Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 102 **2019**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2019.102.12

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Nowak, J., Ogonowski, K., Kustra, M. Selected threats to civil aviation. *Scientific Journal of Silesian University of Technology. Series Transport*. 2019, **102**, 141-150. ISSN: 0209-3324. DOI: https://doi.org/10.20858/sjsutst.2019.102.12.

Jacek NOWAK[1], **Krzysztof OGONOWSKI**[2], **Marek KUSTRA**[3]

SELECTED THREATS TO CIVIL AVIATION

Summary. The aim of this article is to discuss issues related to threats to civil aviation. The authors describe a relatively fresh subject which has been neglected so far due to the lack of knowledge and low popularity of this type of threat. The work identifies and characterises new threats to civil aviation. In order to achieve this aim, the article contains defined possibilities of using anti-aircraft mines and methods of using anti-aircraft rocket sets against civil aircraft in the operational area of the airport. The threats resulting from the use of unmanned aerial systems in the operational area of the airport are described together with the use of the cyberspace in a criminal manner in relation to civil aviation.

Keywords: anti-aircraft mines, portable anti-aircraft missile sets, unmanned aerial vehicles, cyberspace, cyber threats

1. INTRODUCTION

The authors of the article are of the opinion that these days potential terrorists do not have to infiltrate, physically or personally, the system of the airport security. The same effects can be achieved by using, for example, the so-called cyberspace, or open space of communication

[1] Faculty of National Security and Logistics, The Polish Air Force University, Dywizjonu 303 no. 35 Street, 08-521 Dęblin, Poland. Email: jacek.nowak@wsosp.pl
[2] Faculty of National Security and Logistics, The Polish Air Force University, Dywizjonu 303 no. 35 Street, 08-521 Dęblin, Poland. Email: k.ogonowski@wsosp.pl
[3] Faculty of National Security and Logistics, The Polish Air Force University, Dywizjonu 303 no. 35 Street, 08-521 Dęblin, Poland. Email: m.kustra@wsosp.pl

via computers and computer memories operating worldwide. This relatively new environment allows interaction and coupling of tools of creating information, registering, and communication. Today, the common storage of information in information systems makes cyberspace the main centre in which information exists. Therefore, it is possible to effectively manipulate this information or even generate false information, which threatens the security of civil aviation.

It should be assumed that terrorists can also take action in the so-called operational sector of the airport. This is understood by the airport facilities and the surrounding area, in which other entities provide assistance to an endangered aircraft within the of radius 8,000 m, in the case of a certified airport and 3,000 m, in the case of airport with limited certification or an airport for exclusive use - from the airport reference point [6]. In the operational zone of the airport, an act of unlawful interference may be used by minelaying, small arms, rocket-propelled grenades, portable missile kits and unmanned aerial vehicles. These are measures that effectively target objects at low altitudes.

One should not underestimate the possible use of anti-aircraft missile sets by terrorists in order to shoot down a civil passenger aircraft, especially during take-off or landing. Currently, it is estimated that there are several tens of thousands of anti-aircraft missile sets, which are beyond any control. It should be expected that these means may fall into the wrong hands.

The development and miniaturisation of unmanned aerial vehicles denote that they are being increasingly used not only in the armies of different countries but also by civil institutions and individuals. Drones are characterised by a low unit price, which makes them very attractive to use. Low price and the growing fighting capabilities of these vehicles turn them into an increasing air threat. A collision of a passenger plane with such an object can have tragic consequences.

The aim of this article is to identify and characterise new threats to civil aviation, which have often been disregarded. The research problem has been put in the form of a question: How do anti-aerial mines, anti-aircraft missile sets, unmanned aerial vehicles and cyberspace operations threaten civil aviation? In order to achieve the purpose of the article and answer the adopted problem, the authors focused on the following hazards. In aviation, it is believed that threats are the potential or existing phenomena, situations or actions affecting the aviation safety, posing a danger to life and health, property (aircraft and all aviation infrastructure), environment as well as limiting opportunities of the development of aviation organisations. The discussed threats are connected with: the ability to use anti-aircraft mines and anti-missile kits against a civil aircraft in the operational airport zone, the use of unmanned flying systems in the operational area of the airport and the use of cyberspace in a criminal way, in relation to civil aviation.

