of the Aeronautical Sciences
Belo Horizonte, Brazil; September 09-14, 2018

IMPACT STUDY ON CYBER THREATS TO GNSS AND FMS SYSTEMS

R. Geister, J.-P. Buch, D. Niedermeier*, G. Gamba, L. Canzian, O. Pozzobon **
***German Aerospace Center, ****Qascom**

Keywords: *Cyber Security, Flight Management System, Flight Simulation, Human Factors*

Abstract

Within this work, that was carried out following a call for tender by the European Aviation Safety Agency (EASA), the impact of cybersecurity threats especially on Global Navigation Satellite Systems (GNSS) and Flight Management Systems (FMS) was assessed. In order to do so, simulation studies were carried out.

The German Aerospace Center (DLR) operates the research simulator AVES (Air Vehicle Simulator) which was used for the flight simulation exercises within this project. The AVES combines two facilities to simulate airplanes and helicopters to the highest technical level. The cockpit unit used was a complete replica of an Airbus A320. The corresponding simulation software (incl. flight dynamical models and system simulation) is entirely developed at DLR according to the official documentation providing full access and flexibility in the investigations. The motion platform provides a motion system with six degrees of freedom, whose motion cueing algorithms can be specifically tuned for a given task if needed. This unique infrastructure has been built during the last years with the aim of providing a highly-representative test platform for new cockpit functions and flight crew training research.

To assess the impact of cyber-attacks on GNSS and FMS, different scenarios were developed and ranked by their likelihood of occurrence and their expected impact on safety and the continuation of the flight. Based on the identified threats, realistic scenarios according to airline operations were designed and implemented into the AVES research simulator. Synthetic error models reproducing the same effects on the aircraft systems as identified in the projects preceding GNSS and FMS threat assessment work were integrated into the AVES software architecture. In particular, the impact of GNSS jamming and spoofing attacks during satellite based approach procedures was investigated. In addition, attacks on the FMS through the open protocol of the Aircraft Communications Addressing and Reporting System (ACARS) were assessed.

In this paper, we are going to present the results that were obtained during the simulations with airline pilots holding Air Transport Pilot's Licenses (ATPL) with a special focus on the attacks on the FMS and its related systems. We are going to describe the simulation setup and the reaction of the pilots and we will give pilot training and cockpit systems design recommendations in order to mitigate risks that stem from the investigated threat scenarios.

1 Introduction

Cybersecurity threats are of increasing importance for aviation. As aviation systems (on-board and on the ground) are getting more complex and increasingly interconnected, the vulnerability to cyber-attacks must be taken into account. Currently, European projects are focusing on the whole Air Traffic Management (ATM) system, e.g. [1]. In addition, some activities have been focusing on aircraft systems themselves, e.g. [2]. In this work, the primary focus is on the impact of cyber-attacks on the flight crew.

The scope of the project encompasses the preliminary risk assessment at system and aircraft level for potential cyber-attacks to the Flight Management System (FMS) and to the Global Navigation Satellite System (GNSS) receiver, including GBAS and SBAS augmentations. Furthermore, this work was used to assess the impacts of such cyber-attacks on the flight crew in simulator trials.

The work is conducted considering generic functional architectures for aircraft systems and does not encompass the development of detailed system architecture. The assessment covers the analysis of potential failure cases and the characterization of potential impact for flight operations (covering all flight phases), while considering the main (existing) mitigations at the level of flight crews working methods and operational procedures.

2 Test Setup

During the project, a security risk assessment was carried out for different attacks. The methodology used was similar to the methodology described in [3] and a proposed methodology in [4]. In general, the attacks were assessed in terms of attacker capability and exposure level of the assets. In our case, the assets are the functionalities provided by the FMS and the GNSS receiver.

This assessment led to a likelihood assessment of the attack. This likelihood was put into context with the safety impact of the attack. This classification was similar to the risk assessment used in the certification of large airplanes [5]. With this methodology, the severity of the attacks was ranked. After that, we selected some of the high ranked attacks and used them for simulator trials with airline pilots.

2.1 The AVES Simulator

The AVES simulation is performed on a distributed simulation network comprising a multitude of computers (see Figure 1). It has a centralized communication structure with the Interface Computer (IC) being the source and destination for all simulation data, i.e. each software module gets its input data from the IC and returns its computed data to the IC. All of the communication except for some infrastructural ones is performed using UDP connections.

