging systems are represented by vehicle MT-55. As support bridging systems the Slovak Armed Forces are using PMS-60 floating bridge. All of mentioned bridge bays can be considered as Orthotropic bridges. [2]

Orthotropic bridges are described like bridge structure which consisted of relatively thin sheet plate components. Road of the bridge is made from thin sheet plate, based on bridge bay load capacity. Road is supported by a series of closely spaced longitudinal ribs with support by orthogonal transverse floorbeams. Construction is normally supported by two main longitudinal beams. [1]

Mentioned description is absolutely valid for all mentioned bridge bay types which are in use of Slovak Armed Forces.

Orthotropic bridge bays can be divided in to two groups based on the shape of longitudinal ribs. It is a bridge bay with open ribs and bridge bay with closed ribs. Both construction types can be seen on Fig. 1. [1]

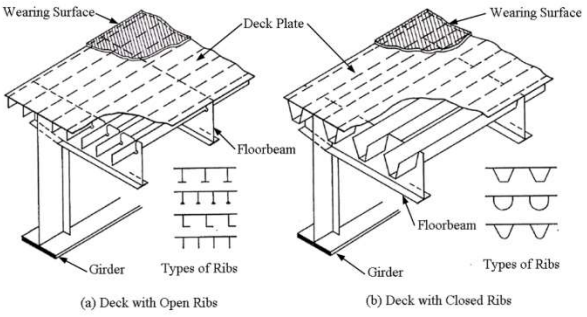


Fig. 1 Orthotropic bridge bays with open and closed ribs
Source: [1].

2 BRIDGE BAY OF AM-50 VEHICLE

One of the most used bridging equipment in Slovak Armed Forces is assault bridging vehicle AM-50. Construction of bridge bay is made from steel sheets which are connected by welding. Structure consists of two main beams which are stiffened in bottom part. These two beams are connected by several floorbeams and they are interconnected by series of closely spaced longitudinal ribs which are placed perpendicular to them. These longitudinal ribs have L shape. Roadway is made from thin steel sheet which is covering the whole construction from top side. Bottom side is not closed. Description of AM-50 bridge bay construction is exactly aligned to Orthotropic bridge bay with open ribs.[3]

AM-50 bridge bay has length of 13.5 m and as single bridge bay allow to overcome barrier with length of 12.5 m. It was designed for 50 tons load capacity for tracked vehicles and 70 tons for wheeled set. These two parameters are not specified anyhow closer. There are missing basic information and descriptions of contact area between the bridge and tracks or wheels. Spacing between axles of wheel set is missing too and the weight distribution for wheel set is missing as well. Nowadays this vehicle is facing two essential issues which are service age and insufficient tactical parameters. The result of second problem is disable interoperability of AM-50 bridging vehicle with heavy equipment in service of NATO member countries forces. [3]

Vehicle AM-50 went into service in 1977. At the moment the oldest pieces can have 45 years in service already. Because of that it is possible to predict their replacement in close time. [3]

3 REQUIREMENTS ON TACTICAL PARAMETERS OF BRIDGING SYSTEMS

At the moment most of the heavy equipment in service of NATO member states are classified into category MLC70 as per standard STANAG 2021. Based on that fact can be this category considered as minimal requirement for bridging equipment in

service of NATO member states. In some cases, it is possible to find bridging equipment with even higher load capacity MLC80. The length of the obstacle which can be overcome by AM-50 by using of single span can be considered as one of the shortest. Comparable vehicles such as TMM-6 has bridge bay with length of 17 m. [2]

Possible change of bridge bay construction and increasing of the load capacity or length of the bridge will have essential effect on parameters which are defining costs for production of that bridge. Knowledge of dependence of load capacity and the length of the bridge and parameters which are defining the costs for its production can be extraordinary valuable for making decisions during procurement processes of these equipment or any other inhouse processes of their manufacturers.

4 ARTICLE TARGET AND BOUNDARY CONDITIONS OF ITS REACHING

The main target of this article is to present a solution of dependence between the length of the bridge bay of bridging equipment as its tactical parameter and parameters which are defining its manufacturing costs.

Standard STANAG 2021 is not giving details such as basis of design or details regarding structural analysis of bridge components. These can be find in standards used in civil sector. It is for example standard EN 1993-1-1 Design of steel structures and its second part EN 1993-2 Steel bridges. In case of designing of bridge structure it is necessary to make all structural analysis based on these standards. STANAG 2021 is giving different details regarding hypothetical vehicles which will be crossing of bridges or details regarding safety factors, wind conditions etc. In case of designing of military bridge is essential to use both standards.

Study presented in article is showing different possibility of structural analysis made by FEM simulation in limited situations. This analysis can be used for designing of first bridge concepts before their structural analysis as per official standards.

The base for realization of analysis was 3D model of AM-50 bridge bay which was created based on existing design documentation of this vehicle. This 3D model was subjected by static analysis of load capacity as per standard STANAG 2021. Like default category was selected category MLC60. This category was selected due to missing detailed specification of loads and prediction that existing structure could be falling in to mentioned category. STANAG 2021 is defining in total 16 categories of load capacity and for each of them describing hypothetical tracked vehicle and wheeled set. For these hypothetical vehicles determines specific size of contact surface between tracks or wheels and surface of bridge road deck. On the same time defining the load applied on contact surfaces and in case of wheeled set the spacing between each axle. By using of these data was possible to establish the conditions of static analysis of each assessed bridge structure. Load conditions for category MLC60 is possible to see on Fig. 2. [4]

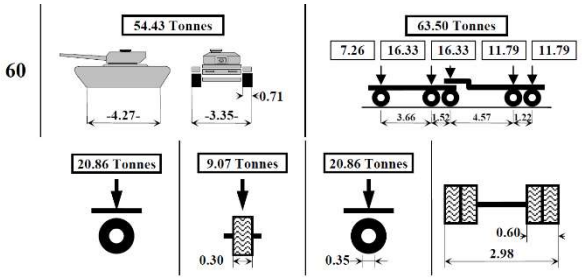


Fig. 2 Definition of hypothetical vehicles of category ML60 as per STANAG 2021
Source: [4].

Presented structural analysis is focusing on stress results in bridge structure from unfavorable situations which are creating the biggest bending moment on the bridge. The biggest bending moment will be applied on the bridge in situation where the vehicle center of the gravity will be on the same plane as geometrical center of the bridge. From logical reasons this should be a most unfavorable situation of placing of load on the bridge for static analysis. That is valid mainly for tracked vehicles. In case of wheeled set, it was impossible to reach different situation of load positioning because complete length of hypothetical vehicle was almost same as the bridge bay length. Because of that fact the geometrical center of the wheeled set was placed in to the same plane as geometrical center of the bridge. In both cases only centric movement will be taking in consideration. [4]

Except the contact surfaces of hypothetical vehicles standard STANAG 2021 defines other condition which must be met also. One of the most important boundary conditions for solving of bridge static analysis is required safety coefficient. Standard defines basic safety coefficient for Bending and/or Tension on level k=1.33. In case of Bearing safety coefficient it is necessary to multiple this value by constant 1.33. Final safety coefficient will looks as follows: k=1.33x1.33=1.7689. It is necessary to take in to consideration inaccuracy of simulation so final safety coefficient can be rounded to k=1.8. [4]

Next boundary condition of FEM static structural analysis is selection of material which will be considered as built material of the bridge. Original bridge bay of AM-50 vehicle was mainly made from steel CSN 15 222. This material under this standard is not possible to find on the market anymore. That was also the reason why company ZTS VVU Kosice a.s., like one of the original manufacturers of bridging equipment AM-50, replaced original steel with a steel S700 for its new products. That is the reason why this steel S700 was selected as built material for static

structural analysis purpose. One of the most important material properties for planned type of static structural analysis is yield strength. In case of steel S700 is maximum yield strength 700 MPa. After applying of safety coefficient as per STANAG 2021 is allowable stress in bridge construction $\sigma_{allowed}$=389 MPa.[5]

All other effects defined by STANAG 2021 such as wind, additional loads like mud, snow and ice load, longitudinal horizontal forces and etc., were not included in this study.

5 STATIC ANALYSIS OF AM-50 BRIDGE BAY AS PER SELECTED BOUNDARY CONDITIONS

All static structural analysis, which were done within this article and as per mentioned boundary conditions, were realized in software ANSYS 2021 R1.

Static analysis of original AM-50 bridge bay was done as per conditions mentioned in capture 4 of this article and for category MLC60 as per STANAG 2021. Like default position for tracked hypothetical vehicle was its place in the middle of the bridge which means that the tracked vehicle´s center of gravity was in the same plane, perpendicular to road way, as geometrical center of the bridge bay. In this situation is prediction of biggest effect of bending moment on bridge bay and prediction of biggest stress in bridge material as well.

Study is focused mainly on maximum stress due to biggest effect of bending moment on bridge bay and therefore no other location of hypothetical vehicle was checked.

Static analysis was done by standard procedure in module "Static Structural". For starting of simulation was necessary to set default material, defining contacts between each construction parts of bridge structure, mesh creation and defining of boundary conditions and application of the loads on the bridge structure.

Like result of the simulation was taken Maximum Principal Stress. The Maximum Principal Stress which was found in bridge bay was σ_{max1}=778.11 MPa. This value is higher than allowed stress but this maximum value was found only on several small areas. Stress in the rest of the structure was smaller than allowed stress. Visualization of the result is possible to see on Fig. 3.

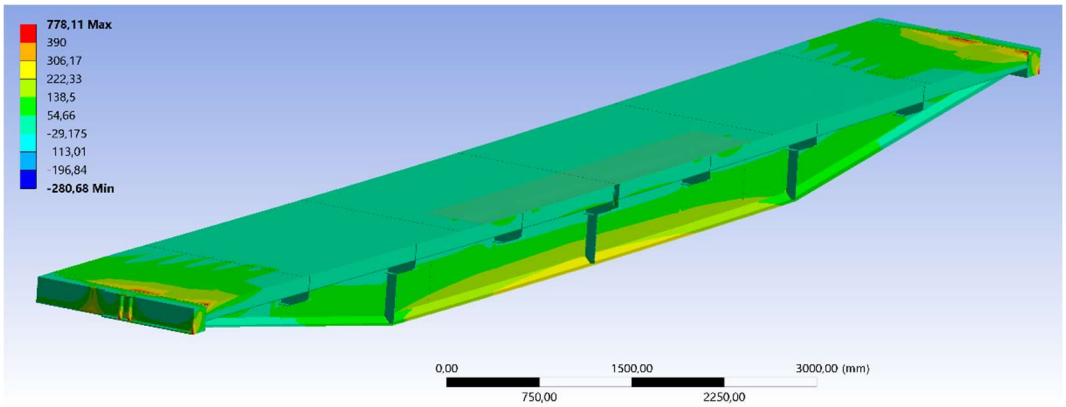


Fig. 3 Graphical result of static analysis of AM-50 bridge bay loaded by hypothetical tracked vehicle as per MLC60
Source: author.

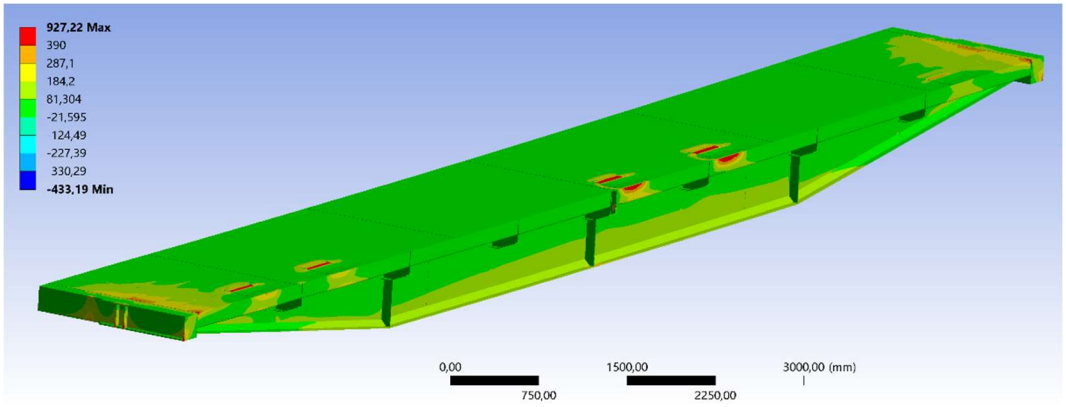


Fig. 4 Graphical result of static analysis of AM-50 bridge bay loaded by hypothetical wheeled vehicle as per MLC60
Source: author.

Second static analysis of original AM-50 bridge bay was done with wheeled set as per STANAG 2021 MLC60 category. Geometrical center of the wheeled vehicle was placed in the plane which is perpendicular to road way and in which is also located the geometrical center of the bridge.

The Maximum Principal Stress which was found in bridge bay due to application of wheeled set load was σ_{max2}=927.22 MPa. In contact area between the wheels and road way of bridge was found higher stress than allowable stress in material. This finding was more serious and more critical in comparison of the results with tracked vehicle. Visualization of the result is possible to see on Fig. 4.

The biggest disadvantage of presented FEM simulation is impossibility of efficient implementation of nonlinear buckling effects on complete model. Nonlinear buckling analysis can be done in mentioned software but efficient it will be only in case of single components analysis which correspond to structural analysis procedure as per mentioned standards EN 1993-1-1 and its second part EN 1993-2.

Based on the gained results is possible to evaluate that original AM-50 bridge bay is not capable to carry loads defined in STANAG 2021 category MLC60. The gained maximal stresses are higher than yield stress which will cause in yielding and plastic deformation in the end. With implementation of nonlinear buckling are expected even worse results. At the same time there is prediction of not positive results for bridge carrying capacity in regards to EN 1993-1-1 and EN 1993-2 as well, but this has to be checked.

6 DESIGN CHANGE OF ORIGINAL AM-50 BRIDGE BAY AND STATIC ANALYSIS AS PER GIVEN BOUNDARY CONDITIONS

Because of unfavorable results of static analysis of original bridge bay structure, it was necessary to accede of its design change. After a series of design changes and they verification by static analysis was created a final version of concept bridge structure for further investigation.

The biggest change was done in bottom part of the main beam. The thickness of this beam remains same but the thickness of bottom support flange which is perpendicular to that beam was changed from original 12 mm to 15 mm. Reinforcement which connected the main beam and support flange, and which was bended, and its thickness was 6 mm was changed also. This original reinforcement was replaced by four longitudinal reinforcements with thickness of 3 mm and placed perpendicular to the to bottom support flange. Advantage of this solution is that it is not increasing weight of original structure, it is easier for manufacturing and welding and improving the stiffness of the structure. Another radical change was done in front area of the bridge bay. In this area have been added four longitudinal reinforcements which are connecting the bottom support flange and roadway of the bridge bay. Their thickness is 3 mm as well. Longitudinal ribs were also changed. Their original thickness was 2.7 mm and for a new bridge design were used ribs with 3 mm thickness. Their spacing were reduced and three on each side of the bridge were added. Final optimized construction has weight of 6 461 kg, width is 4 000 mm and complete length is 13 500 mm. In comparison with original bridge structure is around 510 kg heavier. Components which were changed are marked on Fig. 5 and Fig. 6. [3]

The results of static analysis of redesigned bridge as per conditions mentioned in chapter 4 are in Tab. 1.

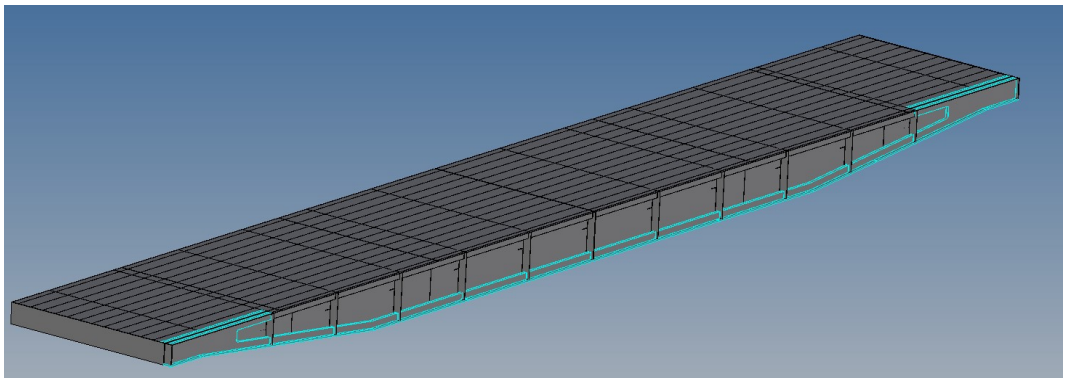


Fig. 5 Visualization of main changes done on original AM-50 bridge bay construction, upper view
Source: author.

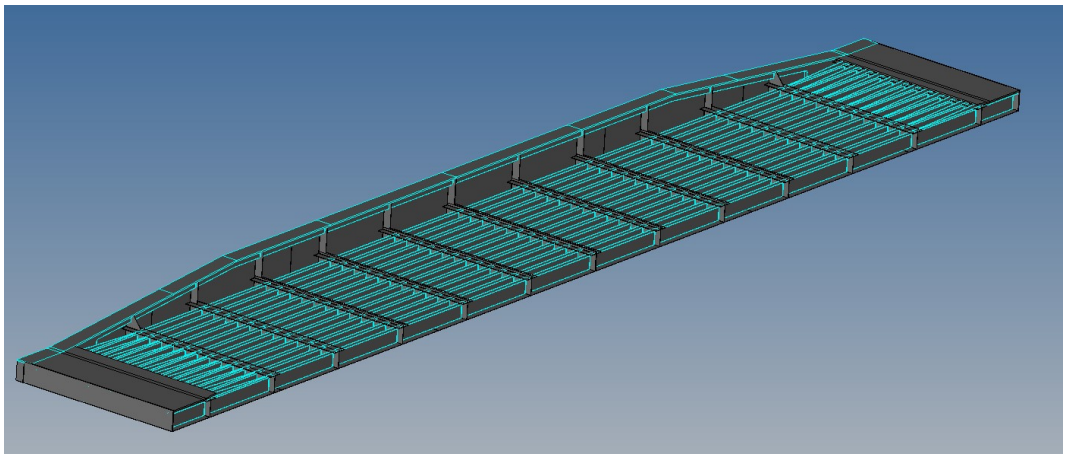


Fig. 6 Visualization of main changes done on original AM-50 bridge bay construction, bottom view
Source: author.

Tab. 1 Results of static analysis of redesigned AM-50 bridge

Principle stress	Tracked vehicle	Wheeled set
Average stress in main beam, bottom support flange and longitudinal reinforcements (MPa)	88.16	61.52
Average stress in floorbeams (MPa)	43.33	30.04
Average stress in longitudinal ribs (MPa)	25.58	15.70

Source: author.

7 STATIC ANALYSIS AND OPTIMALIZATION OF BRIDGE STRUCTURES OF DIFFERENT LENGTHS BASED ON ORIGINAL AM-50 BRIDGE

Successful result of redesigned original AM-50 bridge with length of 13 500 mm and width of 4 000 mm represent starting point for next analysis. Construction of this bridge is marked as variant A in rest of this article.

In next phase of article´s target solving were step by step created four bridge variants which were designed as per construction of variant A. In first phase the thickness of all main components were same. Width of all bridge variant structures was same as variant A. Width of the bridge 4 000 mm was considered as not changeable parameter.

Single length and marking of each bridge structure which were analyzed in this article is possible to find in Tab. 2.

Tab. 2 Marking of each bridge length variant

Length of the bridge (mm)	Bridge variant marking
13 500	A
14 500	B
15 500	C
16 500	D
17 500	E

Source: author.

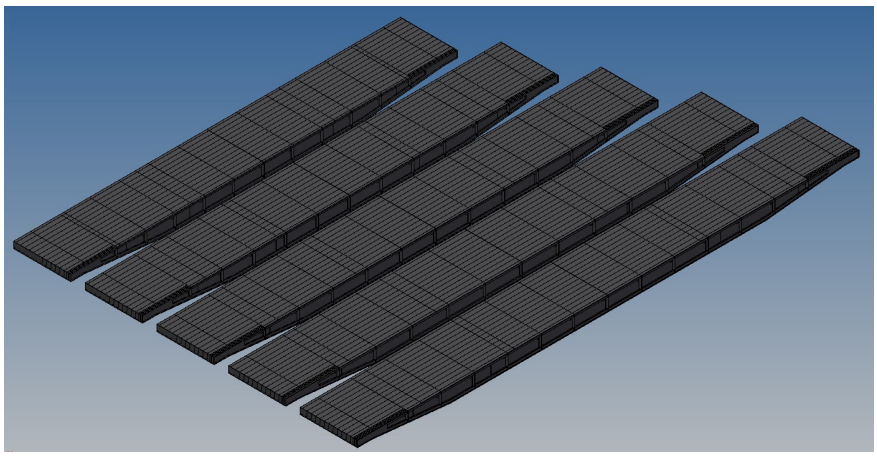


Fig. 7 Graphical presentation of all bridge variants
Source: author.