2. ANTI-AIRCRAFT MINES AS THREATS FOR THE SECURITY OF CIVIL AVIATION

In many armies all over the world, the enhancement of mining to combat air objects has been intensified. Therefore, the application of this means of destruction for terrorist purposes [9] cannot be disregarded. Due to the wide use of the latest technological advances in the field of electronics and materials engineering, efficient mines, both laid manually, in a mechanised manner and remotely operated, have been constructed. Owing to explosives, the so-called directional firing, it became possible not only to destroy armoured targets from large distances but also low-flying objects [9].

The capabilities of these means can be traced back to the example of the anti-helicopter mine, which was developed by the State Scientific Research Centre of Air Systems, on the outskirts of Moscow. The mine is intended to destroy targets at a distance of up to 150 m, using an explosively formed penetrator. It is designed for combat purposes of low-flying aeroplanes, helicopters and UAVs [11].

The mine detects the target using the sound system at a distance of 1 km, rotates the unit towards the target, scans its direction with an infrared sensor and finally fires the explosively formed penetrator. The mine can be laid manually or by means of land or aircraft resources of mining. The time of minelaying manually equals 5 min [11].

The sound sensor sensitivity allows detection of a flying unmanned apparatus at a distance of 0.6 km and in the case of a helicopter, at a distance of 3.2 km. The noise selection system allows detecting the sound of an aircraft or a helicopter engine in the noises of the battlefield. In the case of recognising a target at a distance of approximately 1 km, the mine turns into the direction of the target and activates infrared sensors (4-6 sensors), which ensure accurate homing-in.

Fig. 1. Russian anti-helicopter mine [11]

It is not possible when another target is being intercepted.Simultaneous operation of acoustic sensors and infrared sensors exclude a reaction of a mine to thermal traps fired by the target. After the target enters the firing zone of destruction (a hemisphere with a radius of 150 m), the explosively formed penetrator is fired, which hits the target at a speed of approximately 2,500 m/s. The operating time of a combat mine is not less than 3 months [11].

3. PORTABLE ANTI-ANTICRAFT ROCKET SETS - A SIMPLE AND DANGEROUS WEAPON.

A portable anti-aircraft missile is a lightweight anti-aircraft rocket intended to fight visually observable air targets, including planes, helicopters and other objects emitting radiation in the infrared spectral range. Due to the risks involved by this type of weapon, its possession, as well as international sales, are tightly controlled. Furthermore, too much attention is placed on terrorist attacks and on international trade, also in view of the threat of terrorist attacks using anti-aircraft rocket sets. The advances of technique and technology made it possible to construct portable anti-aircraft missile sets, operated on the battlefield by

one soldier. They are now used at all levels of air defence. They are capable of fighting objects at distances ranging from several hundred meters to several hundred kilometres and altitudes between several meters to tens of kilometres. Thus, there is no doubt that anti-aircraft sets which remain in the hands of terrorists and accidental persons pose a threat to civil aircraft.

Despite the continuous development of aircraft, portable anti-aircraft rocket kits still remain an extremely dangerous and very effective means of combating air targets. They are a focus of attention of all armies globally and, most importantly, of terrorist organisations. This is proved by the increasing incidents of stealing anti-aircraft sets from military depots and an ongoing demand in the market of illegal arms trade.

MANPADS (Man-Portable Air-Defence Systems) are systems for combating air targets, mainly intended for operation by a single soldier. They have been frequently used in various armed conflicts since 1969, that is, since the Egyptian-Israeli border clashes. The main element of MANPADS is an anti-aircraft rocket, placed in a tabular launcher, which guides itself to the most intense source of thermal radiation, which is the aircraft engine. By assumption, it is designed to be an inexpensive system, which is why its construction is simplified. For example, the same rocket does not have a proximity fuse, but an impact one, hence the eruption occurs at a time when it directly hits the warmest place of the aircraft. In addition, generally external detection systems are not used, and the detection itself is made by using a rocket homing head, in-built in the launcher tube. Moreover, the launch device is switched off and can be reused after replacing the used launcher.