All simulation software was produced at DLR with the overall focus on human factors experiments and flight experiment preparation mostly dealing with flight performance and flight dynamics analyses with DLR's research aircraft fleet. The following list summarizes a short statement for all major simulation modules used within the basic AVES simulation.

- Aircraft Model: The aircraft model containing the flight performance and flight dynamics is based on flight test data gathered with DLR's Airbus A320 research aircraft and resembles the aircraft behavior with a high accuracy for a wide flight envelope. For research, a variety of different aircraft models can be used in AVES. However, for the experiments conducted within the current activity the A320 simulation model will be used as it is most suitable for this task (commercial transport aircraft of the 4th generation).
- System Simulation: It creates the functionality behind all cockpit switches. The basic software design consideration behind the system simulation was to focus on reproducing the correct system logic and behavior for the pilot by using the official system documentation from DLR's Airbus A320 ATRA aircraft (FCOM, FOM, QRH, AMM) augmented with comments from DLR's A320 test pilots and data from accident reports that sometimes reveal the correct system behavior that is opposing to the aircraft documentation.
- Visual System: For the simulation of the outside vision a visual database was generated using satellite images (taken by DLR) on top of a terrain model. The visual database contains the area of Germany exclusively.
- Sound Simulation: The sound simulation comprises generic transport aircraft noise which is augmented by type

specific sounds (e.g., warning sounds, power transfer unit sound, etc.).

- Motion System: The motion system uses a 6 degree-of-freedom electro-pneumatically driven Stewart platform for simulating forces and is provided with acceleration values from the aircraft model.
- Simulator Runtime Environment: The runtime environment contains all elements that are needed to either let the simulation run or control it (e.g., start, stop, hold). The Interface Computer (IC) that holds and distributes all simulation data to all simulation modules or the Instructor Operator Station (IOS) are two prominent members of the simulator runtime environment.

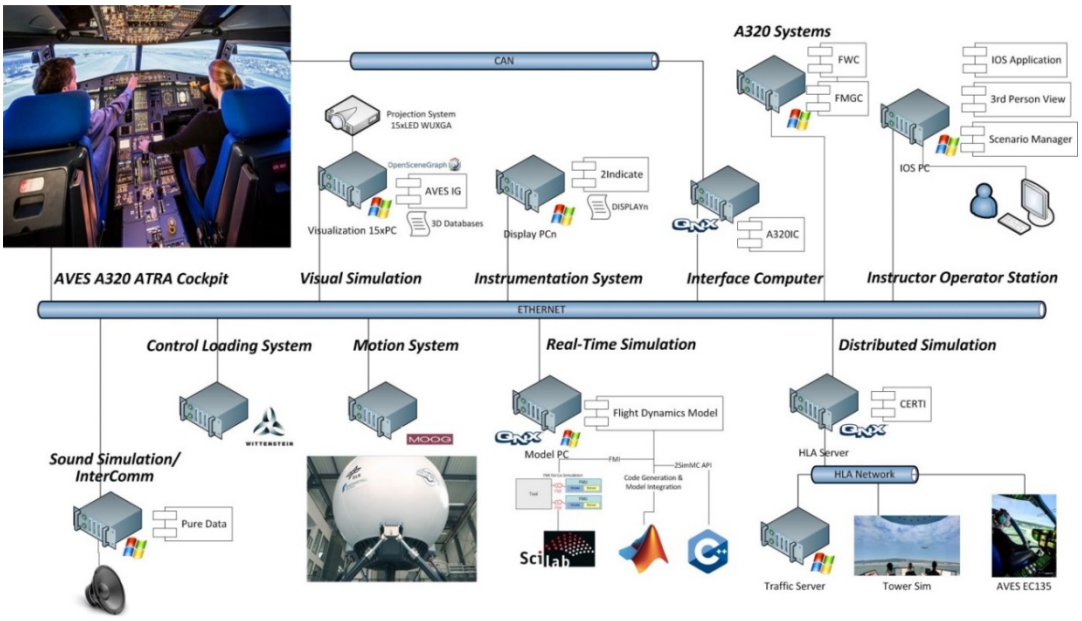


Figure 1: AVES system architecture

2.2 Simulator Scenarios

In total, seven simulator trials were conducted. Each trial was set up as a scheduled flight from Munich airport (EDDM) to Hanover airport (EDDV). In order to focus on the essential scenario flight, the taxi phase is skipped and the aircraft was positioned at holding point A13 of runway 26R in Munich. The RNAV (GPS) standard instrument departure "INPUD2N" was used for departure.