Each bridge variant mentioned in Tab. 2 was subjected by static analysis in software ANSYS 2021 R1. Based on this analysis each bridge structure was optimized to meet same requirements as bridge variant A. For elimination of possibility of changes which will lead to too high stiffness or opposite to lower stiffness than other bridge structure it was set a parameter of average stress for tracked vehicle load situation in main bearing elements. This value was set as per results from variant A static simulation. 88.00 – 88.50. During optimalization process was emphasized on keeping the same construction scheme as variant A. Main design improvements were done by changing of thickness of components or by addition of components to increase stiffness of the structure. Mostly were changed thickness of longitudinal enforcements on support flange. Design of these components had biggest impact on monitored average stress. Most of the rest of the components were changed only because of the change of the bridge structure length.

Results of static structural analysis of each bridge variant is possible to see in Tab. 3.

Tab. 3 Results of static analysis of each bridge variant

Principle stress	Tracked vehicle	Wheeled set
Variant B		
Average stress in main beam, bottom support flange and longitudinal reinforcements (MPa)	88.02	64.37
Average stress in floorbeams (MPa)	47.26	35.00
Average stress in longitudinal ribs (MPa)	23.19	14.81
Variant C		
Average stress in main beam, bottom support flange and longitudinal reinforcements (MPa)	88.50	68.34
Average stress in floorbeams (MPa)	49.94	39.39
Average stress in longitudinal ribs (MPa)	21.73	14.65
Variant D		
Average stress in main beam, bottom support flange and longitudinal reinforcements (MPa)	88.47	71.30
Average stress in floorbeams (MPa)	52.40	43.71
Average stress in longitudinal ribs (MPa)	19.97	14.08
Variant E		
Average stress in main beam, bottom support flange and longitudinal reinforcements (MPa)	88.15	73.76
Average stress in floorbeams (MPa)	54.72	47.69
Average stress in longitudinal ribs (MPa)	19.51	14.17

Source: author.

8 DEPENDENCE EXPRESION OF BRIDGE LENGTH OF BRIDGING EQUIPMENT AND PARAMETERS WHICH ARE DEFINING COSTS FOR ITS MANUFACTURING

After successful finish of all static analysis and optimalization of each bridge construction was necessary to define basic parameters which are defining costs for bridge manufacturing. Based on practical experiences were set two basic parameters which were:

a) Weight of construction – based on information about weight of the structure is possible to evaluate some costs for bridge manufacturing. It is for example calculation of costs for construction material, costs linked with assembly and manipulation with structure. This parameter was divided in to two groups:
   - Weight of the main beam, longitudinal enforcement, and bottom support flange.
   - Weight of longitudinal ribs and floorbeams.

b) Size of surface content – based on information about the content of all bridge surfaces is possible to evaluate costs which are needed for application of paints or coatings. This parameter was divided in to two groups also:
   - Surface content of the main beam, longitudinal enforcement and bottom support flange.
   - Surface content of longitudinal ribs and floorbeams.

On the graphs below is possible to see dependence expression between bridge length and each parameter which is describing manufacturing costs of the bridge structure. All cost parameters were gained from 3D files of each bridge variants, A up to E, in the software Inventor 2019.

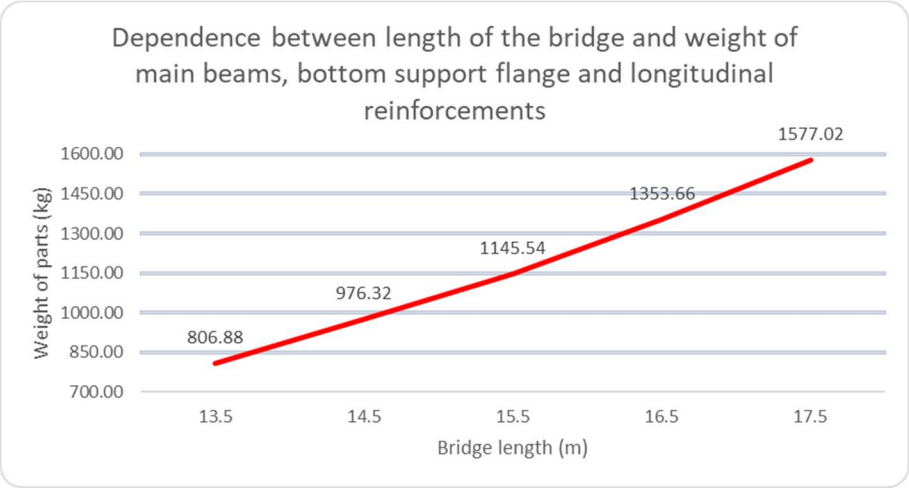


Fig. 8 Graph of dependence between bridge length and weight of main beams, bottom support flange and longitudinal reinforcements
Source: author.

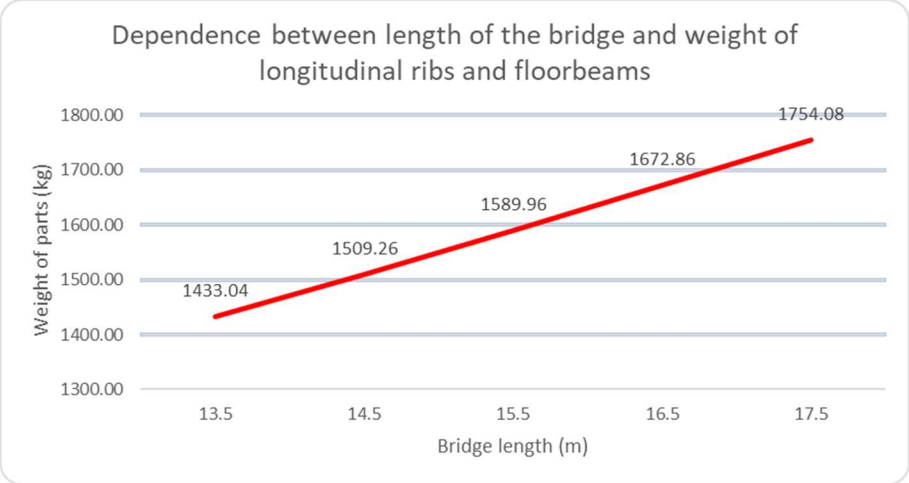


Fig. 9 Graph of dependence between bridge length and weight of longitudinal ribs and floorbeams
Source: author.

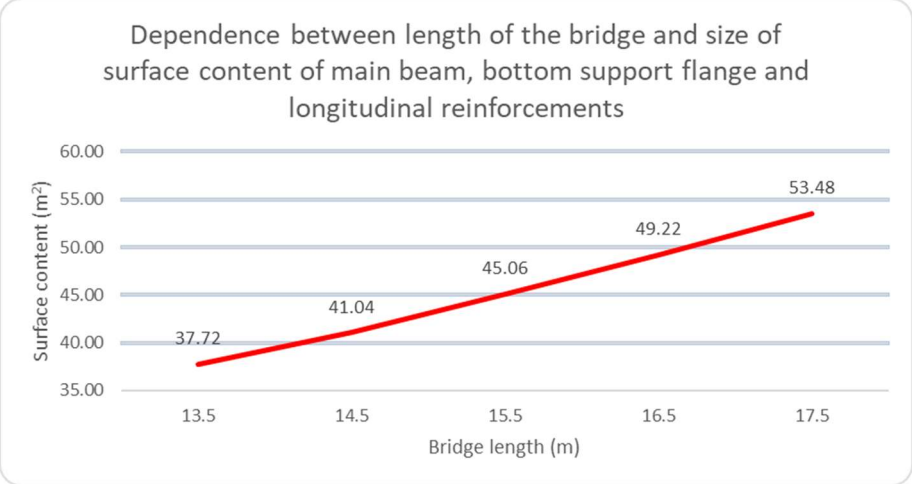


Fig. 10 Graph of dependence between bridge length and surface content of main beams, bottom support flange and longitudinal reinforcements
Source: author.

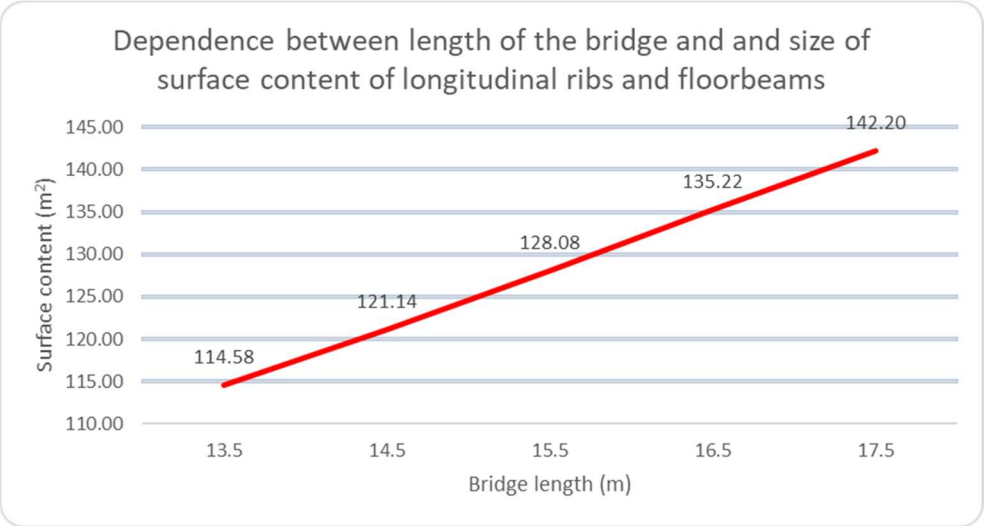


Fig. 11 Graph of dependence between bridge length and surface content of longitudinal ribs and floorbeams
Source: author.

From graphical dependence expression of each cost´s parameter on the length of the bridge is possible to evaluate, that for both parameters for main beams, bottom support flange and longitudinal reinforcement dependence have slightly exponential look. For Longitudinal ribs and floorbeams are dependence for both parameters linear. These results are logical because during increasing of the bridge length the stress in material of main beams, bottom support flange and longitudinal reinforcement was raising and here was necessity of material addition. In the rest of the structure the impact of length change was not significant to the stress cumulated in material. Therefor only addition of material due to length change was needed and this was on linear basis. Based on that it is possible to create an exponential or linear function for prediction of each parameter in case of different bridge length to the variants which were checked in this article. Functions which are describing each parameter were gained from software Excel by using of trendline.

Growth curves of these parameters is possible to define also by polynomic function. They will be valid only for bordered curves by exact length of the bridge from 13 500 mm up to 17 500 mm and it will be not possible to use them for predictions out of these limits.

Functions which are expressing each dependence are looking as follows:

a) Function for dependence expression between length of the bridge bay and cost parameter weight of main beam, bottom support flange and longitudinal reinforcements is:

$$y = 86.058e^{0.1667x} \quad (1)$$

$$y = -2.6158x^4+163.47x^3-3808.6x^2+39396x-152241 \quad (2)$$

b) Function for dependence expression between length of the bridge bay and cost parameter weight of longitudinal ribs and floorbeams:

$$y=80.568x+343.04 \quad (3)$$

$$y=-0.5133x3+24.741x2-314.69x+2435.2 \quad (4)$$

c) Function for dependence expression between length of the bridge bay and cost parameter size of surface content of main beam, bottom support flange and longitudinal reinforcements is:

$$y=11.492e^{0.088x} \quad (5)$$

$$y=-0.05x^3+2.4693x^2-36.37x+201.7 \quad (6)$$

d) Function for dependence expression between length of the bridge bay and cost parameter size of surface content of longitudinal ribs and floorbeams:

$$y=6.932x+20.798 \quad (7)$$

$$y=-0.045x^3+2.1668x^2-27.652x+203.7 \quad (8)$$

9 CONCLUSION

The basic target of this article was to find a dependence between length of the bridge bay which was coming out from original bridge of AM-50 vehicle and cost parameters which are defining manufacturing costs for these structures. This basic target has been achieved.

Like two mains cost parameters were set weight and surface content of the bridge structure. Both

of these parameters were divided in to two groups defined by exact components. First group was made by main beam, bottom support flange and longitudinal reinforcement. The second group consisted of longitudinal ribs and floorbeams of the bridge. Dependence expression of bridge length and costs parameters for each group is possible to find in chapter 8 of this article. Except the graphical expression of mentioned dependences is also possible to find functions for each curve of these dependences in chapter 8. These functions can be used for calculation of cost parameters for the bridges out of the scope of this article.

In addition to the basic target was found that the bridge of the bridging vehicle AM-50, which is now in equipment of Slovak Armed Forces, does not meet the requirements of MLC60 category of standard STANAG 2021. This finding was done by FEM simulations in specified conditions, see chapters 4 and 5. To confirm this conclusion is necessary to subject the bridge to the complex structural analysis according to EN 1993-1-1, part 2 in combination with STANAG 2021.

References

[1] CONNOR, R. J. at all. *Manual for design, construction, and maintenance of orthotropic steel deck bridges*. United States Department of Transportation. Federal Highway Administration. [online]. 2012. [cit. 2022-03-15]. Available at: https://www.fhwa.dot.gov/bridge/pubs/if12027/if12027.pdf

[2] MAKO, P. Analysis of Bridging Systems Within Slovak Armed Forces and Possibilities of their Replacement. In *Science & Military Journal,* 2020, 15(2), 5-11 s. ISSN 1336-885.

[3] Ženijný predpis OS SR. ŽEN-24-14 Mostný automobil AM-50, 1977.

[4] STANAG 2021 „Military Load Clasification of Bridges, Ferries, Rafts and Vehicles", 2005.

[5] FÜRBACHER, I., K. MACEK, J. STEIDL et. al. *Lexicon of technical materials*. (in Czech) Verlag Dashöfer, 2005.

[6] BOCKO, J., P. LENGVARSKÝ, R. HUŇADY and I. DELYOVÁ. *Simulation in Programm ANSYS* (in Slovak). TU SjF Košice, 2019.

[7] ZIENKIEWICZ, O. C. and R. L. TAYLOR. In *The finite element method: solid mechanics*. Vol. 1. Butterworth-Heinemann, 2000.

[8] ZIENKIEWICZ, O. C. and R. L. TAYLOR. In *The finite element method: solid mechanics*. Vol. 2. Butterworth-Heinemann, 2000.

[9] ZIENKIEWICZ, O. C. and R. L. TAYLOR. In *The finite element method: solid mechanics*. Vol. 3. Butterworth-Heinemann, 2000.

[10] STN EN 1993-1-1: Design of steel structures. Part 1-1: General rules and rules for buildings, 2005 including its Corrigendum AC: 2006.

[11] STN EN 1993-1-1: Design of steel structures. Part 2: Steel bridges, 2007.

Dipl. Eng. Peter **MAKO**
Armed Forces Academy of General M. R. Štefánik
Department of Mechanical engineering
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: p.mako.peter@gmail.com

Peter Mako was born in Kosice, Slovakia in 1989. He received his Engineer degree in 2013 in field of Automotive production at Faculty of Mechanical engineering of Technical University in Kosice. He is PhD candidate of Department of Mechanical engineering of Armed Forces Academy of General M. R. Stefanik. His research is aimed to military bridging systems of engineery units.

DOI: https://doi.org/10.52651/sam.a.2022.1.14-22

EVASION OF ANTIVIRUS WITH THE HELP OF PACKERS

Andrej FEDÁK, Jozef ŠTULRAJTER

Abstract: Nowadays, almost every malware file comes obfuscated and prepacked preferably with an unknown algorithm. Antivirus programs are taught to deal with these kinds of obstacles with the help of signature databases and heuristic engines. AV systems and their tools are professionally and carefully developed by experts; however, they are not flawless either. They tend to react to any threats that are identified by already-known malicious patterns and bad behaviours. Therefore, malware has to evolve and use new methods to pass these defences. In this paper, the internal components of AV programs and well-known packing techniques are briefly explained while in addition they are tested against each other. This work provides an initial insight into the complex subject of antivirus protection.

Keywords: Antivirus detection; Malware evasion; Scanner; Signature; Heuristic engine; Packer; Obfuscation; Compressor; Crypter; Protector; Portable executable.

1 INTRODUCTION

First things first, in order to evade antivirus protection, researchers or attackers must know how an antivirus product works. Therefore, the aim of this work is to describe the basic components that create the whole structure of the AV program. Individual AV components are introduced together with their internal processes that help in the detection and removal of malicious files. As the attack patterns become more sophisticated, antivirus engines have to adapt and improve their capabilities to identify new potential threats. Malware authors always try to be one step ahead of the competition and develop new methods to mask their activities and hide any traces of their malicious code. One of the many obfuscation techniques is the use of packer programs that are capable to create a new protection layer around the bad executable file. Dozens, nay hundreds of unique packer programs are in circulation and many more to come. In this paper, the effectiveness of the well-known packers is tested as well as some of their shielding features are explained.

2 DEFINITION OF ANTIVIRUS SOFTWARE

Antivirus software is special security software created for the purpose to protect your computer and prevent computer infections by detecting malware. In the vast majority of cases, it is used as a preventive measure. Even such specified software solutions are not perfect and in the case of an uncaught intrusion and infection, they are furthermore designed to completely remove the malicious software and disinfect the computer [1].

Nowadays, several security features come usually built-in within the operating systems such as Windows (Defender) or Mac OS X (XProtect). There is still a vast number of companies (for example Bitdefender, Norton, Kaspersky, Avast, ESET, and many others) that solely focus all of their resources to create special security software that aims to give better protection than that offered by the operating system.

The main feature of AV software is to find known malicious behaviours and patterns in programs, documents, web pages, or network packets. The detection capabilities of AV products are primarily based on experience with previously known malware patterns. Simply, an AV software is not able to identify new unknown threats unless they are based on old known behavioural or static patterns [1].

3 STRUCTURE OF ANTIVIRUS SOFTWARE

The main part of an AV system is called the core or the kernel, which coordinates tasks between all the other components such as the scanning engine (command-line scanner, GUI scanner), daemons or system services, file system filter drivers, network filter drivers, plugins, kernel AV components (signature database, decompressors, emulators, supported file formats). The AV product suite may also include other additional support utilities like browsers, browser toolbars, drivers for self-protection, firewalls, and so on. As you can see, the product is the whole software package the AV company ships to the customer [1].

3.1 Kernel

A kernel forms the core of an AV product. All the routines for unpacking executable programs, compressors, crypters, protectors, and so on are in the kernel's libraries. Hence the kernel must support all the code for opening a very long list of file formats in order to iterate through all the streams in a file, analyse them, and catch malicious exploits embedded in the files. Some file formats (excluding compressors and archives) that need to be supported are OLE2 containers (Word or Excel documents); HTML pages, XML documents, and PDF files; CHM help files; PE, ELF, and MachO executables; JPG, PNG, GIF, and TIFF image file formats; ICO and CUR icon formats; MP3, MP4, AVI, and MOV video and audio

file formats; and so on. Furthermore, the kernel is frequently used by the scanner engine, by the AV resident (or daemon), or by other programs and libraries. Developing an AV kernel is very complex because enormous time and effort are required to support mentioned features [1].

3.2 Scanners

Another common feature of AV products is the scanner, which may be a GUI or command-line on-demand scanner. Such tools are used to scan whenever the user decides to check a set of files, directories, or the system's memory. There are also on-access scanners, more typically called residents or real-time scanners. The resident analyses files that are accessed, created, modified, or executed by the operating system or other programs (like web browsers). It does this to prevent the infection of document and program files or to prevent known malware files from executing. However, the resident is one of the most interesting components to attack. For example, a security bug in the parser of Microsoft Word documents can expose the resident to the execution of a malicious code after a Word document is downloaded (even if the user doesn't open the file). Or a similar approach can be applied to the AV's parser code handling new email messages and their attachments. These bugs can be used to perform a denial-of-service attack on an AV program, which makes it crash or loop forever, thus disarming the antivirus temporarily or permanently [1].