The simplicity of the system does not mean that it is ineffective. Furthermore, it translates into the simplicity of its operation. It does not have any special calibration systems, tests and aiming. Everything is quite tough, and occasionally unaffected by errors of the operators. Initially, the easily accessible Russian rockets were the most effective. A good example can be Vietnamese, who only in the years 1972 - 1975 launched 589 rockets Strela-2 and Strela-2M that hit 204 American aircraft. They were also used in Africa, South and Central America, Asia and the Middle East.

An increasing number of acts of violence aimed at the aviation infrastructure forced the international community to take elementary actions to continuously modernise the level of civil aviation security. According to some estimates, there are probably more than half a million MANPADS around the world. Some models of these weapons are widely available and can be purchased on the black market. The attacks which occurred several years ago by means of short- range infrared homing missiles led to a situation that aircraft developers and supervisory bodies began to consider equipping commercial aircraft with protection systems of missile defence. Various surface-to-air missiles require different defence systems, which creates a number of opportunities for their producers. Only Israel decided to equip its civil aircraft with this device after an incident in 2002, when a plane, Arkia, was fired at in Mombasa during takeoff. Fortunately, the projectile missed the target. In accordance with the governmental Sky Shield programme, jet aircraft belonging to the national carrier El Al Israel Airlines, Arkia Israel Airlines and Israir Airlines are equipped with such equipment, which is manufactured by the local company Elbit Systems. The position of Israel was that the benefits outweighed the costs and insecurity.

The majority of anti-missile systems, designed for aircraft and helicopters, are to counter short-range and shoulder-fired missile threats. The USA equipped most of its military transport units with such protective devices, similarly to the United Kingdom and Australia. The systems manufactured by Northrop Grumman are in service with the heads of states, for

example, the Air Force One carrying the President of the United States as well as the German aircraft transporting the Chancellor.

The most important effect of mounting the system of self-protection on board an aircraft is to enhance the situational awareness for pilots, who are being informed about possible risks from anti-aircraft infrared guided missiles. The main aim of the kit is to defend against terrorists', militants' or various rebels' weapons, that is, against portable anti-aircraft short-range missile kits, MANPADS-type.

The Ukrainian company, ADRON Research and Development Company (R&D Ltd.) from Kiev, jointly with the Institute of NPK Progress in Nieżyn have been developing and producing such systems since 1982. The first of these, originally used in the Mi-24 helicopter was the 166W1AE intended for its protection against heat-seeking missile attacks. It produces an apparent source of infrared radiation in space. The device KT-01AWJe "ADROS" is the most modern version of the device L-166W1AE. On the helicopter Mi-24W with upgraded electrical wiring, the beams may be used interchangeably for both devices. Adron R&D Ltd has designed the equipment which protects helicopters and aircraft from all existing infrared threats, including MANPAD missiles, mistaking or "dazzling" the rocket guidance system and thereby changing the flight trajectory.

"ADROS" protects the aircraft against a direct strike from various types of missiles with infrared guided warheads, which operate in the modulation mode:

- amplitude-phase.
- frequency-phase.
- time-impulse.

The infrared radiation emitted by the radiator lamp with an electromechanical modulator is processed into subsequent thermal impulses. Infrared impulses that occur in such an order give misleading information about the location of the protected aircraft in relation to the optical axis of the head of an attacking missile. The presence of interference in the channel of the rocket control leads to disturbances of its trajectory, missile transition into a flight along an extending spiral until the loss of the tracked target. In the system there is no readiness mode, it runs continuously during the whole mission by providing stable and enduring protection for the plane or a helicopter. The system "tricks" all IR missiles within its range so that it is unnecessary to calculate the position of coordinates of the attacking projectile. The software is designed in the Assembler software code. It is flexible for future reprogramming and future system upgrades.

The aircraft protection against IR guided missiles is one of the priorities in the present time. The reason being the very high effectiveness of such missiles. Recent war experiences show that approximately 90% of all aircraft shot down in armed conflicts are destroyed by infrared- guided missiles.

The protection of aircraft against MANPADS-type missiles is usually ensured by creating false thermal targets by means of thermal or optical active electronic jamming systems. The operation of the electronic-optical active jamming systems is based on the principle of modular jamming of infrared radiation.