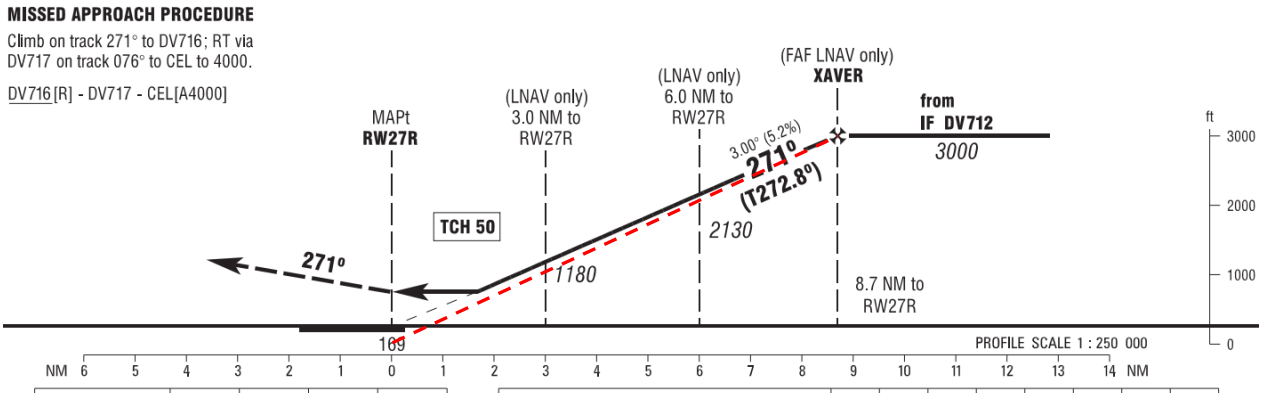
The intended flight plan then contained a standard routing to Hannover at a final cruising flight level of FL300. For the transition between the en-route part of the flight and the approach the arrival route "ELNAT4P" is used.

For the approach in Hanover, a Required Navigation Performance (RNP) 0.1 approach was specifically designed for these trials and implemented in the simulator (see Figure 2). This means, that the cross-track error during the approach shall be less than 0.1NM in 95% of the time. This type of approach was chosen, as satellite based approaches are becoming more common and RNP0.1 approaches impose high requirements on the navigation accuracy and integrity. Such approaches are often used to avoid terrain which makes the potential impact in case of failure very high.

The weather was utilized as a scenario element in the way that for the approach in Hanover the weather will mask the position and altitude deviations introduced by the GNSS and

FMS attack events. In the scenario Hanover is chosen to have broken clouds (BKN) with a base of 300ft Above Ground Level (AGL). The intention behind this is that the flown approaches will have a minimum descent altitude of 250ft AGL and so visual position and altitude deviations will be masked until the aircraft breaks out of the clouds close to the ground. The weather at the departure airport Munich is far less critical with a cloud base of 3000ft AGL which will also be the global could coverage along the whole flight.

The wind situation was generally calm with four to five knots at ground level from a westerly direction. The temperature was simulated according to the standard atmosphere (ISA+0) and therefore there was no need for a temperature compensation for the baro-referenced (LNAV/VNAV) approaches.



OCA (OCH)	A	B	C	D
LNAV 0.1	670 (500)	670 (500)	670 (500)	670 (500)
LNAV / VNAV 0.1	420 (250)	420 (250)	420 (250)	420 (250)

DIST THR / RW27R	2	3	4	5	6	7	8	
ALTITUDE	860	1180	1500	1820	2130	2450	2770	

Timing not authorized for defining the MAPt.