3.3 Signatures

The scanner of any AV product searches files or packets using a set of signatures to determine if the files are malicious. The signatures are the known patterns of malicious files. Some typical signatures are based on the simplest pattern-matching techniques (searching for a specific string, or byte-stream), Cyclic Redundancy Check algorithms (error-detection code that calculates output hash in form of CRC checksums), or MD5 and SHA1 hashes. Relying on cryptographic hashes, like MD5, works only for a specific file (as a cryptographic hash tries to identify just that one whole file), while other fuzzy logic-based signatures, as CRC algorithm applied on specific parts of data, can identify various bad files. AV products usually have different types of signatures which range from simple CRCs to rather complex heuristics patterns based on many PE header properties, the complexity of the code at the entry point of the executable file, the entropy of a section or the whole executable file, and so on [1].

Each kind of signature has advantages and disadvantages. For example, some signatures are very specific and less likely to be prone to a false positive (when a healthy file is flagged as malware) – cryptographic hashes, while others are very risky and can generate a large list of false positives – CRCs. For example, imagine a signature that finds the word "Microsoft" anywhere in a file. This would cause a large list of false positives, regardless of whether it was discovered in malware. Stricter pattern description avoids any false positive detections [1].

3.4 Decompressors and unpackers

Another key part of every AV kernel is the support for compressed or archived file formats like ZIP, TGZ, 7z, RAR, XAR, and so on. AVs must be able to decompress and navigate through all the files inside any compressed or archived file, as well as compressed streams in PDF files and other file formats. Because AV kernels must support so many different file formats, vulnerabilities are often found in the code that deals with this variety of input [1].

An unpacker is a routine or set of routines developed for unpacking protected or compressed executable files. Malware in the form of executables is commonly packed using freely available compressors and protectors or proprietary packers. Some packer tools, like UPX (Ultimate Packer for Executables), just apply simple compression, and unpacking such samples is an easy and straightforward matter. On the other hand, more complex software packers and protectors may in addition transform the code into bytecode and run it with its own virtual machine. Some packers can be unpacked using the CPU emulator of the AV, another by static means, and the rest, more complex ones, using both techniques. The emulator is used up to some specific layer and then a static routine executes when some specific values are known such as the size of the encrypted data, the algorithm used, the key, and so on [1].

As with compressors and archives, unpackers are a very common area to explore when you are looking for vulnerabilities in AV software. The list of packers to be supported is immense, even larger than the number of compressors and archives, and it is still growing. Some of them are used only during a specific malware campaign, so there is ever-growing emergence of new packers hiding the logic of new malware [1].

3.5 Emulators

Most AV cores on the market offer support for a number of emulators such as the most common Intel x86 emulator, AMD64, or ARM emulators. Emulators are not limited to regular CPUs. There are also emulators for some virtual machines that are aimed at inspecting Java bytecode, Android DEX bytecode, JavaScript, and even VBScript or Adobe ActionScript. Usually, files that trigger the emulators are EXE crypters or packers that are too complex to decrypt statically, so the antivirus engineers decided to decrypt them using the emulator.

Nowadays, fingerprinting or bypassing emulators and VMs used in AV products is very common and quite an easy procedure. It is almost impossible that the developers of the AV emulators would implement all of the instructions supported by to-be-emulated real CPUs. For executable ELF or PE files, it is even less likely that the developers would implement the whole operating system environment. Therefore, it is really easy to discover many different ways to fool emulators and to fingerprint them [1].

3.6 Heuristics engines

Another common component in antivirus software that detects malicious code is the heuristic engine. The AV heuristic engines make decisions based on general evidence instead of universal detections or typical signature-based methods. They rely on detection procedures that assess evidence and behaviour as collected from analysing the code statically or dynamically. On the other hand, they do not rely on specific signatures to try to catch a certain family of malware or malware that shares similar properties. Heuristic engines implement a set of algorithms that emulate the decision-making strategy of a human analyst [1].

There are three different types of heuristic engines namely static, dynamic, and hybrid, which uses both strategies. Most often, static heuristic engines are considered true heuristic engines, while dynamic heuristic engines are called Host Intrusion Prevention Systems (HIPS). Static heuristic engines try to discover malicious software by finding evidence statically by disassembling or carefully analysing the file headers. Dynamic heuristic engines try to assess the file or program based on its behaviour by hooking (intercepting) API calls or executing the program in an emulated environment. Learning about various heuristic engines can get some insights into how attackers are evading AV detection [1].

3.7 Static heuristic engine

Static heuristic engines are implemented in many different ways depending on the deployment target. For example, it is common to use heuristic engines that are based on machine learning algorithms (such as Bayesian networks, genetic algorithms, or expert systems) to reveal information about similarities between families by focusing on the biggest malware clusters created by the heuristic engines. Those heuristic engines are deployed and acceptable only in malware research labs because they can cause a large number of false positives and consume a lot of resources. For desktop antivirus products, a much better choice is an expert system that implements a set of algorithms simulating the decision-making process of a human analyst [1].

A human malware analyst can determine that an executable file appears malicious, without actually observing its behaviour, by briefly analysing the file structure and taking a quick look at its disassembled code. The analyst would evaluate several indicators as a whole before labeling the file as a malicious one. Some of the suspicious features could be an uncommon file structure, uncommon characteristics in a PE header, the obfuscated code, compressed or somehow protected program, file packed multiple times, corrupted file, any anti-debugging tricks, change in the icon of the PE file to the different one (used for image files, documents, etc.), dual extension (common in malware that disguises an executable file as a video, picture, document, ZIP file, or other types), and so on. If some of the mentioned features are true, a human analyst would suspect that the file is malicious or at least that it is trying to hide its logic and needs to be closely analysed. He would also compare that sample with some sort of list of known false positives. Such human-like behaviour, when implemented in a heuristic engine, is called an expert system [1].

3.8 Dynamic heuristic engine

Another analytical technique is known as dynamic heuristics. When researchers want to analyse a suspicious code without endangering running systems, they contain the sample in a controlled environment (like a secure lab) and perform a variety of tests. Like this, it isolates the program or piece of code inside a specialized virtual machine or sandbox and gives the AV program a chance to test the code and simulate what would happen if the suspicious file was allowed to run. It examines each command that's executed and looks for any suspicious behaviours, such as self-replication, overwriting files and registry entries, and other actions that are common to malware [2].

Dynamic heuristic engines base their detections on the behaviour of the file or program by hooking API calls or executing the program under an emulation framework. The former approach is more reliable because it involves actually looking at the true runtime behaviour, while the latter is more error-prone because it largely depends on the quality of the CPU emulator engine and the quality of the emulated operating system APIs. It is quite an easy task to bypass heuristic engines based on emulators and virtual execution environments. Malware may execute a code that is not fully supported by the emulators to fingerprint the AV software and change its own behaviour accordingly with the intention of avoiding detection. Bypassing heuristic engines based on hooks, like the typical Host Intrusion Prevention Systems (HIPS), is not complex either and depends on which layer the API hooks are installed (userland or kernel-land hooks) in order to monitor the behaviour of a program [1].

Userland hooks work by detouring or intercepting some APIs to monitor and control the execution of

those APIs. To bypass userland hooks, attackers could read the original prologue of the hooked functions from the disk, execute those bytes, and afterward continue executing the not-hooked part of the function past the prologue bytes. Another simple approach is to unload the hooking library, which will subsequently remove the respective hooks. Kernel-land hooks rely on registering call-backs that monitor the creation of processes and access to the system registry and monitoring real-time file activity. Similarly, kernel-land hooks might be bypassed and uninstalled by malicious code running in the kernel [1].

4 MALWARE DETECTION WITH VIRUSTOTAL

VirusTotal is an online service that allows you to upload a file, which will be subsequently inspected with over 70 antivirus scanners. It can be useful in detecting malicious content and also in identifying false positives (harmless items detected as malicious by one or more scanners). Upon submitting a file, scanning reports are shared with the submitter, and also the public VirusTotal community. As a result, the contributors are raising the global IT security level and helping cybersecurity professionals and security product developers discover harmful files samples for further study, analyse emerging cyber threats, and create new defences [3].

VirusTotal's aggregated data is the output of many different antivirus heuristic engines, known-bad signatures, website scanners, metadata extraction, file and URL analysis tools, many user contributions, etc. Since the end of 2017, it is also integrating a malware analysis system in order to contribute behavioural analysis reports. Thus, its tools are able to comprehensively analyse samples from both static information and dynamic behaviours, trigger and capture behaviours of the samples in the sandbox, and output the results in various formats [3],[4].

Sometimes, the main advantage of using VirusTotal could be also its drawback since all the uploaded files automatically become public. This is not productive if you are researching AV evasion techniques or when doing penetration testing. In the first case, malware creators are also searching through public databases to find out if their malware has already been discovered. If so, they could alter the behaviour of malicious samples or stop using some of its services to hide any tracks. In the second situation, using VirusTotal can be a bad idea if you want to keep your testing payloads private to ensure they evade antivirus products for a longer period of time. Therefore, you need to use a private VirusTotal-like tool and this is where your own offline MultiAV solutions come into play [1].

The actual usefulness of virus scanners to discover new threats is being disputed, but they are able to detect *well-known* threats quite well. In this work, we are mainly interested in the changes in the detection results after applying wrappers on the malicious files. Hence the output provided by VirusTotal is more than sufficient.

5 MALWARE EVASION WITH PACKERS

AV software uses various techniques to identify malicious software, which often self-protects. Today's malware may use many obscure techniques in order to persist by staying hidden during infection and operation and to prevent detection, analysis, and removal. Malware achieves this by adding code that is not strictly malicious but only intended to hide the malicious code in an operating system (see the visualization in Figure 1).

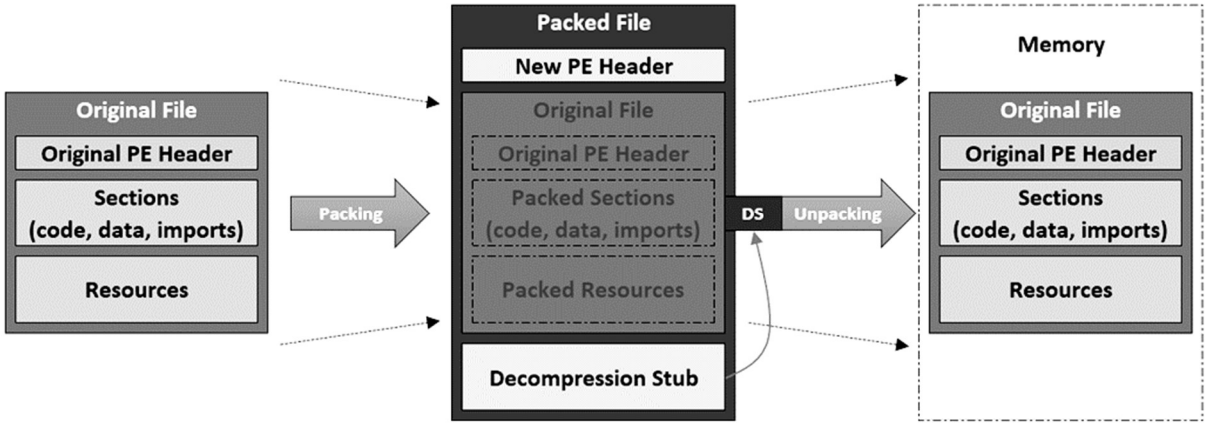


Fig. 1 Life cycle of packed PE (portable executable) file
Source: authors.

According to the used layer of protection, the obfuscation techniques can be divided into three main categories: packers, crypters, and protectors. Definitions for these categories are not carved in stone, differences between them are sometimes blurred, they all have overlap and there are exceptions to the rules [1], [5], [6].

ROT5

Plaintext (ASCII)	R	o	T	a	T	e	M	E
Plaintext (8-bit)	01010010	01101111	01010100	01100001	01010100	01100101	01001101	01000101
Add 5 (8-bit)	00000101	00000101	00000101	00000101	00000101	00000101	00000101	00000101
Ciphertext (8-bit)	01010111	01110100	01011001	01100110	01011001	01101010	01010010	01001010
Ciphertext (ASCII)	W	t	Y	f	Y	j	R	J

XOR operation

Plaintext (ACSII)	h	e	l	l	o	m	a	n	A	B	A ⊕ B
Plaintext (8-bit)	01101000	01100101	01101100	01101100	01101111	01101101	01100001	01101110	0	0	0
XOR key (8-bit)	01010011	01010011	01010011	01010011	01010011	01010011	01010011	01010011	0	1	1
Ciphertext (8-bit)	00111011	00110110	00111111	00111111	00111100	00111110	00110010	00111101	1	0	1
Ciphertext (ASCII)	;	6	?	?	<	>	2	=	1	1	0

Base64 encoding

Plaintext (ASCII)	S								U								B							
Plaintext (8-bit)	0	1	0	1	0	0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	1	0
Ciphertext (6-bit)	0	1	0	1	0	0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	1	0
Ciphertext (Base64)	U						1						V				C							

Fig. 2 Trivial examples of encryption techniques
Source: authors.

5.1 Compressors, original packers

In a lot of cases, the entire malware program is obfuscated using what's known as a packer program (for example UPX, PESpin, MPRESS, ASPack, even WinRAR, and dozens of others). Simply, a runtime packer compresses the original malware file, thus making all the original code and data unreadable. This software prevents anybody from directly viewing the malware's code until it decompresses itself at runtime in the memory where the "packed file" is executed thus revealing the program's original code. Sometimes this technique is also known as "self-extracting archives" or "executable compression" [5], [6].

In the past, this type of compression has been used for legitimate purposes, some of which include protecting against piracy and making executable files smaller because of the then size of portable media and internet speeds. Nowadays, this application became unnecessary, so when you see some packers being used, it is almost always for malicious purposes. They help conceal vital program components to prevent less-experienced reverse engineers from unpacking the malware's contents. The creation of new custom packers defeats modern unpacking scripts and forces reversers to manually unpack the file. Sometimes malware authors will pack their files two times, with a commercial packer and then with their own custom solution [5], [6].

Fortunately, there are many programs available that identify commercial packers, and also advise on how to unpack these files. Some of the file scanners are for example Exeinfo PE, PEID, Detect-It-Easy, or any signature-based database checker [6].

5.2 Crypters

The crudest technique utilized by malware authors to hide malware's internals is called obfuscation which can be commonly seen in scripts. Obfuscation is a technique that at first sight makes binary and textual data (for example malicious URLs or registry keys) unreadable and hard to understand. Its implementation can be as simple as a few bit manipulations and advanced as cryptographic standards (i.e. DES, AES, etc). Thus, a more complex method is actual encryption. A crypter is a type of software that can encrypt, obfuscate, and manipulate malware, to make the hidden executable as hard to detect by security programs as possible [5], [6].

Perhaps the simplest technique is **ROT** which is an ASM instruction for "rotate", hence, for example ROT13 would mean "rotate 13". ROT13 uses simple letter substitution to achieve obfuscated output. The **XOR** operation is probably the most common method of obfuscation. With the simple XOR cipher, a string of text can be encrypted by applying the bitwise XOR operator to every character using a given key. Even without the XOR key, decryption programs are able to cycle through every possible single-byte XOR value in search of a particular string (i.e. "MZ" or "PE"). To make the obfuscation more bulletproof, malware authors might implement a two-cycle

approach (performing two XOR encryptions with different values) or increment the XOR, ROT value in a loop. Furthermore, **Base64** encoding has been used for a long time to transfer binary data (machine code) over a system that only handles text. Its encoding alphabet is commonly used in malware to disguise text strings. Because Base64 encoding is typically easy to identify by its padding character (equal sign "=") and then overcome, malware authors may adjust the order of the alphabet, which breaks standard Base64 decoders. The basic principles of aforementioned cryptographic techniques are illustrated in the Figure 2 [6].

5.3 Protectors

A protector (for example Enigma, Themida, VMProtect, and so on) is software created to keep an attacker from directly inspecting or modifying a compiled application to change its behaviour. It could be described as a shield that keeps an application encrypted and protected against reverse engineering (refer to Figure 3). The obfuscation techniques used by the protectors usually include the best of both packing and encrypting (hybrid). That combination together with some added features builds several protective layers around the payload that a researcher has to face. For example, when a protected application is going to be run, the software protector will first check for possible cracking tools (dissemblers or de-compilers) that may be running on the operating system. If everything is safe the software protector will then proceed to decrypt the protected application and allow it to be executed [5], [7].

Another approach of protectors is code virtualization, which uses a customized and different virtual instruction set every time you use it to protect your application. Such professional protectors are used in the gaming industry against piracy, yet this technique has also made its way into malware, more specifically ransomware. The protection is so efficient that there is no need for the encryption key to be obtained from the command-and-control server, but it can be hardcoded right into the ransomware. Unpacking samples protected by a virtualization packer could be highly time-consuming and sometimes even impossible for researchers to restore the sample into its original code. Detection of these packed samples is extremely difficult with traditional AV unpacking technology [5].

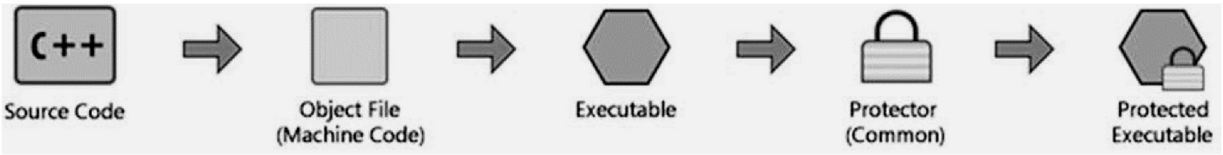


Fig. 3 Philosophy of common software protectors
Source: [7].

The main advantage of using a software protector is to protect an application (in our case, malware) against piracy and reverse engineering, however, that doesn't mean the protected application is unbreakable. That's because software protection is very different from data protection. Even if a software protector encrypts the protected application with the most robust cryptographic algorithm (like RSA, Elliptic curves, and AES), sooner or later the protected application needs to be decrypted part by part in order to be run by the CPU. It is in this phase that most attackers will start their work by dumping the decrypted application from memory to disk thus not having to deal with the cryptographic algorithm and reconstruction of the original application [7].

6 THE EFFECTIVENESS OF COMMON PACKERS

Using obfuscation of any kind can be beneficial for the reuse and recycling of old malware solutions. In this exercise, we will be presented with the results of how effective the usage of common packers in evading AV detection can be. Static evasion techniques are achieved by modifying the contents of the input file, with the help of packer programs, so its hash or checksum is changed and can no longer be detected using signature-based detections. Packed malicious executable files, preferably well-known ones, will face dozens of scanning engines provided by VirusTotal online service. The work of signature checkers and their databases together with static heuristic engines will be adequately tested. However, in real-life situations, there is a high chance that the packed malware will be discovered by the dynamic heuristic engines, therefore it would need more anti-AV modifications. In the conducted small-scale exercise (see Figure 4), it is noticeable that packers have an impact on the AV detection rates (for example 60/69 means how many AV engines found the file malicious out of the whole AV software pool). In this case, statistical deviation could be quite large, since rather a smaller pool of samples was part of the experiment, but it is adequate for illustrative demonstration. Still, the differences in detection capabilities could be seen, even though well-known

packer programs and malware files have been tested against the latest and time-tested signatures and static heuristic engines. Perhaps, the results would be slightly different if other than basic settings of the packers were applied. As only free trial and demo versions of software products have been tried out, some strong security features were not accessible. Almost every packer program offers dozens of options which as a result would produce unique output files each time the different option is checked. In this case, when ten software packers are used and each possible feature would be tested, there might be more than thousands of different outputs. Trying this would be hugely time-consuming and the results might be probably better, but not that significantly different. It also needs to be mentioned that the malware files were already obfuscated with several techniques including packing which was probably used even more times.

A few interesting things could be observed in Figure 4. Harmless Python executable file "py.exe" was marked as a highly suspicious file or even malware by several AV products after the packers were applied. Sometimes packed malware and regular software were evaluated as malicious by the same or similar amount of AV engines. On this note, many of the AV heuristic engines detected suspicious patterns in packed software not because of the malicious internals, but because of the unusual obfuscation and protection layer provided by tested compressors and protectors. Therefore, excessive protection measures may trigger an alarm of some AV products even if the software authors have good intentions, which in the end may prove counter-productive in practical terms. Such software solution would need to be included in the AV white list.