Although the aircraft protection devices against the discussed systems, are produced and mounted on military aircraft, the analysis shows that there is a possibility of fixing them on civil aircraft or helicopters.

Additional equipment of the aircraft with a radar warning receiver (RWR) would be designed to warn the crew against the illumination of air-defence artillery and missile launcher radars so as to take protective measures at an early stage, for example, in the form of

avoiding such positions. In this way, it would be possible to take appropriate measures to prevent an attack.

Presumably, there are a number of measures and aircraft protection systems currently against the most popular MANPADS attacks. They differ in the mode of action, the possibility of using them, the degree of complexity and obviously the price, which undoubtedly is one of the key issues when making a decision on the purchase and the application of a given means by an air carrier.

4. UNMANNED FLYING SYSTEMS - A THREAT IN THE AIRPORT OPERATIONAL ZONE

When considering the subject of threats to aviation, arising from the use of unmanned aircraft, in the first place, it is necessary to explain what they are. An unmanned vehicle is understood as a design for the execution of a flight, able to move cargo with the exception of transporting passengers. A more accurate explanation is included in NATO terminology, where the device is defined as follows: "a power-driven aerial vehicle, disposable or reusable, using aerodynamic forces to provide lift, which is controlled by or piloted remotely, capable of carrying lethal or non-lethal loads "[7]. The discussed aircraft are characterised by a variety of parameters and performance. Among the most important ones are: weight, range, endurance, and the practical ceiling. Due to their properties, the scope of their operators ranges from the armed forces, law enforcement services to civil companies. However, they are a source of threats to civil aviation, including airports. They result not only from deliberate human activity, but also from ignorance, misuse of unmanned aerial vehicles, too easy access to this type of flying devices, and the lack of appropriate legislation.

A significant threat to airports is near miss incidents when unmanned aircraft come too close to manned landing machines which were taking off or performing other air operations in the vicinity of the mentioned sites. In the history of aviation, there are numerous suchlike examples. A serious incident occurred on 20 July 2015 during an approach to landing of the airline Lufthansa at Warsaw Chopin Airport. The threat was caused by a drone, which was approximately 100 m from an Embraer 195. It is necessary to mention an event of March 2014 when a remotely operated rotorcraft was noticed at a distance of 30 m away from a Boeing 777 by its crew at Vancouver airport. Then in April 2014 at the same airport, a camera mounted on board an unmanned aerial vehicle recorded its flight at a very short distance from a landing aircraft. Another example was nearing of an unmanned aerial vehicle to a landing in a US Airways aeroplane at Tallahassee airport, on March 22, 2014 [11]. A dangerous incident took place in December 2014 at Heathrow airport, when a UAV was observed a dozen meters away from a landing aircraft [4]. Two incidents which occurred in the year 2014 in Australia also worth mentioning. On March 19, during an approach to landing at the airport in Perth, the pilot of DHC-8 had to abruptly change the course. This was due to the presence of a small flying object (witnesses of the event described it as a cylindrically-shaped unmanned aerial vehicle). To be precise, the aircraft, belonging to the carrier Skippers, passed the object at a distance of 20 m horizontally and 100 feet vertically. Three days later, the incident was repeated, namely, a rescue helicopter pilot had to perform an evasive manoeuvre to avoid a collision with an approaching unmanned aerial vehicle [1]. These incidents are just a few examples of dangerous near-miss incidents between unmanned aerial vehicles and manned aircraft. The threat results from the possibility of damage to the airframe, executing air operations within an airport, which may result in an emergency landing or even crashing the

machine, and consequently in the damage or destruction of property, loss of health or even life of crew members and/or passengers.

Due to easy access to unmanned aerial vehicles, they are used by terrorist groups. It is extremely dangerous since these devices enable carrying loads which may cause an explosion. In this way, it is possible to easily damage fuel storage depots, aircraft in aprons and even worse, damage terminals exposed to danger. The awareness is further expanded by the fact that these objects are remotely controlled by devices which enable operators to perform precise guidance towards the target. In addition, they are relatively small in size, thus quick detection tends to be difficult. A number of initiatives is being taken to counteract the discussed acts of unlawful interference. Defensive systems are been developed due to the increasing number of hazards connected with the use of unmanned aerial vehicles. An example is a solution applied in France. In case of discovering an unmanned aerial vehicle in a closed air space, the so-called anti-drones are activated, whose aim is to throw metal nets on the rotors of intruders [8].