GS	kt	80	100	120	140	160	180
XAVER - RW27R (8.7 NM)	MIN:SEC	6:32	5:13	4:21	3:44	3:16	2:54
Rate of descent (5.2%)	ft / MIN	420	530	640	740	850	960

Figure 2: RNP0.1 approach (dashed line after simulated attack)

2.3 Operational Setup

For the simulator trials, one airline pilot was invited. He was the captain and the pilot monitoring on the simulated flight. A member of the simulator staff was acting as the co-pilot and the pilot flying to create similar behavior for all the trials. For one experiment two airline pilots were invited to check whether the behavior of the actor pilot was comparable which it was. The general simulator briefing contained information about the experimental run, giving a false clue to the pilots about the experiments intention and excluding cybersecurity matters. Also included in this part was a safety instruction for the AVES simulator and relevant differences that are to be expected in AVES when compared to the real world, including a short familiarization flight in the simulator. This familiarization flight consisted of two ILS approaches onto runway 27R at Hanover airport followed by a visual traffic pattern. The briefing is performed in the AVES briefing room, the familiarization flight is performed in AVES. After the familiarization flight the crew comes back to the briefing room again for the following flight briefing.

For each simulator trial, a short operational briefing was given in form of a Power Point presentation. Afterwards, the documents for the flight were handed to the pilots. The briefing included the departure and destination airports, as well as the flight plan. In addition, the performance calculation including fuel quantity and the weight and balance were presented to the airline pilots.

The weather briefing was the same for all flight trials It was good enough to conduct a non-precision RNP approach but bad enough not to spot the altered approach path before the minimum descent height.

3 Simulation Results

3.1 ACARS Loadsheet update

The threat scenario assumed that an attacker on the ground possesses the ACARS addresses of multiple aircraft and transmits falsified load sheet data via ACARS to the aircraft. On-board, the data is received, either by a print out or directly in the FMS. The worst condition for a take-off would be an aft CG and additionally a nose up trim. The elevator of the aircraft would, at certain values, lose the ability to pitch down the aircraft and that could result in an uncontrollable aircraft state. The attack would occur during the preflight phase but the results would become present in the take-off phase. Therefore, the scenario will be assigned to the take-off phase.

Figure 3: Loadsheet update in the simulator trials

For the attack, it was assumed the aircraft has a center of gravity (CG) that is close to the backmost allowed position. For the attack a falsified W&B with a forward CG was generated. This falsified information is then sent by the attacker to the aircraft via ACARS. Although the computed takeoff weight did not changed, due to the falsified weight distribution the trim setting is 1.6° up instead of 1.6° down. In this situation, the aircraft had a pitch up trim setting with an aft CG. This was leading to an early pitch up moment of the aircraft during the Take-Off roll. This occurred before the rotation speed.

In the simulator trials, this attack was simulated in all seven trials. The falsified data was accepted in six of those seven cases. It was rejected only once.

3.2 ACARS Flight Plan Update

For this scenario, it was also assumed that an attacker on the ground possesses the ACARS addresses of multiple aircraft and transmits falsified flight plan data to an aircraft. The attacker would need to know the departure and the arrival airport and have an idea of the used route to tailor the attack to the actual flight path but the data is easily obtainable through observation. If the pilots accepted the new flight plan, the aircraft would deviate laterally from the desired path (filed flight plan).

The attack changed the en-route part of the flight plan between two IFR waypoints including a change of the proposed arrival route that is changed from the original “ELNAT4P” to the “GITEX4P” arrival.

Further, it was assumed that the bogus flight plan update was transmitted by the attacker via ACARS and printed out on the aircraft’s printer.

This attack scenario was used in two of the seven trials. The new flight plan data was rejected in both cases.

3.3 FMS Denial of Service Attacks

It was assumed that an attacker on board of the aircraft is able to access an interface to the FMS. The attacker starts a denial of service (DoS) attack so that the FMS is not responding and freezes at 100% task load. The complete functionality is lost. No flight planning via MCDU is possible nor is a map displayed. Independent navigation systems (VOR, DME…) are with backup display systems are still available. This situation will lead to an increased workload in the cockpit due to increased communication activities between the

pilots and with Air Traffic Control (ATC). In addition, paper navigation and/or ATC guided navigation will be required.

Once the DOS attack scenario was started, the MCDU screen was frozen and the system did not react to the pilots' inputs. The map on the Navigation Display (ND) disappeared with the "MAP" flag showing up in the ND. Additionally, both autopilots (AP) and flight directors (FD) disengaged and were not resettable.