Samples	Original file	Compressors					Crypters / Protectors				
		MEW v1.2 [8]	MPRESS v2.19 [9]	PElite v2.4 [10]	UPX v3.94 [11]	WinRAR SFX v6.10 [12]	Enigma v7.00 [13]	Obsidium v1.7.4 [14]	PELock v2.11 [15]	Themida v3.1.1 [7]	VMProtect v3.5.1 [16]
py.exe	0/68	17/66	8/69	23/69	2/67	3/66	16/69	13/67	24/68	18/69	12/69
	0,0%	25,8%	11,6%	33,3%	3,0%	4,5%	23,2%	19,4%	35,3%	26,1%	17,4%
Artemis	29/68	23/67	14/69	15/69	ERR	1/67	18/67	19/69	11/69	22/69	12/67
	42,6%	34,3%	20,3%	21,7%	ERR	1,5%	26,9%	27,5%	15,9%	31,9%	17,9%
CryptoLocker	57/66	39/66	31/69	36/67	49/71	13/66	16/69	16/69	30/69	26/69	20/69
	86,4%	59,1%	44,9%	53,7%	69,0%	19,7%	23,2%	23,2%	43,5%	37,7%	29,0%
Kovter	60/69	42/69	ERR	36/69	ERR	12/66	21/70	14/69	26/69	26/68	30/68
	87,0%	60,9%	ERR	52,2%	ERR	18,2%	30,0%	20,3%	37,7%	38,2%	44,1%
Slammer	31/68	31/68	ERR	32/69	22/69	10/67	20/69	21/68	28/69	29/70	28/66
	45,6%	45,6%	ERR	46,4%	31,9%	14,9%	29,0%	30,9%	40,6%	41,4%	42,4%
WannaCry	64/70	45/69	ERR	40/70	ERR	10/67	36/70	30/69	36/69	33/69	30/66
	91,4%	65,2%	ERR	57,1%	ERR	14,9%	51,4%	43,5%	52,2%	47,8%	45,5%
Improvement	/	22,0%	50,2%	32,5%	25,1%	80,7%	51,2%	54,0%	44,6%	38,9%	46,2%

Fig. 4 Impact of packers on AV detection rates (tested by using VirusTotal online service)
Source: authors.

Another interesting result was achieved with the use of WinRAR compression, encryption and SFX features when the only common AV desktop solution, that caught compressed malware, was Bitdefender. To explain the process of obfuscation, the malware file was firstly compressed and encrypted with a password. Then the encrypted malware file together with a decryption script were the main parts of the executable SFX (self-extracting) archive. When the SFX archive was executed, it was set to immediately run the decryption script and afterward the decrypted malware. However, this process would be most likely intercepted by AV software at a time when the known malware file reveals itself in the memory. Despite that unfair approach, it is a demonstration of how unusually regular software can be misused for a bad purpose.

7 CONCLUSION

Even governments participate in writing malware in the form of spying on rebels or sabotaging other countries' infrastructures to protect their own interests. Whatever someone's intentions are, malware authors use several different techniques to achieve the ultimate goal which is being undetectable by any security vendor also known as FUD (Fully Undetectable). The first step is usually to encrypt malware with a strong and resilient protector (preferably with the perpetrator's unknown software solution). Then, malware authors will privately scan hundreds of unique copies of their malware with multiple AV security products (similar to VirusTotal) and choose only copies that can bypass all of them. And finally, they use zero-day exploits and cyber-attack techniques to increase the chance of a successful infection [17].

Signatures checkers and static heuristic engines are sometimes prone to mark a good file as malware. For example, when one or two VirusTotal scanning engines out of 70 identify suspicious files as a threat and dynamic analysis doesn't sound the alarm, it is most likely a false positive case. If an experienced user is sure that the file is false positive, packers could be quite helpful when you use it as a form of hiding the false positive files from your sensitive AV software, however, the new layer of obfuscation can again falsely trigger other AV solutions. Besides that, these protection tools are handy in terms of keeping your proprietary software away from prying eyes, but they are also often misused by malware authors as a form of obfuscation technique. Keep in mind that the use of a protector might result in an unwanted false positive detection, which is not acceptable during the wide distribution of your own software solutions.

References

[1] KORET, J. and E. BACHAALANY. *The Antivirus Hacker's Handbook.* John Wiley & Sons, Inc., Indianapolis, 2015. ISBN 978-1-119-02875-8. s. 360.

[2] *What is Heuristic Analysis?* [online]. [accessed 10. February 2022]. Available at: https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis

[3] *How it works?* [online]. [accessed 10. February 2022]. Available at: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

[4] *Malware analysis sandbox aggregation: Welcome Tencent HABO!* [online]. [accessed 10. February 2022]. Available at: https://virustotal10.rssing.com/chan-4742985/article104-live.html

[5] *Explained: Packer, Crypter, and Protector.* [online]. [accessed 10. February 2022]. Available at: https://blog.malwarebytes.com/cybercrime/malware/2017/03/explained-packer-crypter-and-protector/

[6] *Obfuscation: Malware's best friend.* [online]. [accessed 10. February 2022]. Available at: https://blog.malwarebytes.com/threat-analysis/2013/03/obfuscation-malwares-best-friend/

[7] *Themida.* [online]. [accessed 10. February 2022]. Available at: https://www.oreans.com/Themida.php

[8] *MEW.* [online]. [accessed 15. February 2022]. Available at: https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/MEW-SE.shtml

[9] *MPRESS.* [online]. [accessed 15. February 2022]. Available at: https://www.autohotkey.com/mpress/mpress_web.htm

[10] *PEtite Win32 Executable Compressor.* [Online]. [accessed 15. February 2022]. Available at: https://www.un4seen.com/petite/

[11] *UPX.* [online]. [accessed 15. February 2022]. Available at: https://upx.github.io

[12] *WinRAR.* [online]. [accessed 15. February 2022]. Available at: https://www.win-rar.com

[13] *Enigma Protector.* [online]. [accessed 15. February 2022]. Available at: https://enigmaprotector.com/

[14] *About Obsidium.* [online]. [accessed 15. February 2022]. Available at: https://www.obsidium.de/home

[15] *Software protection system.* [online]. [accessed 15. February 2022]. Available at: PELock Software Protection & Software License Key System

[16] *VMProtect software.* [online]. [accessed 15. February 2022]. Available at: https://vmpsoft.com

[17] *Fully UnDetectable (FUD).* [online]. [accessed 15. February 2022]. Available at: https://www.neushield.com/learn/fully-undetectable-fud/

1st Lt. Dipl. Eng. Andrej **FEDÁK** (PhD. student)
Armed Forces Academy of General M. R. Štefánik
Department of Computer Science
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: andrejfedak@gmail.com

Prof. Dipl. Eng. Jozef **ŠTULRAJTER**, CSc.
Armed Forces Academy of General M. R. Štefánik
Department of Computer Science
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: jozef.stulrajter@aos.sk

Andrej Fedák was born in Žiar nad Hronom in 1994. He received his engineering degree from the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in the field of Military Communication and Information Systems. He is currently an officer of aeronautical ground information systems - Air Force Headquarters. His research is focused on computer networks, information systems, information and cyber security.

Jozef Štulrajter works as a professor at the Department of Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. He graduated (Ing.) at the Military Technical College in 1974. He obtained the degree of CSc. diploma in Theoretical Electrical Engineering - Theory of Circuits and Systems of the Military Academy in Liptovský Mikuláš in 1992. His research interests include Information and Communication Technology (ICTs), computer architectures, image coding, computer security.

DOI: https://doi.org/10.52651/sam.a.2022.1.23-28

SEARCHING FOR THE CAUSES OF ABNORMALLY FAST DEGRADATION OF ENGINE OIL IN A DIESEL COMBUSTION ENGINE

Pavol LUKÁŠIK, Vladimír KADLUB, Jindřich STEHLÍK

Abstract: Today, modern tribodiagnostics offers sophisticated analyzes of motor oils with fast and accurate results. However, finding the causes of some undesirable processes of engine oil degradation often requires long-term monitoring of the operating facility. In this case, it was a problem of diesel engine oil in the Citroën Jumpy 2.0 HDi service minibus, which has been in use by the Department of Mechanical Engineering (Armed Forces Academy of General M. R. Štefanik, Demänová) for more than 13 years. The fuel system (conditioners of injectors) on this vehicle has also been monitored for a long time in the period 2019-2021, an article about it was also published in the journal Science & Military (No. 2 / Vol. 14/2019). The cadets of the Deptartment of mechanical engineering Armed Forces Academy of General M. R. Štefanik, were also involved in the diagnostic process. In parallel with the fuel system, the quality of the engine oil was regularly monitored in the time interval 20.1.2020 - 22.4.2021 at a start of 2185 km from the last oil change. During this monitoring, a very rapid degradation of engine oil was found in some parameters, which is atypical during normal vehicle operation. This article discusses the measured results and possible causes of this adverse event.

Keywords: Tribology; Tribodiagnostics; Engine oil; Diesel engine; Engine oil parameters; Carbon black content.

1 INTRODUCTION

From the point of view of maintaining competitiveness on the market, very high demands are placed on today's high-performance motor oils. These are technologically very complex products with a number of parameters that must meet performance parameters under different load conditions. Despite the time and mileage declaration of the service life interval from the manufacturer, there may be cases where there is an accelerated degradation action and the associated risk of premature wear.up to the crash limit engine. The service life of the engine oil is determined by a set of operating factors (eg. cold starts, number of starts, operator's approach to gradually warm up the engine to operating temperature, technical condition of the engine, vehicle load, length of operating distances, operation in difficult terrain, operation in dusty environment etc.). It is the operation of technology in the Armed Forces of the Slovak Republic that is significantly influenced by the above factors. Therefore, in order to maintain the combat capability and reliability of military equipment, it is necessary to pay increased attention to monitoring and evaluating the degradation of motor oil. [1]

Lubricating oil is often exposed to unforeseen operating conditions that affect its service life. We know 3 general criteria that determine the reason for changing the lubricating oil. These include the degradation of the base oil, the loss of additives and impurities in the lubricating oil. The degradation of the base oil itself can be caused by the ongoing oxidation process, thermal degradation (hot spots) and chemical degradation. The choice of lubricating oil, the choice of base oil and suitable additives, or the loss of additives also have a certain influence on the degradation of the lubricating oil. [2]

Additives are added to base oils to reduce destructive processes and improve beneficial properties. For example, antioxidant additives help slow down the oxidation rate. Detergent additives help prevent deposits and sludge. Anti-wear additives are added to some engine oils to form a layer on metal components and prevent wear. The depletion of additives is one of the main reasons why engine oil loses its effectiveness and must be changed. Although all engine oils deteriorate over time, synthetic oils last longer than conventional oils and provide improved protection against wear and deposits. [3]

2 OBJECT DIAGNOSTIC MONITORING

The request for tribodiagnostic monitoring came from the vehicle operator, ie from the Dept. of Mechanical Engineering AOS Lipt. Mikuláš, which has been using the vehicle since 2008 to fulfill transport tasks. The vehicle is subject to high requirements in terms of functionality and reliability.

2.1 Fuel system problem

The problem with the fuel system has been solved since 2019 - the diagnostics revealed an uneven supply of fuel through the injectors due to their clogging with carbon. The initial solution to the problem was an intensive cleaning treatment of the fuel system by using cleaning additives for diesel. This cleaning process has had positive effects on the fuel system. Injector values have approached an almost ideal, i.e. uniform fuel supply (Graph 1).

However, this can be a problem for the operation of the oil change, as the fuel additives are characterized by high cleaning effects and aggressiveness. The influence of the cleaning system of the fuel system therefore has a negative impact on the quality of the oil filling. And this is what the next

part of the article discusses. This was a specific operating stage of the vehicle (from 20.1.2020 to 22.4.2021 at the start of 2185 km since the last oil change), when the fuel (diesel) was significantly concentrated with cleaning additives VIF Super Diesel Additive for winter and summer operation of he vehicle. (Fig. 2). Additive preparations were continuously added to the fuel at each refueling of the vehicle in the maximum recommended doses, resp. in slightly exceeded quantities (the manufacturer does not consider an overdose to be harmful to the engine and fuel system).

Company car tested (Armed Forces Academy of General Milan Rastislav Štefánik, Department of Mechanical Engineering, Demänová): Citroën Jumpy 2.0 HDi

Engine 2.0 HDi specification:

- Power (kW): 88 kW
- Horsepower: 120 hp
- Horsepower: 118 bhp
- Rev. at Max Power: 4000 / min
- Torque: 300 Nm
- Torque (lb-ft): 221 lb-ft
- Rev. at Max Torque: 2000 / min
- Displacement: 2 l
- Displacement: 1997 cc
- Number of Cylinders: 4
- Number of Valves per Cylinder: 4
- Bore: 85 mm
- Stroke: 88 mm
- Compression Ratio: 17.6: 1
- Common Rail Diesel System

INCLUDE PICTURE "http://shared.autorubik.sk/upload/2014/06/citroen_ew7j4.jpg" \ * MERGEFORMATINET

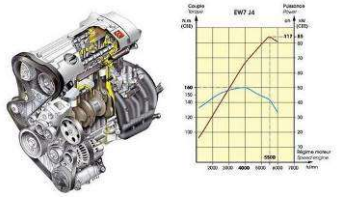
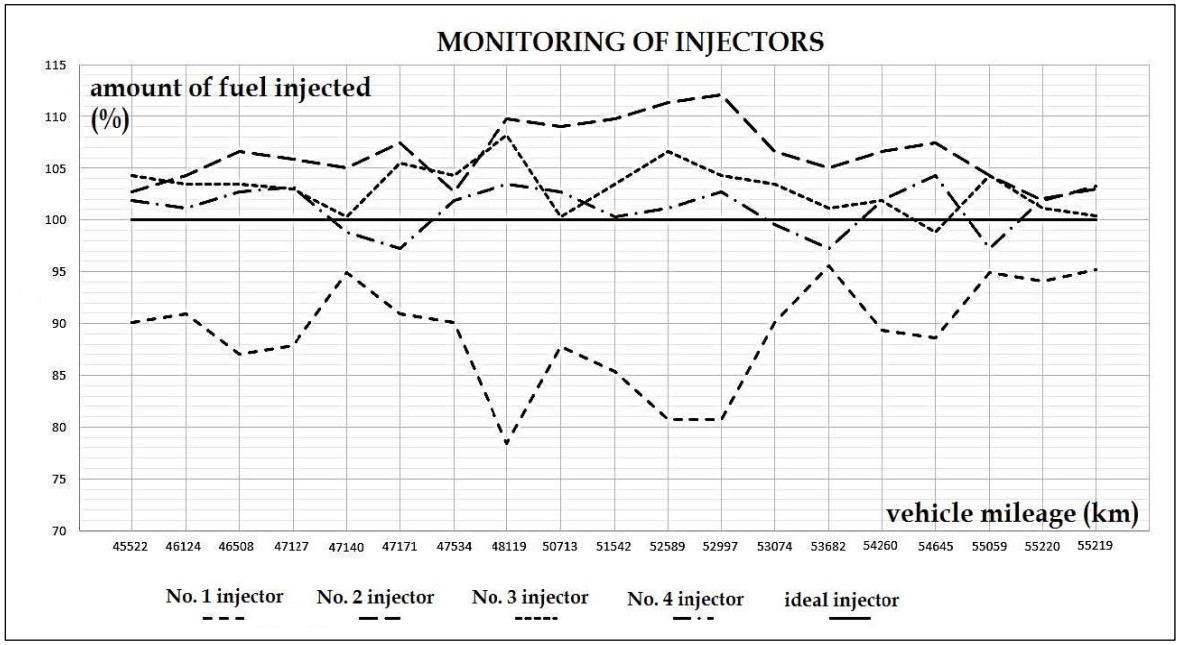


Fig. 1 Monitored vehicle Citroën Jumpy 2.0 HDi
Source: authors [5, 6].

Fig. 2 Additives added to diesel
Source: authors.

VALVOLINE Syn Power
XL III Full Synthetic
SAE 5W-30
ACEA C2, C3, A3 / B4
BMW LL-04MB 229.31;
229.51VW 504.00,
07.00Porsche C30

Fig. 3 Engine oil specification
Source: authors.



Graph 1 Condition of injectors in the period 13. 5. 2019 - 22. 4. 2021 during the start of 9998 km
Source: [4].

Table 1 Current quality of VALVOLINE Syn Power XL III 5W-30 oil filling in the period 20. 1. 2020 to 22. 4. 2021 at the start of 2185 km

vehicle operation	1/21/2020 *	8/13/2020	9/7/2020	9/8/2020	9/9/2020	2/2/2021	4/22/2021	allowed values	results for vehicle operation
	engine oil change at 53035 km	route: AOS - Bratislava and back	route: AOS - Bratislava and back	route: AOS - Nitra and back	route: AOS - Trebisov and back	route: AOS - Sučany and back	route: AOS area - AOS area		
	mileage of the car: 0 km	mileage of the car: 647 km	mileage of the car: 1225 km	mileage of the car: 1610 km	mileage of the car: 2024 km	mileage of the car: 2185 km	mileage of the car: 2185 km		
oil parameter	total mileage of the car: 53035 km	total mileage of the car: 53682 km	total mileage of the car: 54260 km	total mileage of the car: 54645 km	total mileage of the car: 55059 km	total mileage of the car: 55220 km	total mileage of the car: 55220 km		
Glycol (%)	0	0	0	0	0	0	0	max. 0	passes
Oxidation (abs /0,1)	19,2	22,1	25,1	20,5	21,9	24,2	32,4	max. 40	passes
Soot (% wt)	0	0,49	0,53	0,61	0,64	0,70	0,71	max. 3	passes
Sulfation (abs /0.1)	23,9	24,4	24,5	23,7	23,9	24,6	26,7	max. 40	passes
TBN parameter (mg.KOH/g)	8,1	7,1	5,8	6,9	6,7	6,0	3,5	min. 3	passes
Water content (ppm)	239	112	133	76	217	119	221	max. 5000	passes
Kinematic viscosity at 40 ° C (mm^2/s)	72,7	79,5 (+ 9,3%)	79,4 (+ 9,2%)	79,4 (+ 9,2%)	81,1 (+ 11,6%)	83,8 (+ 15,3%)	80,05 (+ 10,11%)	max. difference ± 20% compared to the new sample	passes
Kinematic viscosity at 100 ° C (mm2/s)	12,4	13,3 (+ 7,3%)	13,2 (+ 6,5%)	13,2 (+ 6,5%)	13,5 (+ 8,9%)	13,8 (+ 11,3%)	13,3 (+ 7,3%)	max. difference ± 20% compared to the new sample	passes

* Reference (new) engine oil comparison sample VALVOLINE Syn Power XL III 5W-30.

2.2 The problem with fast engine oil degradation

Oil sampling of the Citroën Jumpy 2.0 HDi was carried out during operation, usually after returning from business trips. The oil sample of the Dutch manufacturer VALVOLINE (Fig. 3) was subsequently subjected to analysis by modern instruments in the tribodiagnostic laboratory of the Department of Mechanical Engineering (Fig. 4).

Fig. 4 Tribodiagnostics laboratory
Source: authors.

The kinematic viscosity of the oil sample was evaluated with a Spectro Visc Q-3050 optical-electronic instrument.

Chemical parameters were evaluated with a Fluid Scan Q-1000 FTIR method. Infrared spectrometry with Fourier transformation (FTIR spectrometry) is an optical non-destructive analytical method, which is providing quick and complex information about the state of used lubricant. One of the FTIR spectrometry advantages in comparison to the classical methods, the contamination by foreign substances does not occur. It is also possible to discover the change of sample quality caused by mixing with another oil type or another working liquid, or such fact exclude. They are devices working on emission interference principle, which in comparison with dispersion devices measuring the interferogram of emission modulated beam after the transit through the sample. These devices are requiring application of Fourier mathematical method (cosines) transformation, in order to get classical spectral record. [7]

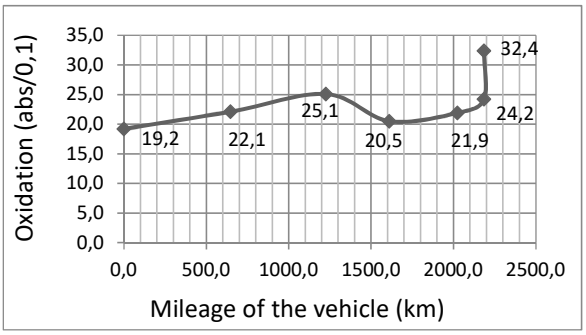
$$I(d) = \int_{-\infty}^{\infty} I(\tilde{v})\cos(2\pi d\tilde{v})\,d\tilde{v} \qquad [7]$$

I - emission intensity,
d - way difference of patterned rays,
v ~ - wave number (1 /λ)

One of the methods ascertaining the properties changes of worn or otherwise devalued lubrication oil, fuel or another mixture by help of FTIR spectrometry it is a technique of used and new liquid spectrums subtraction. [7]

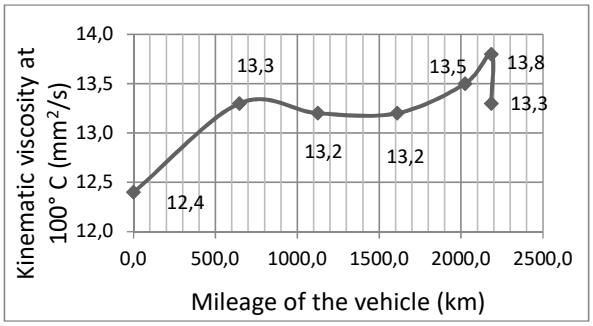
Table (Table 1) contains the measured data - the course of the change of individual physico-chemical parameters of the engine oil depending on the mileage operation of the vehicle. After passing each route, seven tribodiagnostic measurements of the oil sample were performed. In the following section, the individual diagrams show the most significant degradation changes of the monitored physico-chemical parameters of the engine oil.