5. ACTIVITY IN CYBERSPACE AS A THREAT TO CIVIL AVIATION

For several years, actions which breach security in the cyberspace, have been increasingly important. They are as important as the traditional ones. Cyberspace is the "space of processing and exchange of information generated by teleinformation systems [...] with the links between them and the relationship with users," [2]. In view of the above, it may be considered a virtual sphere designed to transfer, collect and share data. However, that is not all. The applications are linked with the possibility of attacks against information systems. In the case of the discussed subject, these are airport systems. For this reason, it is essential to care about maintaining an appropriate level of cybersecurity, which is understood as "a set of organisational and legal, technical, physical and educational designed to ensure uninterrupted functioning of cyberspace"(5). With regard to airports, this notion can be defined among others as the detection, response or prevention, counteracting deliberate actions conducted in cyberspace that are aimed at the violation of the information systems used at airports. Due to a wide spectrum of possibilities to pose threats in the discussed area, the examples of these were divided into intentional and unintentional actions. Intentional actions include the use of [13]:

- malware: a virus, a network worm, a Trojan horse, a dialler, a botnet.
- breaking security: unauthorised logs, account hacking, hacking into an application.
- internet publications: offensive content, copyright breaching, misinformation.
- gathering information: scanning, wiretapping, social engineering, espionage.
- computer sabotage: unauthorised exchange of information, unauthorised access or unauthorised use of the information, denial of access, deleting data, use of vulnerabilities in devices.
- the human factor: deliberate violations of security procedures, violating binding legal regulations.
- cyber terrorism:a terrorist crime committed in cyberspace.

On the other hand, unintentional activities are [13]:

- accidents and fortuitous events: hardware failures, link and software failures.
- the human factor: an unintentional violation of procedures, negligence, incorrect configuration of a device.

Due to increasingly occurring offences in cyberspace, in almost every sphere of human life, the scientific and aviation community began to research, seeking preventive and protective solutions. This is evidenced by conferences devoted to this subject. So far, two high-profile meetings have been held on cyberspace in civil aviation. The authors of this article participated in the second meeting (High Level International Conference on Cybersecurity in civil aviation), which was held on 08-09 November 2017 in Cracow. During the deliberations, an adoption of a strategy of proactive conduct in cyberspace was stressed. It was also suggested that the fragmentation of the management systems should be avoided. Attention was also drawn to the *Directive of the EU Parliament and the Council on measures to promote a high common level of security of networks and information systems in the EU (Directive NIS). The document obliges the Member States to implement* the national strategy for the security of networks and information systems. Moreover, in accordance with the development of *Cyber-Security, a new challenge for the aviation and Automotive industries* suggestions were listed which seem to be most appropriate for the security of the aviation industry and, in particular, airports against cyber threats. These, among others, include [14]: an introduction of tests checking the resistance of systems cyberthreats, testing of critical systems by external and independent companies that have genuine knowledge of cybersecurity, ensuring a high level of security of critical systems for communication. Moreover, every company in the airline industry should assess their needs in the perspective of cybersecurity; governments should establish appropriate norms and regulations in the field of cybersecurity.

On the basis of the above considerations, it appears that cyber threats are a relatively new, but extremely significant threat to airports. For this reason, numerous initiatives are taken to strengthen the resilience of systems to this type of threats. Unfortunately, the continuous development of technology promotes more frequent offences in cyberspace, making it difficult to conduct preventive actions.