The DOS attack was triggered during the en-route part of the flight. The DOS attack had a duration of 180 seconds. This scenario was used in two of the seven trials. The effects of this simulated attack were detected instantaneously; however they were not identified as cyber-attacks.

3.3 FMS Database Attacks

In this scenario, an attacker was able to access the servers of a FMS database provider. As the approach data (waypoints, altitudes…) for RNP or SBAS approaches are stored solely on the database on-board the aircraft, an altered database poses a threat to the integrity of the approach. In our scenario, the final approach segment data of one or several approaches are altered. Specifically, the data for a RNP0.1 approach is changed. The attacker was able to lower the threshold height so that the glide path leads into the ground way before the real runway. The aircraft concluded an approach in poor weather conditions with a cloud ceiling around 250ft. The attacker was able to change the data so that the aircraft reaches that altitude before the actual runway starts.

The attacker managed to generate a FMS database with a falsified threshold height for the approach to runway 27R of Hanover airport. The nominal threshold height for this runway was 169 ft MSL before the attacker set it to 0 ft MSL while leaving the altitude of the final approach fix XAVER of 3000ft AGL unchanged. This changed geometry leads to a potential ground contact approximately 0.5 NM in front of the threshold of runway 27R.

As the corrupted database would have to be loaded into the FMS prior to the flight, this attack would already have been performed long before the actual flight. In the AVES simulator the attack is triggered similarly by the way that already before the start of the scenario a falsified FMS database is loaded into the system. The database is an identical copy of the nominal AVES simulator FMS dataset, except for the threshold altitude of runway 27R of Hanover Airport.

This scenario was used in six of the seven simulator trials. Out of those six times the effects of the attack were detected by the flight crew. Due to the fact that the approach was cross-checked by the Pilot Monitoring (PM) with the approach chart, the flight crew was able to detect the deviations from the desired flight path. Only during one simulator trial, this cross-check was not carried out and therefore, a go-around was initiated at the decision height as visual contact to the runway was not established.

4 Discussion of the results

The results show, that the investigated scenarios are relevant to common airline operations. The involved pilots stated that the scenarios were realistic in terms of operational procedures. For instance, it is not uncommon that pilots receive several loadsheet updates before the flight. Given the venerable nature of the used data link (see also [2]), this threat scenario needs to be considered in future applications.

Within the trials, the loadsheet update was accepted six out of seven times and subsequently used to change the values in the FMS. It has to be stated however, that the test setup might have played a role as pilots stated that in reality they would have further investigated this huge change in the trim setting.

Regarding the ACARS flight plan update, the results show that such an attack will very likely not be able to change the route of an aircraft in flight as all changes would have to be negotiated with ATC. In this work, the flight plan update was disregarded in both simulator trials. However, it could lead to increased workload and voice communication especially if an attack on multiple aircraft within a single ATC sector is considered. Additionally, digital

communication and ATC clearances were not considered here.

The DoS attack on the FMS was not identified as a cyber-attack by the pilots. However, the effects were noticed instantaneously in both cases they were used. As soon as the flight crew noticed that the aircraft was still controllable and raw navigation data was available, the event was handled in a routine manner. This is due to the fact that a FMS failure is a scenario that is usually trained in recurrent simulator training. The pilots started interacting with ATC to resolve the situation. Therefore, a dangerous situation did not arise. However, workload is increased in the cockpit and also the required amount of voice communication is increased.

The scenario with the altered FMS database was used in six out of the seven simulator trials. In five of the six cases, the effects of the attack were discovered through the cross checking of the altitude with the approach charts. The deviation of the flight path was discovered and a go-around was initiated before the minimum descent altitude. In one case, the altitude cross-check was not conducted. Therefore, the approach was flown down to the minimum descent altitude and there a go-around was initiated as no visual contact was made to the runway. As a go-around is a standard procedure, no critical situation arose from the attack. Still, the corrupted database could affect multiple aircraft and could lead to congestion and an increase of voice communication demand.