The primary physical parameter - the kinematic viscosity of the oil during the monitored operating interval was within the allowed values, did not exceed the allowed range ± 20 percent compared to the reference sample (Graph 2).

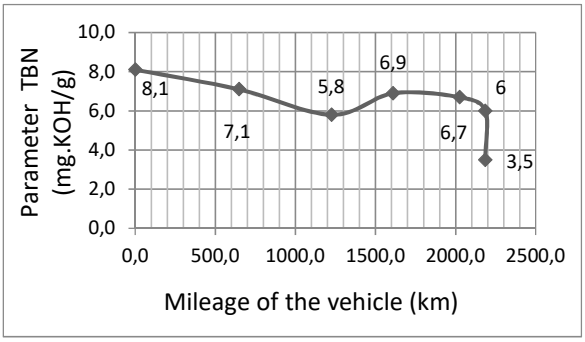


Graph 2 Kinematic viscosity profile at 100 °C
Source: authors.

Engine oil showed quite good oxidative stability during the observed interval (Graph 3). Apart from the last measurement, no significant increases and decreases in oxidation were recorded.

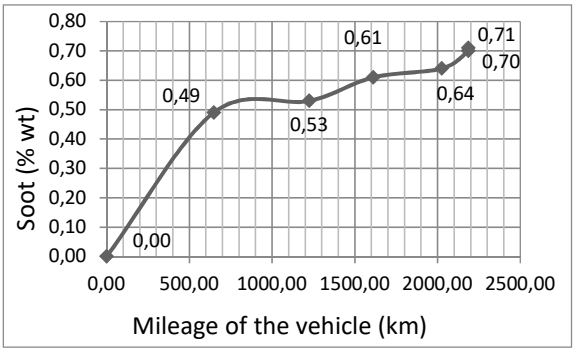


Graph 3 Oxidation process in engine oil
Source: authors.



Graph 4 Course of the TBN parameter in engine oil
Source: authors.

Engine oil maintained a relatively stable base reserve TBN (total base number) during the reporting interval (Graph 4). However, the last measurement showed a significant decrease to 3,5 mg/KOH and a dangerous approach to the permitted minimum value of 3 mg/KOH. This parameter, which affects the corrosivity of lubricating nodes, proved to be the least stable in the oil filling after the 2185 km run-in (as is traditional) and significantly worsened the overall chemical picture of the oil filling.



Graph 5 The course of carbon black content in engine oil
Source: authors.

Regular measurements showed a significantly increasing soot content during the entire operating interval (Graph 5). This phenomenon is given the most attention in this article.

Soot is burned when diesel is burned in diesel engines. Most of the soot leaves the combustion chamber with exhaust gases, but some of them also gets into the engine oil. If an EGR valve is installed in the engine, part of the exhaust gases return to the cylinder, thus increasing the amount of soot that penetrates the engine oil. Soot generated in the engine can cause hard sludge, high lubricant viscosity or oil gelling. The carbon black is made of almost pure carbon, which is hard, has sharp edges and causes blackening of the oil. The limit value for the carbon black concentration in the oil is 3% wt. The large amount of soot in the engine oil not only causes an increase in its viscosity and thus wear of the engine. It can also result in depletion of dispersants. The soot then accumulates into larger dimensions and there is a risk of clogging of the oil filter and failure of the oil supply to the entire system. [8]

Although in tribodiagnostics the maximum value of carbon black content is allowed at the level of up to 3 % wt, the value of 0,71 % wt is very high after only 2185 km. This probably also points to the cleaning effects of the added additives in the fuel, which significantly release carbon deposits in the working space of the engine and subsequently get into the oil charge. The intensive cleaning procedure of the fuel system with the help of cleaning additives in the fuel has, with a certain probability, resulted in a significantly faster degradation of the oil filling than under normal vehicle operating conditions. In practice, the impact of cleaning agents on the quality of the oil should have only a negligible impact, but the measured values show that the new oil filling recorded a very significant increase in soot content and kinematic viscosity during the first 2185 km. The increased carbon black content can be attributed to the cleaning effect of the additives in the diesel, which gets into the oil especially during cold starts. The carbon deposits in the combustion chamber of the engine were dissolved while operating and subsequently entered into the oil charge. The result has just been an increasing concentration of carbon black in the engine oil. The soot in the form of solid particles, due to their thickening effect, also caused a decrease in the fluidity of the oil, i.e. there was a gradual increase in the kinematic viscosity. Figuratively, the comparison that the oil level after the first 2185 km showed results, as in normal circumstances at a range of several times more kilometers, or as a vehicle with a heavily worn engine (the vehicle reached a total start-up of only 55220 km at the end of the measurement - considers with negligible engine wear).

Even after a relatively low mileage, the 13 - year - old engine was characterized by high working space (carbonation), as evidenced by clogged injectors at the beginning of the cleaning treatment, as well as rapid oil degradation during cleaning. The cleaning process in the monitored period was significantly helped by the operation of the vehicle over long distances (in the order of hundreds of kilometers), mainly on highways, where the engine operated for a long time at high speeds and engine operating temperature.

The other monitored oil parameters did not show any special deviations from the standard course of degradation. It is also worth mentioning the water content parameter, which was lower during operation than with the new oil filling, precisely due to the operation of the vehicle, mainly over long distances, where the water evaporated from the oil filling.

However, during the last measurement (after a longer service downtime), a sharp, almost step change in all physicochemical parameters was recorded (Graph 2-5), which also indicates a significant increase in engine oil degradation. In this case, the oil degraded significantly even during a long downtime.

3 CONCLUSION

The tribodiagnostic analysis of the oil level, despite the low start-up (2185 km), provides important information for the vehicle user, especially the fact about the end of the oil level's life in the near future. In previous random sampling of the oil (when no cleaning agents had yet been added to the fuel), the degradation of the engine oil was not as significant as during this cleaning stage. An important factor in the significant degradation of oil was also the time aspect - the age of the oil (20.1.2020 - 22.4.2021).

It follows from the above that the vehicle operator should, as far as possible, pay due attention not only to the fuel system but also to the engine lubrication system. The relative cleanliness of the systems can be ensured mainly by using quality media and regular replacement of filter components. It is also recommended to add additives to the fuel on a regular basis. However, in the case of more intensive cleaning processes (as in this case), it is also necessary to monitor the quality of the engine oil or to change the oil preventively before the vehicle manufacturer prescribes it. In such cases, it is recommended to change the engine oil after starting the vehicle for 5000 km (max. 7000 km), or after a time of max. 2 years.

References

[1] LUKÁŠIK. P. and M. MARKO. *Deterioration dependability diagnostics. Monitoring of motor oils degradation by the operation of the vechiles 155mm ShKH Zuzana type 2000*, 2017. ISBN 978-80-7582-009-9.

[2] *Guidelines for diesel engines lubrication.* [online]. Available at: https://www.cimac.com/cms/upload/Publication_Press/Recommendations/Recommendation_22.pdf

[3] ČERNÝ. J. *Vlastnosti motorových olejů Oxidační stabilita, nitrace olejů.* [online]. Available at : https://www.oleje.cz/clanek/Vlastnosti-motorovych-oleju-Oxidacni-stabilita-nitrace-oleje

[4] HALUŠKA, M. *Diagnostika a ošetrovanie palivovej sústavy vznetových motorov osobných vozidiel v OS SR.* Bakalárska práca. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, 2021.

[5] *Citroën JUMPY. Príručka na údržbu, obsluhu a záruky.* Creátion 4D Concept Automobiles Citroën – RCS Paris 642050199, Imp. en U. E. 06/09, ENT-SQ-9006/2, 2006.

[6] *Citroën JUMPY. Návod na obsluhu.* Creátion 4D Concept Automobiles Citroën – RCS Paris 642050199 – Edition ALTAVIA/ PRODITY, Imp. en U. E. 06/09, G9VU – SQ – 2006.

[7] HURTOVÁ. I. and M. SEJKOROVÁ. *Analysis of Engine Oils Using Modern Methods of Tribotechnical Diagnostics. Perner's Contacts*, *11**(4)***, 47–53, 2016, Available at: https://pernerscontacts.upce.cz/index.php/perner/article/view/569

[8] HURTOVÁ. I. *Hodnocení karbonového znečištení motorových olejů. Perner's Contacts*, *15***(2)**, 2020. Available at: https://doi.org/10.46585/pc.2020.2.1652

Dipl. Eng. Pavol **LUKÁŠIK**
Armed Forces Academy of General M. R. Štefánik
Department of Mechanical Engineering
Demänová 393
031 01 Liptovsky Mikulas
Slovak Republic
E-mail: pavol.lukasik@aos.sk

Dipl. Eng. Vladimir **KADLUB**
Armed Forces Academy of General M. R. Štefánik
Department of Mechanical Engineering
Demänová 393
031 01 Liptovsky Mikulas
Slovak Republic
E-mail: vladimir.kadlub@aos.sk

Bc. Jindřich **STEHLÍK**
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovsky Mikulas
Slovak Republic
E-mail: jindrich.stehlik@aos.sk

Pavol Lukášik was born in Liptovský Mikuláš, Slovakia in 1980. He received his M. Sc (Ing.) at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in 2004. He started his dissertation studies in 2017. His research interests are focused on tribology and diagnostic. He is currently working as an assistant professor at the Department of Mechanical Engineering, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. He is a member of the Slovak Society for Tribology and Tribotechnics (SSTT).

Vladimir Kadlub was born in Trstená, Slovakia in 1981. He received his M.Sc (Ing.) at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in 2004. He started his dissertation studies in 2019, his research interests are focused on repairs and maintenance. Currently he is working as an assistant professor at the Department of Mechanical Engineering, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Jindřich Stehlík was born in Levice, Slovakia in 1999. He received his M.Sc (Bc.) at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in 2021. He started his engeneering studies in 2021, in the ZSZČ study section.

DOI: https://doi.org/10.52651/sam.a.2022.1.29-36

THE HUMAN INTERFACE DEVICE (HID) ATTACK ON ANDROID LOCK SCREEN NON-BIOMETRIC PROTECTIONS AND ITS COMPUTATIONAL COMPLEXITY

Sebastián POTOCKÝ, Jozef ŠTULRAJTER

Abstract: Nowadays, information obtained from mobile phones is often the subject of evidence in front of a court. Forensic analysts often come across smartphones about which they have no prior information. However, they need to extract data from them. The main prerequisite to extract the data is to bypass Android lock screen protection. The HID attack is a promising method to break Android lock screen protection. In many cases, this is the only way how to break the smartphone´s non-biometric lock screen protections on newer Android OS versions. The article contains examples of three non-biometric types of Android smartphone lock screen protections and their computational complexity. The paper describes hardware and software requirements for implementation of HID attack.

Keywords: Android; HID; Attack; Bypass; Protection; PIN; Pattern; Password.

1 INTRODUCTION

It is not an impossible task to break into a locked device and access the data. There are various ways how their lock screens can be breached or bypassed. Some of them are applicable for all Android devices, or all possible situations. Generally, there are three common techniques how to access data from Android devices. They are manual, logical and physical data acquisitions [1].

Manual acquisition utilizes the user interface to investigate the contents of the phone´s memory and it only acquires the data that appears on the mobile phone. Manual extraction introduces a greater degree of risk in the form of human error, and there is a chance of deleting evidence [1].

Physical acquisitions like imaging an Android phone, JTAG (join test action group), the chip-off technique is a bit-by-bit copy of the physical storage. From Android version 6.0 is encryption turned on by default with full disk encryption or file based encryption and not like a user option and therefore the JTAG and chip-off techniques are almost useless. Thus, this work will not deal with physical acquisition of data due to the encryption mentioned [1].

Logical acquisition extracts logical storage objects, such as files and directories that reside on a filesystem. It contains ADB pull data extraction, ADB dumpsys extraction, ADB backup extraction, browsing SQL data. Data obtained by logical extraction such as call history, SMS/MMS, photos, videos, documents, calendars, GPS locations, browser history information, social networking chats, backup extraction, dumpsys extraction are usually sufficient to clarify the case [1].

The main prerequisite for a successful logical acquisition is to break the locked screen protection of device. Device´s lock screen protection types are divided into biometric and non-biometric ones and can be bypassed with root privileges, but, in some cases, also without them [1].

Rooting usually wipes the phone, so all your files (non-system files) are unlinked, deleted [1].

A human interface device (HID) attack is a simulation of human activity programmatically. A HID attack vector is a combination of customized hardware and restriction bypass via mouse or keyboard emulation [2].

It is a scenario in which an attacker takes a programmable embedded development platform such as the Teensy, Arduino or in our case smartphone and an associated software package to create a USB device which, when plugged into a smartphone, will execute a pre-configured set of keystrokes to break the lock screen protection and allow the logical acquisition [2].

There are two main advantages of the HID attack. The locked phone does not need to be rooted. There is no need to enable USB debugging. USB debugging allows an Android device to communicate with a computer that's running the Android SDK tools in order to use advanced operations [1] [2].

Based on this, HID attack is a promising method for obtaining data from Android devices.

This attack can be executed on the non-biometric lock screen protections, such as pin, pattern or password.

The goal of this paper is to explain the HID attacks and describe their input structure and computational complexity.

2 TYPES OF NON-BIOMETRIC LOCK SCREEN PROTECTIONS AND THEIR COMPUTATIONAL COMPLEXITY

Complexity is a measurement of how fast and efficient an algorithm performs based on an input size and situation in which the algorithm has to run [3].

Computational complexity is divided into two types, memory complexity and time complexity [3].

Memory complexity measures how much computer memory the algorithm would take. Memory

requirement is irrelevant in HID attack, given the huge resources modern computers possess [3].

Time complexity measures approximate number of operations an algorithm takes when processing an input of a certain size [3].

The vital pointer is time requirement which is mostly affected with timeouts during the HID attack. Timeout is a certain period of time that the user has to wait before entering a new combination of pin, pattern or password after too many incorrect attempts have been entered [4].

Each manufacturer specifies different types of timeouts for different types of their phones. There is no way to bypass timeout without previous exploiting. Even though, timeouts are a means of protection against brute force attacks, but, in some cases, it is still possible to execute a HID attack [4].

For instance, Samsung smartphones use timeouts which are mentioned below [4]:

- After 1-5 wrong attempts – 1x 30 seconds timeout.
- After 6-10 wrong attempts – 1x 30 seconds timeout.
- Between 11-41 wrong attempts – 30 seconds timeout after each wrong attempt.
- After 41 wrong attempts – 60 seconds timeout after each wrong attempt.

2.1 Invalid attempt

Each attempt must meet some minimum requirements. If the entered attempt to break the PIN, pattern and password does not meet even the minimum requirements, this attempt is not affected by the timeout.

When a PIN, passcode or pattern consisting of fewer than four characters are entered ("entered" meaning followed by the "Enter" key), Android does not consider that an actual unlock attempt. It will show no message from the Android Lock Screen saying "Failed Attempt", "Try Again," etc. Incorrect Passcode event wouldn't trigger due to an incomplete attempt. If the input is four digits or greater, Android will display a message along the lines of "PIN incorrect, please try again" or "Wrong PIN" [5].

Therefore, inputs smaller than 4 digits or characters, will not be taken into account during measures.

2.2 PIN

Rules:

- Software requirement of a PIN input in android devices prerequisite minimum 4 digit input, but no more than 16 digit input, which consist of Arabic numerals.

A formula for computational complexity is variation with repetition.

$$V_n^k = n^k \tag{1}$$

The table below shows the time complexity of breaking an Android screen protected by a PIN of different lengths. Total time was calculated from the number of attempts executed in the worst-case and the timeouts of Samsung smartphones between incorrect attempts which were mentioned in section 2.

Tab. 1 Time complexity (total attempts) of check all PIN inputs calculated with the formula of variation with repetition

n	k	Total attempts	Total time
10	4	10 000	6,927 days
10	5	100 000	69,427 days
10	6	1 000 000	1,902 years
10	7	10 000 000	19,025 years
10	8	100 000 000	190,258 years
10	9	1 000 000 000	1902,587 years
10	10	10 000 000 000	19025,874 years

Source: author.

2.3 Pattern

A valid unlock pattern should follow the following rules:

- A pattern should connect at least 4 dots.
- A dot can be connected only once, meaning that
  a pattern connects no more than 9 dots.
- A pattern will always connect the first unconnected dot along its path. Then it may go further to connect other unconnected dots.
- A pattern can go through a previously connected dot along its path in order to connect an unconnected dot [6].

At first glance, it might seem that the total number of attempts is calculated using variation without repetition formula. However, because of the limitations mentioned above it is much less.

$$V_n^k = \frac{n!}{(n-k)!} \tag{2}$$

For comparison, the table below shows the computational complexity of the PATTERN, if it were calculated according to the variation without repetition formula.

Tab. 2 Time complexity (total attempts) of check all PATTERN inputs calculated with the formula of variation without repetition

n	k	Total attempts	Total time
9	4	3024	2,083 days
9	5	15120	10,483 days
9	6	60480	41,983 days
9	7	181440	125,994 days
9	8	362880	251,983 days
9	9	362880	251,983 days

Source: author.

Problem of all valid PATTERNs was solved by generating all patterns that follow the rules described above. [6], [7].

The table below shows the time complexity of breaking an Android screen protected by the PATTERN of all possible combinations in a 3 x 3 grid, which is default option in the most smartphones. Total time was calculated from the number of attempts executed in the worst-case and the timeouts of Samsung smartphones between incorrect attempts which were mentioned in section 2.

Tab. 3 Size statistics of all valid patterns

n	k	Total attempts	Total time
9	4	1624	1,079 days
9	5	7152	4,949 days
9	6	26016	18,049 days
9	7	72912	50,616 days
9	8	140704	97,694 days
9	9	140704	97,694 days

Source: [6].

The table below proves, that real computation complexity of PATTERN is on average 2,3x less than expected.

Tab. 4 Comparing of real computation complexity with variation without repetition

n	k	Variation without repetition	Real computation	Total
9	4	3024	1624	1,862x less
9	5	15120	7152	2,114x less
9	6	60480	26016	2,325x less
9	7	181440	72912	2,488x less
9	8	362880	140704	2,579x less
9	9	362880	140704	2,579x less

Source: author.

2.4 Password

Rules:

- Software requirement of a password input in Android devices prerequisite minimum 4 character input, but no more than 16 character input, which consist of small letters, capital letters with or without diacritics (it depends on language), Arabic numerals and special characters.

A formula for computational complexity is variation with repetition (1).

The tables below show the time complexity of breaking an Android screen protected by a PASSWORD of four and five digits lengths. PASSWORDs containing lowercase, uppercase, and numbers are included in the comparison. Total time was calculated from the number of attempts executed in the worst-case and the timeouts of Samsung smartphones between incorrect attempts which were mentioned in section 2 [8].

Tab. 5 Four digits password

Small letter	Capital letter	Numbers	n	k	Total attempts	Total time
YES	NO	NO	26	4	456 976	317 days
YES	YES	NO	52	4	7 311 616	13,910 years
YES	YES	YES	62	4	14 776 336	28,113 years

Source: author.

Longer PASSWORDs are irrelevant for comparison due to their high computational complexity already with a 5-character password, a significant increase can be seen.

Tab. 6 Five digits password

Small letter	Capital letter	Numbers	n	k	Total attempts	Total time
YES	NO	NO	26	5	11 881 376	22,605 years
YES	YES	NO	52	5	380 204 032	723,371 years
YES	YES	YES	62	5	916 132 832	1743,022 years

Source: author.

Special characters that would only increase the computational complexity were not taken into account in the comparison.

2.5 Overview of time complexity

Up to now, HID attack has been described as a brute-force attack with timeouts. Looking at the time complexity, it is clear that HID attack is not effective in every case. It does not make sense to run attack that can last several years in the worst case. Every HID attack should finish within a reasonable time.

Therefore, it is desirable to know the time complexity of each case in the worst case.

The Table 6 below shows the time complexity of non-biometric Android lock screen protections from the weakest to the strongest.