6. CONCLUSION

The article is entitled: “Selected threats to civil aviation”. In relation to the subject, the authors adopted the following objective: identification and characteristics of new threats to aviation, which had previously been overlooked. The research problem is included in the question: How do anti-aerial mines, MANPADS, unmanned aerial vehicles and cyberspace operations threaten civil aviation? The answer to the research problem required careful analysis and, consequently, a synthesis of the literature and the use of knowledge acquired in the course of learning and professional work. For decades, the threat posed to civil aviation by individuals, have been associated with their presence and a physical attempt to overcome all sorts of security measures and regulations. Currently, this situation is changing. As it is commonly known, persons seeking to jeopardise this branch of transport are usually one step ahead of the law and security. This considerably hampers the work of services and induces a search for new legal or technical solutions.

The authors focused on four types of threats, that is, the ability to use anti-aircraft mines, MANPADS against a civil aircraft in the operational airport zone, the use of unmanned aerial vehicles flying in the operational area of the airport and the use of the cyberspace in a criminal way with regard to civil aviation.

Obviously, there are already technical systems which disturb the drone control or cause its physical destruction, however, they will not always be effectively used. Despite the existing technical solutions in that matter, the legal ones lag behind.

With regard to the protection of aircraft against air-mines, it seems that the only sensible solution is to patrol the operational airport zone, conducted on the ground and also in the air by means of unmanned aerial systems. By applying them, it is also possible to detect other threats such as tracking suspicious vehicles or individuals from the air.

MANPADS pose a serious threat, yet, due to advances in modern technology, this threat will be mitigated. Available off-the-shelf solutions should be implemented. It is worth investing in these measures.

The greatest challenge for civil aviation is its protection in cyberspace. The availability and universality of networking solutions intensifies this challenge even further. It cannot be stated that civil aviation is here, completely helpless. In the present conditions, the applied solutions bring appropriate results, however, still the question might be asked whether we will not be astonished by future developments?

References

1. ATSB Transport Safety Report.
2. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej.* Warsaw 2015. [In Polish: *Cybersecurity doctrine of the Republic of Poland*].
3. Evans A.E. 1969. „Aircraft Hijacking: Its Causes and Curve". *American Journal of International Law* 4.
4. Marszałkiewicz J. 2017. „Zagrożenia dla portów lotniczych ze strony bezzałogowych statków powietrznych". *Przegląd Komunikacyjny* 12: 2-12. [In Polish: „Threats to airports on the part of unmanned aerial vehicles"].
5. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*. Warsaw 2013. [In Polish: *Policy for Cyberspace Protection of the Republic of Poland*].
6. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 4 kwietnia 2013r. w sprawie przygotowania lotnisk do sytuacji zagrożenia oraz lotniskowych służb ratowniczo-gaśniczych (Jornal of Laws 2013 item 487). [In Polish: Regulation of the Minister of Transport, Construction and Maritime Economy of April 4, 2013 on the preparation of airports for emergency situations and airport rescue and fire-fighting services (Journal of Laws 2013 item 487)].
7. *Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje w NATO*. Brussels 2011. [In Polish: *Dictionary of NATO terms and definitions containing military terms and their definitions in NATO*].
8. „Tajna wojna anty-dronów". *Świat wiedzy.* 2015. [In Polish: „Secret war of anti-drone". *World of knowledge.* 2015].
9. Zajas S. 2007. „Przeciwdziałanie zagrożeniom terrorystycznym na lotniskach". *Zeszyty Naukowe AON* 2(67): 38-56. ISSN 2543-6937. [In Polish: „Counteracting terrorist threats at airports"].
10. Adron. Available at: http://adron.ua/en/weoffer/developments.
11. Military Institute of Armament Technology. Available at: http://www.witu.mil.pl/www/biuletyn/zeszyty/20080107p/33.pdf
12. Unmanned aerial vehicle. Available at: https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle#Aircraft_near-miss_incidents

13. CSIRT GOV. Available at: https://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731,Katalog-zagrozen-stosowany-przez-CERTGOVP L.html
14. „Cyber-Security, a new challenge for the aviation and automotive industries". Available at: http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf.
15. Petrus J. van V. Coetzee, Pieter A. Swanepoel. 2017. "Spatial relationships and movement patterns of the air cargo industry in airport regions". *Journal of Transport and Supply Chain Management* 11: a297. DOI: https://doi.org/10.4102/jtscm.v11i0.297.

Received 12.10.2018; accepted in revised form 30.12.2018