Based on the results of the tests and on the feedbacks from the involved pilots the following list of recommendations should be considered in order to implement procedures for threat mitigation:

- The altitude / height cross-check during GNSS based approaches (i.e. RNP0.1) is a valuable and important safety net, it should be strictly enforced and considered as a valid safety tool; indeed one test showed that without checking the altitude the wrong flight path was only noticed at the Minimum Decent Altitude, whereas in the other tests the pilot monitoring checked the altitude and was able to identify the deviation from the charted path before the MDA which led to a go-around at a higher altitude.
- The altitude / height of the runway threshold should be displayed explicitly in the FMS in order to be checked in the approach briefing; the tests showed that the coordinates of the runway threshold as well as the height of the threshold could not be checked properly beforehand. It would be beneficial to clearly display the threshold data in the MCDU so that it can be cross-checked before the approach. That would help to identify mistakes at an earlier stage.
- For ACARS updates, a procedure should be considered to ensure the validity of the received information, for example through an authenticated data transmission or by letting the flight crew respond to or confirm the changes in a secure way. This especially includes updates of the flight plan on the ground; the tests showed that in the simulator environment, the Loadsheet update via ACARS was accepted in 6 out of 7 cases. This means, that there is a lack of control possibilities to validate the correctness of the update. It was also identified that a flight plan update on ground could be a dangerous attack as this is usually not checked and confirmed with ATC.
- The pilots and ATCO should be trained to be aware of the possibility of cyber-attacks and the effects they could have; In general, the pilots did not suspect cyber-attacks behind the malfunctions during the trials. Therefore, the awareness for possible attacks and their impact should be intensified.

5 Conclusion

Within this work, seven simulated flights were performed with airline pilots, emulating several cyber-attacks on FMS and GNSS at different flight phases. The pilots were invited to the

trials under false pretenses in order to obtain unbiased results.

During each flight trial, three simulated attacks were conducted. No involved pilot associated the experienced effects to a cyber-attack. Indeed, the pilots were very interested in the results afterwards and their awareness in cyber-security was increased.

Most of the considered cyber-attacks were not detected by the crew at the time of the attack. Miss-detected attacks always led to an increased workload of the crew and of the ATCO, but they never resulted in critical situations during the flight exercises. However, the results of the flight exercises are limited to the considered flight route scenario and statistical considerations cannot be derived because of the limited number of tests. In fact, some pilots considered certain attacks as potentially dangerous in real scenarios.

Among the considered attacks, the two attacks that were considered most critical are the “Hacked database” attack and the “GNSS spoofing attack”. The “Hacked database” attack was discovered five out of six times by the monitoring pilots, thanks to the cross checking of the actual distance/altitude with the approach chart.

In addition to help in understanding the cyber-attacks effects during a flight, test exercises performed with real pilots were also useful to collect the feedback from the pilots, such as the most critical attack scenarios, differences in operations/procedures of different airlines, and recommendations for threat mitigation procedures. The outcomes of the trials show that important mitigation procedures include altitude/height cross-checks, interaction among pilots and ATCO to confirm updates and aircraft positions, and pilots and ATCO awareness of the possibility of cyber-attacks.

Even though additional investigations should be conducted to derive statistically significant results and different scenarios should be evaluated to assess the impact of different types of attack route and attack configurations, even this limited number of simulations performed here show the importance for the aircraft industry to investigate the impact of cyber-attacks on different aircraft systems. In particular, putting the pilots “in the loop”, analyzing their actions during simulated attacks, collecting their feedback afterwards and increasing their awareness regarding possible effects and attack possibilities appears to be the correct path to pursue this investigation.

8 Contact Author Email Address

Robert.geister@dlr.de

References

[1] T.-H. Stelkens-Kobsch, M. Finke, “Validating an ATM Security Prototype – First Results”, 35th DASC, Sacramento, USA, 2016

[2] H. Teso, “Aircraft Hacking”, April 2013, https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf, accessed on 11.06.2018

[3] EUROCAE, ED-202A – Airworthiness Security Process Specification, 2014

[4] S. Gil Casals, P. Owezarski and G. Descargues, "Risk assessment for airworthiness security", Computer Safety Reliability and Security (SAFECOMP'12), vol. 7612, pp. 25-36, 2012.

[5] European Aviation Safety Agency (EASA), “Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25”, Amendment 12, 13.7.2012, https://www.easa.europa.eu/sites/default/files/dfu/agency-measures-docs-certification-specifications-CS-25-CS-25-Amdt-12.pdf, accessed on 11.06.2018

Acknowledgement

This work was performed within the “Impact Assessment of Cybersecurity Threats” project. The authors would like to express their gratitude to EASA for their support and the funding of the project.

Copyright Statement