Tab. 7 Overview of type protections and their time complexity

Type of protection	Time complexity in worst case
4 dots pattern	1,079 days
5 dots pattern	4,949 days
4 digits pin	6,927 days
6 dots pattern	18,049 days
7 dots pattern	50,616 days
5 digits pin	69,427 days
8 dots pattern	97,694 days
9 dots pattern	97,694 days
4 digits password from small letters	317,327 days
6 digits pin	1,902 years
4 digits password from small and capital letters	13,910 years
7 digits pin	19,025 years
5 digits pin from small letters	22,605 years
4 digits password from small, capital letters and numbers	28,113 years
8 digits pin	190,258 years
5 digits password from small and capital letter	723,371 years
5 digits password from small, capital letters and numbers	1743,022 years
9 digits pin	1902,587 years
10 digits pin	19025,874 years

Source: author.

It is obvious that the 5 dot long pattern is similar in strength to a 4 digit PIN combination and a 7 dot long pattern is similar in strength to a 5 digit PIN combination. However, a 6 digit PIN is already more secure than all the patterns combined together.

Breaking a 6 or more digit PIN with brute-force is irrelevant, because it will take a lot of time.

As it can see on table above, HID attack of passwords is computationally intensive.

Otherwise, the time complexity can be significantly decreased by entering password´s inputs successive from the most to the least probable, like in the dictionary attack. There is no other effective option because random guessing of letters is ineffective.

The difference with brute force attack is that, in brute force, a large number of possible key permutations are checked whereas, in the dictionary attack, only the words with the most possibilities of success are checked and therefore it is less time consuming than the brute force one.

There are many articles that deal with the probability of selected pins, passwords or patterns according to human psychology [9], [10], [11].

Locked and attack devices have the ports for charging their batteries occupied during the whole HID attack. It is necessary to interrupt the attack while recharging the batteries. This situation can occur several times during an attack [4].

Therefore, the total time of breaking a lock screen protection will be affected by charging time of the locked or attack devices.

3 HARDWARE AND SOFTWARE REQUIREMENTS

There are many tools that can perform a HID attack like Rubber Ducky [12], Teensy [13], Cellebrite [14], XPIN Clip [15], etc. However, these solutions require special hardware and no documentation is published, as they are commercial paid tools.

First of all, we have to create a cracking device. It means we need a rooted Android device with HID kernel support. The most famous software is Kali NetHunter. Kali NetHunter is a free and open-source mobile penetration testing platform for Android devices, based on Kali Linux. However, Kali NetHunter is not necessity. The most important thing is to prepare enabled HID endpoints and these are then mirrored to our victim device.

The basic HID handling is done in the kernel, and HID reports can be sent/received through I/O on the /dev/hidgX devices (keyboard, mouse, joystick). For our purposes it is /dev/hidg0 for keyboard and /dev/hidg1 for mouse [16].

To use these devices properly, formatted input has to be sent to them.

3.1 USB keyboard keypress mechanism

Report format must be created according to certain rules and must be of a certain length.

The USB keyboard report may be up to 8 bytes in size, although not all these bytes are used, it's possible to implement a proper implementation using only the first three or four bytes [17].

Tab. 8 B.1 Protocol 1 (Keyboard)

Byte	Description
0	Modifier keys
1	Reserved field (unused/reserved for OEM)
2	Keypress 1
3	Keypress 2
4	Keypress 3
5	Keypress 4
6	Keypress 5
7	Keypress 6

Source: [18].

Not every character on the keyboard corresponds to a single keystroke. To write uppercase letters, special characters and diacritics is necessary to use modifier keys.

Modifier keys in HID report is a bitfield, where each bit corresponds to a specific modifier key. When a bit is set to 1, the corresponding modifier key is being pressed [18].

Tab. 9 The bit structure of modifier keys byte

Bit	Bit Length	Description
0	1	Left Ctrl
1	1	Left Shift
2	1	Left Alt
3	1	Left GUI (Win/Super key)
4	1	Right Ctrl
5	1	Right Shift
6	1	Right Alt
7	1	Right GUI(Win/Super key)

Source: [17].

Reserved field in report format is unused or reserved for OEM (original equipment manufacturer). This byte is reserved by the USB HID specification, and thus software should ignore it [17].

Keyboard report can indicate up to 6 keypresses. All these values are unsigned 8-bit values [17].

The exact description of keypresses is in the specification of HID Usage Tables for Universal Serial Bus version 1.22 expressed by Usage ID.

Usage IDs are part of the HID Report descriptor and supply an application developer with information about what a control is actually measuring or reporting. During HID attack Usage ID determines key codes to be used in implementing a USB keyboard [19].

For instance, sending a Capital H in normal keyboard requires press Right shift and small h. Right shift keystroke requires the fifth bit set to 1. Binary number 00100000 is converted to hexadecimal number 20. Usage ID of keystroke of small h letter is 0B. These values are pasted into the correct location in the keyboard report. The report can be sent to /dev/hidg0 device using long version or short version of the report.

Long version of the report:
\0x20\0x00\0x0B\0x00\0x00\0x00\0x00\0x00

Short version the report:
\x20\0\x0B\0\0\0\0\0

3.2 USB mouse X, Y movement

During creating a USB HID report is important to take account that graphical pattern is not a set of random numbers or characters like at PINs or PASSWORDs.

The structure of the PATTERN can be imagined as a set of consecutive lines that are connect at a common point.

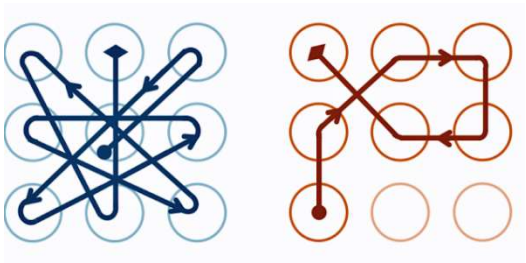


Fig. 1 Example of pattern
Source: [20].

Each line can be drawn using a Cartesian coordinate system with X and Y coordinates.

Therefore, each line will be the separate input in the proper format.

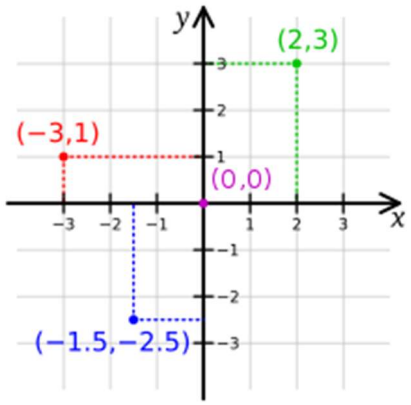


Fig. 2 Cartesian coordinate system
Source: [21].

USB mouse, just like any other HID device, communicate with the software using reports, which are sent via endpoints. Only the first three bytes of the USB mouse report are defined. The remaining bytes, if exist, may be used for device-specific features [17].

Tab. 10 B.2 Protocol 2 (Mouse)

Byte	Bits	Descriptions
0	0	Button 1
	1	Button 2
	2	Button 3
	4 to 7	Device-specific
1	0 to 7	X displacement
2	0 to 7	Y displacement
3 to n	0 to 7	Device specific (optional)

Source: [18].

When pattern is drawing to smartphone screen, finger is in contact with the screen all the time. It is equivalent to create a line in computer screen when the left button of the computer´s mouse be pressed during a mouse movement. In the USB mouse report is button status set in the first byte. This byte is a bitfield, in which the lowest three bits are standard format. The remaining 5 bits may be used for device-specific purposes [17].

Tab. 11 The bit structure of button status

Bit	Bit Length	Description
0	1	When set to 1, indicates the left mouse button is being clicked.
1	1	When set to 1, indicates the right mouse button is being clicked.
2	1	When set to 1, indicates the middle mouse button is being clicked.
3	5	These bits are reserved for device-specific features.

Source: [17].

The HID attack on PATTERN requires a left mouse button to be pressed during each attempt. The direction and length of the line are determined by X and Y movements.

X movement is a 8-bit signed integer (0x00) that represents the X movement. When this value is negative, the mouse is being moved to the left. When this value is positive, the mouse is being moved to the right [17].

Y movement is a 8-bit signed integer (0x00) that represents the Y movement. When this value become negative, the mouse was moved up. When the value is positive, the mouse is being moved down [17].

In decimal notation, the convention is to precede the number with „+“ or „-“ to indicate whether it´s positive or negative, usually omitting the „+“ to simplify the notation for positive numbers. In binary this problem is solved by signed magnitude [22].

For instance, sending a mouse movement 300 pixels right and holding left mouse button at the same time requires proper formatted input below.
The report can be sent to /dev/hidg1 device using long version or short version of the report.

Long version of the report:
\0x01\0xFED4\0x00\0x00

Short version of the report:
\x01\0\xFED4\0\0

4 HID ATTACK IMPLEMETATION

Android-PIN-Bruteforce is an open source solution developed by Adam Horton. The solution uses a USB OTG cable to connect the locked phone to the Nethunter device. It emulates a keyboard, automatically tries PINs and waits after trying too many wrong guesses. The USB HID Gadget driver provides emulation of USB Human Interface Devices. This enables an Android Nethunter device to emulate keyboard input to the locked phone, like plugging a keyboard into the locked phone and pressing keys [4].

Fig. 3 Involvement of HID attack
Source: [4].

Required components: [4]

- A locked Android
- A Nethunter phone (or any rooted Android with HID kernel support)
- USB OTG (On the Go) cable/adapter (USB male Micro-B/C to female USB A), and a standard charging cable (USB male Micro-B/C to male A).

Advantages: [4]

- No need to enable USB debugging
- The locked phone does not need to be rooted
- Special hardware is not required
- Backoff time to crack other types of devices is configurable
- Detects when the phone is powered off (Low Power warning pop-ups)
- Detects when the phone is unplugged and waits while retrying every 5 seconds
- Optimised PIN list sorted by probability
- Log file

Disadvantages: [4]

- Only for Android
- Only for PINS
- No log of the correct guessed PIN

Android-PIN-Bruteforce was executed on 10 devices of different version of Android. In the measurement, only the executability on device was examined not total time of execution. The first point of measurement was whether Android-PIN-Bruteforce could repeat the attack with another PIN according to the configuration after an incorrect attempt on measured device. The second point measured whether the device was properly unlocked after sending the correct PIN. The table below shows that the Android-PIN-Bruteforce could not be launched only on devices with a version of Android lower than 5.0.

No.	Smartphone/tablet type	Android version	USB type	Executable
1	Smartphone Samsung galaxy S4 mini	4.4.2	USB B	NO
2	Tablet Lenovo Yoga 2-10 50F	5.0.1	USB B	YES
3	Tablet Huawei MediaPad T5	8.0.0	USB B	YES
4	Tablet Lenovo Touchpad 2016	8.1.0	USB B	YES
5	Smartphone Samsung galaxy J7	9	USB B	YES
6	Xiaomi Mi A2 Light	10	USB B	YES
7	Samsung galaxy A10	10	USB C	YES
8	Samsung galaxy S10x	11	USB C	YES
9	Samsung galaxy A71	11	USB C	YES
10	Samsung galaxy S10x	12	USB C	YES

Tab. 12 Measurements of HID attack.
Source: author.

5 CONCLUSION

This work presents an overview of time complexity of all types of Android lock screen protections.

PATTERN is vulnerable to HID attack due to its low computational complexity.

In this paper it has been presented that PIN and PASSWORD time complexity grow exponentially.

The HID attack is effective only for 4 and 5 digit PINs.

For PASSWORD it is beneficial to create a table of the most commonly used passwords, like in the dictionary attack.

The paper also describes creation of proper formatted inputs, which an attacker has to send to the locked device.

The attack is executable on the vast majority of devices with a higher version of the operating system of Android.

Further work might be focused on creating a cracking device and executable scripts, which can bypass not only PIN, but also PASSWORD and PATTERN protections

We can study:

- Using other methods of generating inputs. For example, using the Linux USB HID gadget driver.
- Testing them on different types of smartphones or tablets with different timeouts from different manufacturers.
- Determine that a HID attack has been performed on a device using forensic analysis.
- Design of a method to protect your phone from HID attacks.

References

[1] TAMMA, H., H. SKULKIN, H. MAHALIK and S. BOMMISETY. *Practical Mobile Forensics Fourth Edition.* Birmingham: Packt Publishing, 2020. s. 604. ISBN 978-1-83864-752-0.

[2] SYED MUQARRAB-UL-AHAD ZAIDI. *What are HID Attacks? How to perform HID Attacks using Kali NetHunter?* [online]. Pakistan: U.S. University of Agriculture, 2018. Available at: https://www.researchgate.net/publication/323111273_What_are_HID_Attacks_How_to_perform_HID_Attacks_using_Kali_NetHunter

[3] *Demystifying the Big O Notation.* [online]. [accesed 27. October 2021]. Available at: https://www.digitalonus.com/demystifying-the-big-o-notation/

[4] *Android PIN Bruteforce.* [online]. [cit. 30. August 2021]. Available at: https://github.com/urbanadventurer/Android-PIN-Bruteforce

[5] *Incorrect Passcode and the Android pattern lock.* [online]. [cit. 17. September 2021]. Available at: https://personal.support.lookout.com/hc/en-us/articles/202929734-Incorrect-Passcode-and-the-Android-pattern-lock

[6] SUN, Ch., Y. WANG and J. ZHENG. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. [online]. In *Journal of Information Security and Applications*, 2014, 19. 4-5: 308-320. Available at: https://doi.org/10.1016/j.jisa.2014.10.009

[7] Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX conference on Offensive technologies, WOOT'10. Berkeley, CA, USA: USENIX Association; 2010. Available at: https://dl.acm.org/doi/10.5555/1925004.1925009

[8] *Letters in the alpha bet.* [online]. [cit. 10. September 2021]. Available at:

https://www.worldometers.info/languages/how-many-letters-alphabet/

[9] LØGE, M. D. *Tell Me Who You Are and I Will Tell You Your Unlock Pattern*. [online]. U.S. Master's Thesis. Norwegian University of Science and Technology, Department of Computer and Information Science July, 2015. Available at: https://core.ac.uk/download/pdf/154670387.pdf

[10] *PIN analysis.* [online]. [cit. 30. September 2021]. Available at: https://datagenetics.com/blog/september32012/index.html

[11] MARKERT, P. et al. This pin can be easily guessed: Analyzing the security of smartphone unlock pins. In *2020 IEEE Symposium on Security and Privacy (SP).* IEEE, 2020. p. 286-303. Available at: https://doi.org/10.1109/SP40000.2020.00100

[12] *USB rubber ducky.* [online]. [cit. 17. December 2021]. Available at: http://www.sigint.sk/e-shop/758/5/radio-prijimace-vysielace/rubber-ducky-detail

[13] *Teensy® USB Development Board.* [online]. [cit. 17. December 2021]. Available at: https://www.pjrc.com/teensy/

[14] *Cellebrite.* [online]. [cit. 17. December 2021]. Available at: https://cellebrite.com/

[15] *XPin Clip.* [online]. [cit. 17. December 2021]. Available at: https://xpinclip.com/

[16] *Linux USB HID gadget driver.* [online]. [cit. 8. October 2021]. Available at: https://xpinclip.com/https://www.kernel.org/doc/html/latest/usb/gadget_hid.html>

[17] *USB Human Interface Devices.* [online]. [cit. 15. September 2021]. Available at: https://wiki.osdev.org/USB_Human_Interface_Devices

[18] USB IMPLEMENTS' FORUM. *Device Class Definition for Human Interface Devices (HID) Firmware Specification* - 6/27/01 Version 1.11, 1996-2001. 97 s.

[19] *HID Usage Tables for Universal Serial Bus version 1.22.* [online]. [cit. 5. September 2021]. Available at: https://www.usb.org/sites/default/files/hut1_22.pdf

[20] *Hacking Android Pattern Lock (ALP).* [online]. [cit. 12. November 2021]. Available at: https://www.hackcave.net/2015/08/hacking-android-pattern-lock.html

[21] *Cartesian coordinate system*. [online]. [cit. 16. November 2021]. Available at: https://en.wikipedia.org/wiki/Cartesian_coordinate_system

[22] *Two's complement*. [online]. [cit. 2. September 2021]. Available at: https://en.wikipedia.org/wiki/Two%27s_complement

Lt. Dipl. Eng. Sebastián **POTOCKÝ** (PhD. student)
Armed Forces Academy of General M. R. Štefánik
Department of Computer Science
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: sebastian.potocky@gmail.com

Prof. Dipl. Eng. Jozef **ŠTULRAJTER**, CSc.
Armed Forces Academy of General M. R. Štefánik
Department of Computer Science
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: jozef.stulrajter@aos.sk

Sebastián Potocký was born in Slovakia in 1994. He received his engineering degree from the Armed Forces Academy of General M. R. in the field of Military Communication and Information Systems. He is currently a web applications group commander - the base of stationary communication and information systems. His research is focuses on development of application, reverse engineering, cyber security.

Jozef Štulrajter works as a professor at the Department of Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. He graduated (Ing.) at the Military Technical College in 1974. He obtained the degree of CSc. diploma in Theoretical Electrical Engineering - Theory of Circuits and Systems of the Military Academy in Liptovský Mikuláš in 1992. His research interests include Information and Communication Technology (ICTs), computer architectures, image coding, computer security.

DOI: https://doi.org/10.52651/sam.a.2022.1.37-42

THE IMPACT OF TECHNOLOGICAL CHANGES ON THE DEVELOPMENT OF MILITARY LEADERS

Jan NOHEL, Zdeněk FLASAR, Milan PODHOREC, Bryan PAKULA

Abstract: The article focuses on possible directions of development of leadership in future military operations. It describes the principles of leading people and the functions of a leader-commander necessary for fulfilling tasks. However, as the rate of automation and robotization in leading military operations increases, the role of a leader-commander changes. Communication and information technologies allow directing military operations in a larger area with a higher degree of independence of the individual elements of the deployed forces as well as the decentralization of command and control. The increasingly more common use of autonomous systems brings a sizable challenge in the shape of commanding robots into the leadership process.

Keywords: Automation; Autonomy; Robotization; Commander; Leader; Leadership.

1 INTRODUCTION

Leading people is currently a process in which an individual decides the direction a group of people should go and by what procedure (method) will it achieve its goal. Leader is someone people follow and want to follow without needing to be forced to do so, or even being subjected to negative conditions and threats as criteria for advancing towards the completion of the task. Leader is a man with a vision, who chooses the direction and knows the way He is the one always in front, so he can lead others, and helps those, who wander or are out of breath, find the way. He is the example worthy of being followed. [1, p.25] The task of leader is leading men and caring for their needs. A man has to grow into the position of a leader, build it within himself. Leadership can be employed everywhere, where there are people who depend on the leader and want to follow him. [1, p.26-27]

Every leader-commander of a military unit has to be an example to his subordinates, help them and show them the way while fulfilling tasks and achieving goals. Only then can he fulfil other requirements stemming from his function as a leader:

- work out and comprehensibly formulate his idea of the goal, manner of focusing and ways of conducting preparations;
- require his subordinates to understand and fulfil tasks;
- ensure the preparation of his subordinates across the whole organizational structure, require, support and direct the development of his subordinates' abilities;
- motivate towards reaching the best results possible;
- play a large part in the preparation process;
- insist on fulfilling the requirements and standards of preparation;
- encourage environment conducive to preparation.

Of great importance is the specialization of the leader-commander as well as his experience with commanding the specific unit. [1, p.129-131]

The article describes the current ways of leading people, the role of the leader-commander and the way to achieve this, in contrast with the increasing level of automation of the command and control of military units. The increasingly frequent integration of autonomous robotic systems into the composition of units and the use of automated command and control information systems will also have an impact on the functions of the leader-commander. The main goal of the article is to identify the differences between the current leadership and the possible leadership of communication-connected soldiers, units and autonomous robotic systems, using automated tools for decision support in the near future. The article describes the current ways of leading people, the role of the leader-commander and the way to achieve this, in contrast with the increasing level of automation of the command and control of military units. The increasingly frequent integration of autonomous robotic systems into the composition of units and the use of automated command and control information systems will also have an impact on the functions of the leader-commander. The main goal of the article is to identify the differences between the leadership of people today and the possible leadership of communication-connected soldiers, units and autonomous robotic systems, using automated tools for decision support in the near future.

During the writing of the article, the documents and text analysis methods were used to obtain the knowledge base of leadership, as well as the participation observation method in the practical implementation of the process of command and control of military units. Based on the information and knowledge obtained in this way, together with the use of experiments in modelling the axis of maneuver of robotic systems and military units, the induction method was applied to describe the possible implementation of military leadership in the near future.

2 FUNCTIONS OF THE LEADER-COMMANDER

According to [1, p.101], the functions of leader-commander can be divided into planning, organising, leading, supervising and delegating.

Planning is a decision-making process of selecting goals and the means of their fulfilment. It is the basis for all the other functions. It includes setting goals and selecting the ways they are to be fulfilled. Any thought out, conscious sequence of future actions is a plan. A military commander can achieve the goals through a decision-making process, which can either take the mental form of an OODA loop, see [2], or a procedural form dependent on the size of the unit in the shape of TLP (Troops Leading Procedures) and MDMP (Military Decision-Making Process), see [3].

Organising is the effective deployment and arrangement of all available resources in a way that allows for achieving the set goals in time through the planned means. It includes the creation of organisational structure which will allow effective cooperation of the work team or unit towards achieving set goals. [1, s.103]

Leading is a conscious process of influencing colleagues and effective use of their skills and abilities, motivating and leading them towards high-quality and active creative fulfilment of tasks which will help reach set goals [4]. The behaviour of the leader and his style of commanding then tends to be percieved as the way in which he acts towards the group of his colleagues. Classic leadership theory or leadership according to the type of behaviour differentiates between three main styles: authoritative, democratic, and liberal. [5]

Supervising is an objective evaluation of the carried out work from the point of view of fulfilment of the set goals. Its point is the identification and removal of imperfections in work processes, in order for the set goals to be achieved as efficiently as possible.

Delegating is the transfer of work duties and responsibilities to colleagues.

3 AUTOMATION OF COMMAND AND DIRECTION

Currently a number of communicationally interconnected information systems for assisting in decision-making and the sensors with GPS support integrated within them are entering the process of commanding and controlling units. In the case of infantry, it is the set of the future soldier, see [6], which will, alongside vehicle platforms, give the commanders information about the current deployment of the unit. It allows sharing of the information acquired by the set, sending text messages and data layers, while also monitoring the physical state of the soldier and technical state of the vehicle including the current ammunition supply. The set of the future soldier (depicted in Fig. 1) in the combination with the information systems gives the commander an overview of the situation on the battlefield, allows him to control his whole unit in coordinated manner over a larger operational area and deploy soldiers effectively where they are needed. The commander's station can be within his unit, inside of a commanding vehicle or helicopter or at the base.

The information within the network of communicationally interconnected stations is shared across the board among all users or based on authorised access, which allows natural coordination of all of the unit's members' activities.

Fig. 1 The future soldier
Source: [7].

There is a trend towards an increasing degree of automation and robotization in the development of modern combat units, see [8-10]. Automatic robotic weapons systems, such as the one shown in Fig. 2, use variety of sensors and have already surpassed humans in, for example the speed of identifying enemy objects and destruction of set targets through fire. Control of their actions can be semi-automatic with only an occasional assistance from the robot group operator, or autonomous with the use of AI algorithms.

Fig. 2 THeMIS Unmanned combat vehicle
Source: [12].

Autonomous robotic systems can then simply receive a task. The task may be to SEEK and DESTROY, GUARD, or OBSERVE with the specification of operational area. Accurate identification of objects of interest can be achieved via ATR (Automatic Target Recognition) system, LIDAR (Light Detection And Ranging) and a database of pre-defined enemy soldiers and military vehicles, see [11].

Mathematical algorithmic models using tactical-geographic data and information can be used to advance automation and autonomy and fulfil tasks in future military operations. One of such models is TDSS (Tactical Decision Support System), which has been in development at the University of Defence of the Armed Forces of the Czech Republic, see [13]. TDSS consists of several mathematical algorithmic models, such as optimization of observation station model, aerial recognisance planning model, ground units manoeuvre control model (MCS CZ Maneuver Control System CZ) and others, see [14-18]. The manoeuvre axes for individual aerial or ground systems up to a swarm of such systems can be calculated in these models based on the impact of the updated situation on the battlefield, see Fig. 3.

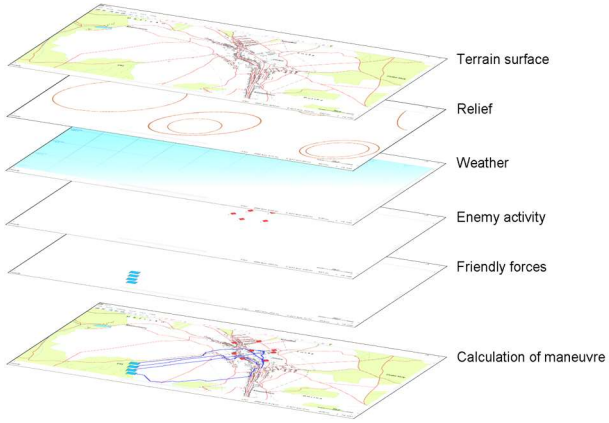


Fig. 3 Layers of MCS CZ
Source: author.

MCS CZ can be used to calculate spatially coordinated axes of ground manoeuvres, which can be used during operations of units of the future soldiers as well as for deployments of swarms of robotic systems [19].

4 FUTURE LEADERSHIP

With the expected development of automation and autonomy of command and control in future military operations, leadership as a process of leading and directing subordinates' efforts will see the disappearance of the people-subordinates. From the point of view of leadership development, we can then speak mainly about the development of "Self-leadership", see [20,21], - knowing one's strengths and weaknesses, motivation, one's own decision-making, goal selection, stress management, rejecting pessimism etc. Inefficient behaviour can be eliminated via a number of strategies, such as self-observation, self-evaluation and self-perception, which encourage leader to achieve higher efficiency. [22,23] The question of cognitive management in contrast with the technological development and NNEC (NATO Network Enabled Capability) conception is further explored in [24].

The basic functions of leader-commander are then also significantly modified. Planning of activity-manoeuvre of subordinates in order to achieve goals remains. But for the sake of speed and higher accuracy it will most likely transform from a personal mental process of the commander into a qualified approval of a variant of the manoeuvre calculated by the information system. Qualified approval, however, requires knowledge of functioning principles and computational functions of information systems as well as advanced experience with carrying out the computed manoeuvres in practice, which will allow the leader-commander to estimate the situation of his units before during and after the manoeuvre. [25]

In the case of remote coordination of units in a larger operational area, organizing will be mainly limited to preparation and supplying with necessary material before the start of the operation.

The leading function will most likely be limited exclusively to the remote authoritative style with the commander giving out the tasks necessary for achieving the required final state based on up-to-date situation on the battlefield, current state of the unit and the required final state. Just like the planning and organising functions, remote leading of subordinate commanders or robotic systems will place significant demands of continuous personal development of the leader-commander in the use of modern technologies, information systems and tactics of leading combat in a way that achieves goals in a military operation. [26]

All authorized unit members will be able to continuously control the implementation of the planned activities in the collective awareness of the battlefield situation environment using the communicationally interconnected information systems, see Fig. 4.

Fig. 4 Future commanders
Source: [27].

Delegating authorities and duties to subordinates using online control will be significantly easier and in the case of decentralized command of operations over a larger area also more suitable.

In the case of autonomous operation of robotic combat units, we can speak of "robotic leadership," which will mostly emphasise the planning of targets and final state in the military operation and subsequent control of its realisation.

5 CONCLUSION

Military operations in the 21st century will be characterised by increasing degree of automation of command and control of units as well as of autonomy of robotic systems. This trend will change what is required of commanders. Despite the remote command and control, this will still have to include those of technological-practical character. Up-to-date awareness of the situation on the battlefield will be provided via communicationally connected information systems for decision-making assistance, the functionality of which also allow for calculating manoeuvres of subordinate units. This will require advanced knowledge of functioning and controlling of these information systems and qualified estimation of the development of the battlefield situation based on practical experience. That is the only way to utilize the advantages of quickly and effectively calculated manoeuvres, which may give us the operational superiority on the battlefield.

A significant part of this "technological leadership" can or even has to be its moral aspect. While controlling "robots" (semi-automatic, automatic), the human-commander of the operation in question has to be aware of the fact that somewhere outside of his present station a "robot" is carrying out activities that may have consequences possibly even fatal ones for a human-enemy.

The comparison of the leadership of people, military units and robotic systems described in the article and their possible realization in the future indicates the direction of development of the functions of future leaders-commanders. In military practice, it will be used by units that will apply the NNEC concept, with a predominant degree of automation of command and control of autonomous robotic systems.

References

[1] KOČVARA, P. *Vedení lidí v armádě.* 1. vydání. Vyškov: Vojenská akademie, 2015. 273 s.

[2] The OODA Loop: How Fighter Pilots Make Fast and Accurate Decisions. Farnam Street [online]. Ottawa, Canada, 2022 [cit. 2022-01-07]. Available at: https://fs.blog/ooda-loop/

[3] FM 5-0 THE OPERATIONS PROCESS. Washington: Headquarters department of the army, 2010, p. B-1 - C-10, distribution number: 110412.

[4] VODÁČEK, L. a O. VODÁČKOVÁ. *Moderní management v teorii a praxi.* Prague: Management Press, 2006. 118. ISBN 80-7261-143-7.

[5] BĚLOHLÁVEK, F., P. KOŠŤAN a O. ŠULEŘ. *Management 1.* Olomouc: Rubico, 2001. 151. ISBN 80-85839-45-8.

[6] READING, Dale F. and J. EATON. Biotechnology & Human Enhancement. In *Science & Technology Trends 2020-2040: Exploring the S&T Edge.* 1. Brussels, Belgium: NATO Science & Technology Organization, 2020, 94-103.

[7] U.S. ARMY / DARPA. The future soldier will be part human, part machine [online]. 2014 [cit. 2022-01-24]. Available at: http://2045.com/news/32846.html

[8] NOHEL, J., M. PAVLAČKA a P. STODOLA. Budoucí taktické bezpilotní vzdušné systémy Armády České republiky. In *Vojenské rozhledy* 2022, 31(1), 51-70. ISSN 1210-3292. Available at: https://doi.org/10.3849/2336-2995.31.2022.01.051-070

[9] *Top 10 military robots and unmanned ground vehicles in the world.* RoboticsBiz [online]. [cit. 2020-03-19] Available at: https://roboticsbiz.com/top-10-military-robots-and-unmanned-ground-vehicles-in-the-world/

[10] Top 10 best military robots in the world, Auto journalism, Jim Carrey, [online]. 7.6.2021, https://autojournalism.com/top-10-best-military-robots-in-the-world/

[11] SCHACHTER, Bruce J. *Automatic Target Recognition (3).* pp. 330. Bellingham USA: SPIE Press, 2018. ISBN 9781510618572. Available at: https://doi.org/10.1117/3.2315926

[12] THeMIS Combat with PROTECTOR RWS: Combat. MILREM Robotics [online]. Tallinn, Estonia, 2022 [cit. 2022-01-24]. Available at: https://milremrobotics.com/product/themis-with-protector-rws/

[13] STODOLA, P. and J. MAZAL. Tactical decision support system to aid commanders in their decisionmaking. In: Hodicky, J. (ed.) *MESAS 2016.* LNCS, vol. 9991, pp. 396–406. Springer, Cham (2016). ISBN 978-3-319-47605-6. Available at: https://doi.org/10.1007/978-3-319-47605-6_32

[14] NOHEL, J. Possibilities of Raster Mathematical Algorithmic Models Utilizations an Information Support of Military Decision Making Process. In: Mazal, J. (ed.) *MESAS 2018.* LNCS, vol. 11472, pp. 553-565. Springer, Cham (2019). ISSN 0302-9743. ISBN 978-3-030-14984-0. Available at: https://doi.org/10.1007/978-3-030-14984-0_41

[15] NOHEL, J., P. STODOLA, and Z. FLASAR. *Model of the Optimal Maneuver Route.* [Online First], IntechOpen, pp. 79-100. London (2019). Available at: https://doi.org/10.5772/intechopen.85566

[16] NOHEL, J. and Z. FLASAR. Maneuver control system CZ. In: Mazal J., Fagiolini A., Vasik P. *Modeling and Simulation for Autonomous Systems. MESAS 2019.* Lecture Notes in Computer Science, vol 11995. Switzerland, Cham: Springer. (2020). pp. 379-388. ISBN 978-3-030-43889-0. Available at: https://doi.org/10.1007/978-3-030-43890-6_31

[17] NOHEL, J., Z. FLASAR and P. STODOLA. Combat UGV Support of Company Task Force Operations. In: Mazal J., Fagiolini A., Vasik P. *Modeling and Simulation for Autonomous Systems. MESAS 2020.* Lecture Notes in Computer Science, vol 12619. Switzerland, Cham: Springer. (2021). pp. 29-42. ISBN 978-3-030-70739-2. Available at: https://doi.org/10.1007/978-3-030-70740-8_3

[18] NOHEL, J., P. ZAHRADNICEK, Z. FLASAR Z. and STODOLA, P. *Modelling the Manoeuvres of Ground Reconnaissance Elements in Urban Areas.* 2021 Communication and Information Technologies (KIT), 2021, pp. 1-6. Available at: https://doi.org/10.1109/KIT52904.2021.9583749

[19] NOHEL, J., STODOLA, P. and FLASAR, Z. Swarm Maneuver of Combat UGVs on the future Digital Battlefield. In: *MESAS 2022* proceedings. Unpublished.

[20] STEWART, G., S. COURTRIGHT and Ch. MANZ. Self-Leadership: A Multilevel Review. In *Journal of Management,* 2011. 37. pp. 185-222. Available at: https://doi.org/10.1177/0149206310383911

[21] DAUD, Y. M. Self-leadership and its application to today's leader - A review of literature. T*he Strategic Journal of Business & Change Management, 2020,* 8 (1), pp. 1 – 11. ISSN 2312-9492.

[22] MANSHI and SUNIL, K. Mishra. Self-Leadership as a Tool for Enhancing Performance at Workplace. In *International Journal of Geographical Information Science 14,* 2019. pp. 76-88. Available at: https://doi.org/10.26643/gis.v14i6.11628

[23] SHEK, Daniel T. L., Cecilia M. S. MA, T. T. LIU and Andrew M. H. SIU. The Role of Self-Leadership in Service Leadership. In: *International Journal on Disability and Human Development*, v. 14, no. 4, (2015), pp. 343-350. Available at: https://doi.org/10.1515/ijdhd-2015-0455

[24] AMBROŽOVÁ, E., J. KOLEŇÁK, D. ULLRICH a V. POKORNÝ. *Kognitivní management*. Brno: Key Publishing, 2016, p. 190. ISBN 978-80-7418-254-9.

[25] KILIÇ, Y. and M. ÇELMELI. Adapting Military Leadership. In *Changing Warfare Environment, Journal of Military and Information Science.* Vol 2(4), pp. 88-95. Available at: https://doi.org/10.17858/jmisci.49006

[26] AMIR, S. Outline of Future Military Leadership Characteristics: An Analysis (2018). In *Electronic Research Journal of Behavioural Sciences*, Volume 1 (2018). pp. 5-16. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3611228

[27] *Future Force Company Commander Screenshots.* Moby Games [online]. 2012 [cit. 2022-01-24]. Available at: https://www.mobygames.com/game/windows/future-force-company-commander/screenshots/gameShotId,592587/

Capt. Dipl. Eng. Jan **NOHEL**, Ph.D.
Department of Intelligence support
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: jan.nohel@unob.cz

Assoc. Prof. Dipl. Eng. Zdeněk **FLASAR**, CSc.
Department of Tactics
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: zdenek.flasar@unob.cz

Dipl. Eng. Milan **PODHOREC**, Ph.D.
Department of Tactics
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: milan.podhorec@unob.cz

SFC. Bryan **PAKULA**
School regiment
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: bryan.pakula@unob.cz

Jan Nohel is active as lecturer at Department of Intelligence support at the University of Defense in Brno in Czech Republic. He holds Ph.D. in Military management (2015). His research interests include the information support of the decision-making process of commanders at the tactical command and control level, tactical and terrain analyses and cross-country movement modelling. He is focused on the issue of mathematical algorithms design for data processing and fusion and their integration in C4ISR systems. Before starting his research career, he accumulated military experience from being a commander and staff officer of Czech Republic army units.

Zdeněk Flasar is an Associate Professor at University of Defense in Brno, Czech Republic, where he works as a senior researcher of the Department of Tactics. He served as battalion commander and started his research career in 1985. His scientific and professional also educational work is connected with tactics of military units, Command and control process and methodology of military training. He participates on national military exercises, research and cooperation projects.

Milan Podhorec works as a senior researcher of the Department of Tactics of the University of Defense in Brno. He served as a deputy of reconnaissance battalion commander. He has been working as chief of the Military Intelligence and Electronic Warfare Group of the Military Management and Tactics Department since 2003. His scientific and professional also educational work is connected with intelligence and reconnaissance in combat and non-combat operations, security situation and its impact on the army and current issues of tactics and military management development.

Bryan Pakula is a 5th year student of the Control and use of armed forces masters' programme with the Commander of reconnaissance units specialization at the University of Defence, Brno. His fields of interest include modern military technology, technological means of reconnaissance and information support of command and control.

DOI: https://doi.org/10.52651/sam.a.2022.1.43-48

METHODS FOR DETERMINING THE RISK FACTORS FOR ROAD TRANSIT IN HUNGARY

Péter BODA[1], Tibor KOVÁCS[2]

Abstract: Road transport is affected by number of hazards in Hungary also. Timely exploration of these risk factors can help to reduce the severity of unexpected consequences. In this article we present and evaluate some of the procedures that can help in this work. The solutions we have now chosen are the mathematical methods, the questionnaire survey and the modeling.

Keywords: Road transit; Risk factor; Hazard source; Traffic system; Mathematical methods; Questionnaire survey; Modeling.

1 INTRODUCTION

The global terrestrial system is very complex because it includes the living and inanimate (natural and built) environment as well as human society (see figure 1). A part of this global environment is the transport/traffic system, which also reacts to changes as a result of events (predictable or unexpected) due to other changes in the global system. The impacts that trigger changes are, in the vast majority of cases, external impacts and how a given system responds to these impacts (affecting the way the system works) is called the sensitivity of a system. The disruptive impacts on transport/traffic systems are basically divided into three major groups, such as:

a) intentional or harmful acts,
b) natural hazards (natural disasters),
c) human-triggered and technological hazards.

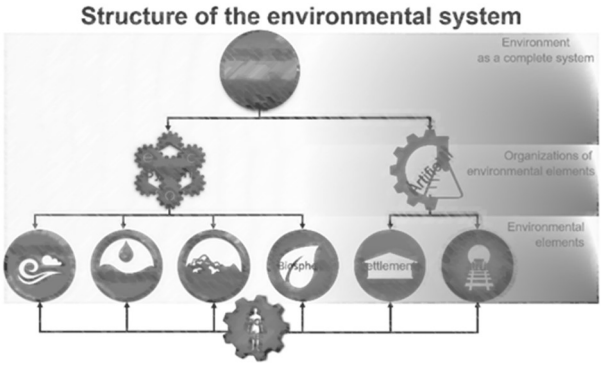


Fig. 1 Major groups of environmental systems
Source: edited by the authors, based on Kerényi. [1]

The factors influencing the sensitivity of transport/traffic (transit of goods) systems can be very diverse.

The territorial segregation of human activities has created a need for relocating and forwarding products, and this need is also the basis for traffic analysis and forecasting. Their analyses and forecasts also include the determination of the sensitivity of transport/traffic systems, the methods of reducing their damage, and the possibilities of increasing their resilience, one version of which is illustrated in this article.

The concept and content of safety/security are constantly changing today due to the development of civilization. Because of this change, we can now distinguish several dimensions of safety/security. [2]

All of the risk factors (such as disruptive or threatening factors) affect the safety of the economy, and thus indirectly the safety of traffic and transportation. In the following we examine, how we can predict the risk factors in order to prevent and reduce the effects of them.

2 CONDITIONS ENDANGERING ROAD TRANSIT (OF GOODS) IN HUNGARY, POSSIBLE METHODS FOR THEIR DETERMINATION

Proper assessment of environmental risks and disruptive impacts and the management of their impacts was performed using three methods, comparing the results obtained. The methods we have chosen and used are as follows:

- determination of the factors influencing the safety of road transit using mathematical methods,
- determination of influencing factors by means of a questionnaire survey,
- modelling.

a) Determination of factors in the road transit (of goods) system influencing its safety using mathematical methods

When examining the determination of the factors by mathematical methods, we started from the fact that we have to perform a risk assessment to prove their determinability. In the calculations, we must therefore accept that a certain risk can be assigned to each hazard, depending on the probability of the event occurring and the severity of the consequences of an

[1] ORCID: 0000-0003-1528-8935.
[2] ORCID: 0000-0001-5987-8289.

event. A risk is a combination of the frequency or probability of the occurrence of a particular hazard event (F) and the severity of the consequence (C):

$$R = C \times F \quad (1)$$

In the case of a complex system consisting of independent elements (see transport/traffic system), the total risk can be defined as the sum of the risks associated with each independent hazard:

$$R = \sum ni = 1Ci \times Fi \quad (2)$$

In the calculations, we have to accept that we cannot always fully determine the risk of an emergency. Identified risk is a ratio that indicates whether the risk of our activity is acceptable to us, taking into account the indicators we have defined or set by standards. Of course, determining the degree of risk is not an end in itself, as it allows us to determine the degree of safety of a given activity (resilience, risk-free status - S).

$$S = 1/R \quad (3)$$

However, in order to identify the risks associated with road traffic, such as road transit, for a given event or process, we also need to distinguish between two basic concepts, such as risk and uncertainty. [3] According to Homolya, "*A precarious situation is a broader category. We speak of uncertainty when the outcome of future developments is unknown and we cannot say with certainty what the outcome will happen."* [3;10] The uncertainty factor can be determined by the following formula:

$$(\%) = \frac{100 \cdot \mu_{\alpha.} \cdot STDVE}{\overline{X}} \quad (4)$$

$\overline{X}$ is the expected value of a given parameter; STDEV is the standard deviation of a given parameter (standard error). [4] It can be seen that uncertainty can also be determined by a certain degree of standard deviation, which is calculated by the relation

$$P(-\mu_{1-\alpha} < X < \mu_{1-\alpha}) = \boldsymbol{\alpha}. \quad (5)$$

Since we have only been able to identify the uncertainties (and their standard deviations) in the calculations outlined so far, we have found that a simpler and thus faster procedure is needed to determine the risks in the road transit system. We started this work using the *"total probability theorem": "In probability calculation total event system (TES) is the name of a maximally countable system of events (B1, B2, ...) for which the following are satisfied:*

$$P\Sigma B_{ii}) = 1 \quad (6)$$

$$P\left(B_i B_j\right) = 0\ (\forall_i\ to\ j\ i \int\ i \neq j \quad (7)$$

$$P(B_i) > 0\ (\forall\ to\ i) \quad (8)$$

That is, if Bi-positive-probability events essentially (i.e., apart from a zero-probability event) cover the entire event space, then any two events are substantially disjoint.

If A and B are two events and P(B)> 0, then we define the conditional probability of A for B by the formula P(A | B) = P(AB)P(B), which means that if we already know that event B has occurred, what the probability of event A is.

That is, if Bi-positive-probability events essentially (i.e., apart from a zero-probability event) cover the entire event space, then any two events are substantially disjoint.

If A and B are two events and P(B)> 0, then we define the conditional probability of A for B by the formula P(A | B) = P(AB)P(B), which means that if we already know that event B has occurred, what the probability of event A is.

If now A is an arbitrary event, B1, B2, ... is a TES, then the probability of A can be calculated in the following form:

$$P(A) = \Sigma P(A \setminus iBi)\ P(Bi).\text{" [4;11]} \quad (9)$$

In our study, we found that the total probability theorem is not suitable for determining the extent of road traffic risks because it is a concept that can be defined within zero-order logic, i.e., a logic formula describing a logical operation where the probability of an event is calculated based on another event. Therefore, in areas where risk management methods are used, the continuous form of the Bayes theorem, which can be described by the following formula, is preferred: [3;11]

$$f(y|x) = \frac{f(x|y) \cdot fY(y)}{\int_{-\infty}^{\infty} f(x|y) \cdot fY(y)\ dy} \quad (9)$$

In the study of the Bayes theorem[3;13-21], we found that it is not suitable for identifying the risks affecting the safety of road transit, as the possible scope of this method is to identify the infrastructural factors influencing an accident, mainly by road infrastructural methods and can be influenced by means, i.e., it gives a static technical approach.

József Gyarmati [5] examined the general and specially used concepts of risk and risk management. The aim of his study was to select procedures that may be suitable for determining the risk of critical infrastructure in a Hungarian environment. In his article, he states that *"The study analyzes in terms of critical infrastructure protection, which is fundamentally technical in nature. However, an examination of the other approaches reveals the possible limitations of the fundamentally technical approaches listed so far. The article therefore summarizes the other principles as well as the criticisms of the technical approach."* [5;79]

The above has shown that the risks affecting the safety of road transit and their responses, due to the complexity of their numbers and impacts, cannot be determined by mathematical methods alone. These calculations can only be used to measure the probability of occurrence of the risks posed by each hazard, regardless of their occurrence in real time. Therefore, we have to search a more objective, easier-to-use method should be developed for app the basis of this method is the adaptation of the convolution of the frequency distribution and the severity distribution, as well as the application of the operational risk management, such as "decision tree". [3;11-13]

b) Processing the relevant parts of a questionnaire survey1, drawing conclusions in order to identify the factors influencing the safety of domestic road transport

The aim of the questionnaire survey was to assess the willingness of the target group (mainly carriers, those working in the transport sector) to respond, in addition to learning about some issues related to road safety. The questionnaire survey provided the following results.[2]

The vast majority of respondents (42 %) consider Hungarian public roads to be moderately safe, while the proportion of those who consider road safety to be poor or very poor is close to the same (40 %). 17 % of the respondents consider the situation to be good, while only 1 % of the respondents gave a very good rating.

It was positive in the survey that the respondents placed the safety of Hungarian road transport in the middle compared to European (not only EU) countries. The result is very significant, as the average rating is 44 %, while the remaining 56 % is divided almost equally between worse and better reviews.

The vast majority of respondents consider the condition of Hungarian roads to be unacceptable (very bad 28 %, bad 39 %, medium 28 %), so, it is clear (without any further survey) that our roads need to be reconstructed (not pitted), repaired and our road network (including European corridors) need to be developed.

Regarding the driving safety of Hungarian drivers[3], it can be stated that ¾ (77 %) of the respondents do not consider Hungarian drivers to be more dangerous than foreigners and only 23 % feel that we Hungarians drive dangerously.

Regarding the question on the training and further training of drivers working in goods transport, 81% of the respondents consider the training of professional drivers to be important or very important, and 17 % moderately important, the relevance of which is unquestionable.

The next question examined the overall relationship between transport safety and environmental safety (occupational safety). The answers clearly prove (92 %) that the external influences on drivers affect more or less (rather more) the safety of driving, such as traffic safety and the safety of goods transit. Accepting[4] the survey data requires the following steps[5]:

- identify, through further assessment, which confounding factors in this area (personnel, organizational, infrastructural, their combination) have the most negative impacts on drivers,
- develop an action plan after assessing and prioritizing confounding factors,
- in parallel with the international acceptance of the plan, its implementation in Hungary,
- processing, publishing and fine-tuning the results of the implementation,
- promoting international acceptance by disseminating experience.

The provisions of the EU's mobility package clearly increase the costs for law-abiding carriers, so, that its requirements (without proper control) will give third-country companies a competitive advantage and may adversely affect the operation of intra-EU carriers. The vast majority of respondents (80 %) consider that the unauthorized activity of foreign carriers (belonging to the black or gray zone) is not only an economic problem, but also a road safety problem. [6] Based on the answers to the question, the action to be taken is not in question: more efficient control (technical, organizational), strict sanctions.

By processing the relevant parts of the questionnaire survey and summarizing the findings, we concluded that it ensures data that provide results not suitable for real-time identification of hazards, but this method should be used to refine the results provided by other methods[6].

[1] Based on a questionnaire survey carried out by Péter Boda.

[2] The detailed evaluation of the questionnaire and the detailed presentation of the conclusions drawn from it are the subject of a future study.

[3] During the processing of the questionnaire, we were confronted with the fact that this question was incorrectly worded, as it should have applied to professional drivers working in the transportation of goods. Due to the incorrect wording of the question, no conclusions have been drawn in this regard, the data are only informative.

[4] The relevance of the data is ensured by the fact that 60 % of the respondents (14 % are drivers out of 100) work in some position in the field of road goods transport.

[5] Without details.

[6] In this article not all issues and otcomes are presented that related our topic.

c) *Identification of factors influencing the safety of road transport of goods in Hungary, drawing conclusions by modeling*

In order to make it easier for us to understand the world around us or to get information about its possible changes, in many cases we make a model of things . These models allow us to understand what is happening (has happened or will happen) and why it is happening.

The evaluation of the result of modeling is done by some comparison, which is based on the principle that one model does not exist. A model can always only be interpreted together with an event modeled by it and must satisfy the conditions of similarity between the two. This means that the evaluation is performed in a relation of at least two objects.

Taking into account the previous findings - in one version - we prepared a model for the identification of the factors influencing the safety of road transport in Hungary and for drawing conclusions.

The following options, methods and procedures were considered and selected during the development.

The function of a model is descriptive:

- its structure is analogous,
- its system of criteria is formal,
- its nature is qualitative, including mental,
- it is static based on the examined processes,
- its elaboration is manual,
- its type is: Forrester-Meadows model. [8]

In developing the model, we examine the interaction of six sectors (sub-processes). They are:

- traffic routes,
- traffic technology,
- traffic environment,
- traffic management,
- others (legal environment, resource allocation, emergency response, quality of service, transport IT, sustainability,
- vehicles.

Relationships of each sub-process within the six sectors:

- intentional or harmful acts,
- natural hazards,
- human-triggered and technological hazards.

Since we did not have a computer program to perform the comparison, we performed the modeling manually. Therefore, as opposed to the original Forrester-Meadows model, we did not get run-down curves, but a relationship diagram showing possible responses to an event (confounding factor).

In addition to the theoretical modeling - in another experiment - we also modeled a given (recorded) situation, which was implemented using the *"Graph Model"*. [8] (The presentation of the experiment will be the subject of another study, but the results were used to draw the conclusions of this article.)

During the examination of the identification of the factors influencing the safety of road goods transport in Hungary by modeling, we came to the conclusion that before making transport safety decisions - similarly to the previous two test methods - the possibilities of modeling should be used in order to achieve the most effective results.

3 USE OF RESOURCE AVAILABLE FOR PROTECTION

The resources available for protection are also scarce in relation to the physical extent of the critical infrastructure systems, so, their use needs to be optimized. This is also true for road transit, where increasing the efficiency of the factors assigned to the task of strengthening transport safety also plays a role in increasing it. One way to do this is to apply network theory, which is of great importance in system organization. Among the theses of this interdiscipline is that the stability of networks depends on so-called robustness. The more complex a system is, the more interchangeable elements it contains, that is, the more robust it is, the less vulnerable it is to adapt network theory procedures when sharing security elements. The highlighted nodes that carry the properties of the graphs (see Figure 2) determine the stability of the system. Their failure (to a certain extent) leads to the collapse of the given system (system component). In this way, the level of protection can be enhanced with increased resources by increasing the security/safety of said central components. That is, when applying risk management techniques, protection resources should be focused primarily on the segments that are most at risk. Based on the above, it can be stated that the criticality of a particular infrastructure, and thus the magnitude of the damage caused by hazards, can be reduced by organizing it into a complex network or raising its dependence on resources from a local, regional level to a global level.

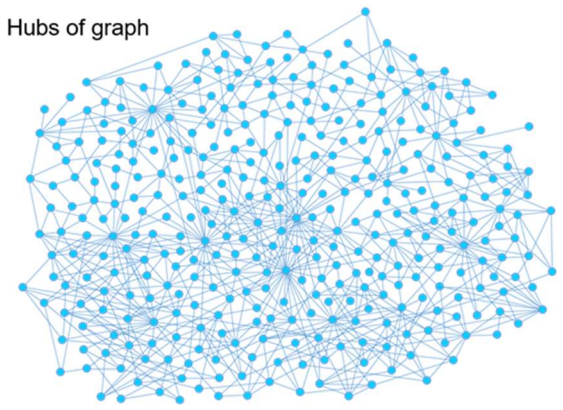


Fig. 2 Large graph with hubs
Source: https://images2.pianshen.com [9].

We can conclude that higher dimensional factors, such as global systems, represent a qualitatively higher level due to their own internal resources and

thus allow access to more resources than those available to users of local capacities.

Based on the above, we can record as the most important tasks of the protection of critical infrastructure, including road transit:

- assessing according to the central requirements and principles (identification of hazards and disturbances) and continuous maintenance of its results,
- planning and monitoring based on uniform criteria,
- preparing the relevant bodies and freight carriers for contingencies, incident management and participation,
- maintaining on-call and monitoring systems, provision of mutual information,
- organizing and maintaining on-call units that can be deployed immediately, providing them with equipment,
- increasing system security/safety (duplication of connection, possibly duplication, etc.).

4 CONCLUSION

The three methods examined in this article are not comparable according to the axioms of the research methodology, as the questionnaire surveys belong to the category of qualitative research, the mathematical methods belong to quantitative research (while modeling, depending on its type) and are used for different purposes to provide results. Nevertheless, in our opinion, the methods are comparable, and the point of connection (apart from the research methodology) is usability.

In terms of usability, the following conclusions can be drawn for the methods studied:

- none of the three examined methods is suitable for real-time forecasting of intentional or harmful acts (hereinafter A), natural hazards (hereinafter B) and human-triggered, technological hazards (hereinafter C),
- the mathematical methods for the three groups (A, B, C) can only be partially used for vehicles (e.g., applicability) and for the so-called forecasts for "others" (legal environment, resource allocation, quality of service, transport IT, etc.),
- questionnaire surveys cannot be used for vehicle forecasts either (for either group), as they require special knowledge and expertise;
- none of the methods can be used to identify all hazard sources (A to C, or even a group of hazards, e.g., 'A') in real time,
- although the questionnaire survey is basically suitable for a combined examination of the emerging hazard sources, it only works for the long-term forecasts and the decision-making process.

In overall, based on our research in our present study, we concluded that a distinction should be made between the definition of hazards and risks in order to adequately define the influencing factors. During the study of the calculation (forecast) of hazards and risks, we have demonstrated that each hazard can be assigned a certain risk, which depends on the probability of the occurrence of the event and the severity of its consequences.

By examining the mathematical method of determining the risk factors influencing the safety of road transit (goods transport), we proved that the risks affecting the safety of road transit and the answers to them cannot be determined only by mathematical methods.

By conducting a questionnaire survey, we proved that the Hungarian society is interested in the issues concerning traffic safety and forms an opinion on them. Based on this, we have established that questionnaire surveys are important in assessing the possibilities of improving and enhancing the situation of traffic safety, but they are not suitable for determining specific, real-time hazard sources.

During the examination of the identification of the factors influencing the safety of road transport in Hungary by modeling, we concluded that modeling is of paramount importance in assessing the situation and improving the possibilities of traffic safety. We also proved that the advantage over mathematical and questionnaire methods is that, if applied correctly, it also shows the possible answers to an occurring event (confounding factor).

In overall, we have concluded that the examined methods should be used together (in combination) before making a given decision on traffic safety. We also found that the investigated methods only have a limited ability to identify the hazard sources (not at all in real time), so, it is expedient to use them in order to determine the possible responses (especially prevention).

References

[1] KERÉNYI, A., T. KISS and G. SZABÓ. *Environmental Systems.* [online]. University of Debrecen, University of Szeged, 2013. [cit. 2021-11-24]. Available at: https://eta.bibl.u-szeged.hu/id/eprint/1315.

[2] ÜRMÖSI, K. *The concept of security.* Military Science Review, Budapest, 2013. Vol. 6, No. 4, p. 149. [cit. 2021-11-24]. Available at: https://epa.oszk.hu/02400/02463.

[3] HOMOLYA, D. Environmental risk assessment. The effect of parameter uncertainty on risk management decision making. In *Management Review* Vol. XXXX, 2009. No. 3. ISSN 0133-0179. [cit. 2021-11-24]. Available

at: http://unipub.lib.uni-corvinus.hu/658/1/vt_2009v40n3p10.pdf.

[4] SIPOS, T. *Development of a model for the development of road safety.* PhD dissertation. Budapest: BMGE, 2016.

[5] GYARMATI, J. Critical infrastructure risk and its measurement methods. In *Chapters on critical infrastructure protection, with a focus on the transport subsystem.* Study. Budapest: Hungarian Military Science Society, 2013. ISBN 978-963-08-6926-3. pp. 76-85.

[6] Association of Hungarian Logistic Service Centres. [cit. 2021-11-24]. Available at: http://mlszksz.hu/mlszksz-sulyos-karokat-okoz-az-onkoltsegalatti-fuvarozas/?v =35b5282113b8.

[7] SZŰCS, E. *Theory and practice of modeling.* [cit. 2021-11-24]. Available at: http://web.t-online.hu/eszucs7/modell/Modell.htm

[8] KOCZISZKY, G. *Impact analysis of regional networks.* Educational supplement. Miskolc, 2007. ROP-3.3.1.-05/1-12-0006/31.

[9] *Large graph with hubs.* Available at: https://images2.pianshen.com.

Péter **BODA (**PhD student)
Óbuda University
Doctoral School of Safety
and Security Sciencs
Béci út 96/b
H-1034 Budapest
Hungary
E-mail: pureglas@gmail.com

Col. (ret.) habil. Tibor **KOVÁCS**, Ph.D.
National University of Public Service
P. O. BOX 60
H–1441 Budapest
Hungary
E-mail: dr.kovacstibi61@gmail.com

Péter Boda was born in 1980. He graduated in Széchenyi István University (Győr) Faculty of Engineering, Department of Transport Engineering as a transport engineer (BsC). In 2008 he obtained a degree in MsC Defense Administration with a "good" qualification in Department of National Defense University. In 2009 he applied to the Miklós Zrínyi University of Technical Military for doctoral training, where he completed his theoretical studies in 2013. He is currently a PhD student at the Doctoral School of Security Sciences of the University of Óbuda.

Tibor Kovács was born in 1961. He graduated in Lajos Kossuth Military College Engineering Speciality (1984), Miklós Zrínyi Military Academy Engineering Speciality (1993). Summa cum laude received his PhD in Fortification from the Zrínyi Miklós National Defence University (1997). He served in the HDF in various positions. He is currently a lecturer at both doctoral schools at the National University of Public Service.

SCIENCE & MILITARY - WRITER´S GUIDELINES

1. Scientific articles submitted for publishing have to be original, topical and never been published before.

2. Articles have to be written in English language and in accordance with ethical standards. For more details, please visit the website of the Science & Military Journal (http://sm.aos.sk/index.php/en/for--authors-en/ethical-standards).

3. Length of the article should not exceed 6 pages in defined format. Microsoft Word text editor must be used for writing. Articles must be written using Times New Roman, single line spacing and follow the following form: Title -12 point bold capital letters aligned to the center. Full author´s (co-author´s) name – 10 point normal letters aligned to the center. Abstract – 9 point normal letters, extent 3-5 lines. Keywords – 9 point normal letters. The article text – 10 point normal letters. Contact - full author´s (co-author´s) name, affiliation, e-mail – 9 point normal letters at the end of the article. The article text will be written in 2 columns format with a 75 mm column width and 10 mm empty space separating the columns. The first line of each paragraph must be shifted 5 mm to the right.

4. Upper and lower margins must be set to 25 mm, left and right margins to 20 mm. Select mirror margins and set binding margins to 10 mm. The distance between the header/footer and the page margin must be 12,5 mm, while different odd and even pages must be selected.

5. Photographs for publication must be in black-white (not in color) of excelent quality with good contrast.

6. Equations in the text are also to be written using the equation editor. (Equation must be typed in Microsoft Equation, which is an integral part of Microsoft text editor.) They must be numbered. Numbers are to be enclosed in parentheses and aligned to the right margin of a column.

7. Figures, graphs and tables must be included in the text and numbered and must contain description. Figures must be identified as Fig. 1 followed gradually by the figure description. Graphs must be identified as Graph 1 followed by the graph description. Tables must be identified as Tab. 1, followed by the table description.

8. References must be fully and accurately documented (according to ISO 690). References should be quoted in the text in square brackets and listed in the order they have appear in the text.

9. The specimen article that can be found on the web-site: http://sm.aos.sk/index.php/en/for-authors-en can be used as an example of the correct format.

10. The editorial board will consider submitted articles in the next scheduled meeting. If it decides to include the article in the next issue it submits the manuscript to the editors for the peer review. The final version (before printing) will be sent to the author for the final revision. The authors are fully responsible for the level of language.

11. Contributions in A4 format edited according to the specimen article should be submitted in one hard copy and also in electronic form to the Editorial board.

12. The deadlines for the delivery of the articles in calendar year are: March 1 and September 1.

SCIENCE & MILITARY

No 1 | Volume 17 | 2022

Contents

ISSN 1336-8885 (print)
ISSN 2453-7632 (on-line)