# Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status

**M B Guzairov[1], A I Frid[1], A M Vulfin[1] and V V Berkholts[1]**

[1]USATU - Ufa State Aviation University, Karla Marksa street 12, Ufa, Russia, 450000

**Abstract**. Modern aviation systems are complex hierarchical computing systems, coupled with a powerful periphery (digital board). The flight is performed with constant communication with ground control points and requires exchange of large amounts of data. The reliability of the systems providing flight can be violated due to equipment failures, human factor and external unauthorized exposure. The paper discusses the issues of guaranteeing the reliability of telemetry information transmission systems on the state of the aircraft and its systems based on artificial intelligence methods in terms of ensuring information security. The structure of the imitation stand is proposed to test the system for transmitting telemetric information about the state of on board airborne systems to the ground. The purpose of such system is to improve the efficiency of modelling and analysis of the system's security.



## 1. The first section in your paper

Provision of dependability telemetric data transmission systems (TMI) is a primary goal of ensuring the efficient functioning of the aircraft.

The application of technologies for monitoring the status of critical elements of the aircraft's design in real time will allow a full (operational and intelligent) analysis of the operational capability of the aircraft systems (LA), crew conditions and control of its actions in the ground control center.

For example, the Bombardier jetliner was demonstrated at the Paris air show. It has a motor that is equipped with 5000 sensors, which generate up to 10 GB of data per second. A single twin-engine aircraft with an average 12-hour flight time can create up to 844 TB of data [1]. The arising malfunctions and failures of the on-board equipment can be diagnosed on the basis of the processed telemetric information. This allows experts of ground technical services to prepare for operational repair even before landing the aircraft. Accumulated and processed TMI will allow specialists to provide reasonable support for decision-making in the event of technical failure of aircraft units or modules.

The possibility of transmitting TMIs on the actual state of individual modules to the manufacturer of aviation equipment units will make it possible to increase the operational efficiency of the aircraft in its normal state and in the event of failures, as well as when investigating incidents. For example, a study of ground-to-board communication systems showed that the ACARS system, despite its versatility and ubiquitous use, is vulnerable, and if it is hacked with ADS-B, an attacker can gain access to the flight control system, download flight plans and detailed commands [2].

The purpose of this study is to increase the security of the TMI transmission system on the status of individual elements of on-board systems in an automatic mode based on the use of modern technologies of protection and processing of TMI using an imitation stand.

To achieve this goal, the following tasks are formulated:

1. Develop a structural scheme for the collection, transmission and reception of telemetric information on the status of individual elements of the aircraft systems of the aircraft;

2. Develop the architecture of the system for analyzing the security of the TMI transmission system on the status of individual elements of the aircraft system.

Formatting Structural scheme for the collection, transmission and reception of TMI on the status of individual elements of the aircraft system.

## 2. Structural scheme for the collection, transmission and reception of TMI on the status of individual elements of the aircraft system

Automated information system (AIS) of ground maintenance services is a set of software and hardware needed to receive, store and process information on technological parameters of complex technical device (CTD). A typical block diagram of the existing TMI processing system of the manufacturer is shown in Figure 1. An analysis of existing approaches to solve the problem of ensuring the reliability of such systems is considered in the work [3].

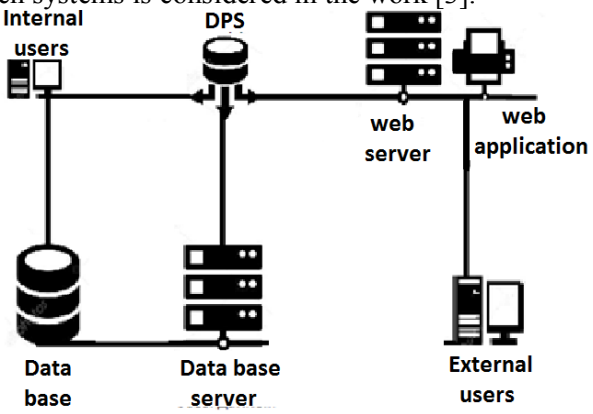



**Figure 1**. Structural diagram of the TMI processing system.

AIS solves the main tasks associated with receiving information about the state of a complex technical device. Data is planned to be received in three different ways (figure 2):

1. Directly from the system. STD is a component of this system;

2. By reading the event log from the CTD module sensors. The status of the modules is read and stored during the previous period of operation.

3. Entering events into the database manually. The operator processes the information and enters information through the WEB application.

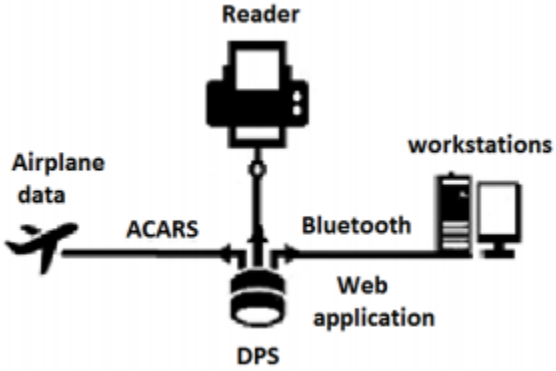
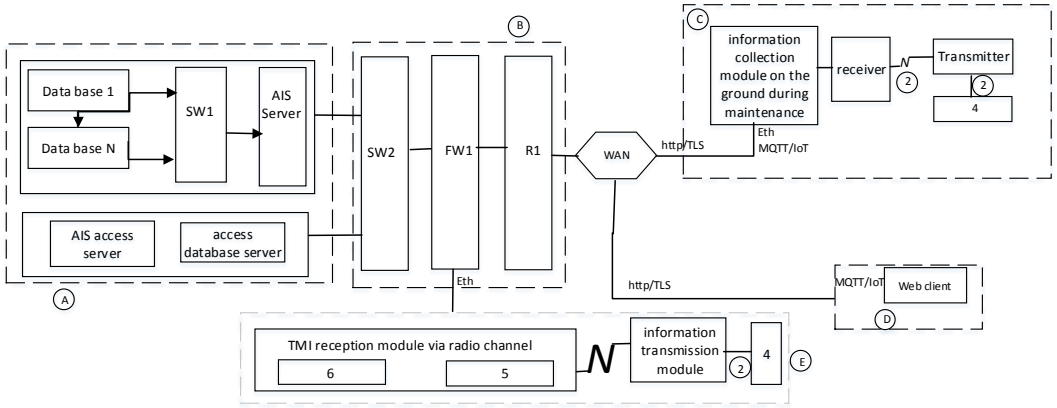



**Figure 2.** Methods of obtaining TMI.

Data is entered into the database via web-application in the second and third cases. WEB-application is an insulating layer between external networks and internal structure of AIS, since access from an external network is one of the most vulnerable places of the system. The structural scheme of the collection and transmission of TMI is presented in Figure 3.




A-simulation model of the server part of the processing system
B- module for simulating the network subsystem
C-module for information collection at stations. Services
D - module for simulating access via web-client
E- data transfer via radio channel

1. Database replication
SW1- communication equipment of the AIS module
SW2- communication equipment of AIS network
FW1-Firewall
R1-Router NAT
2. RS-485 / Modbus
3. NIST Technical Series Publication (Bluetooth)
4. TMI collection assembly from aircraft

**Figure 3**. Structural scheme for the collection, transmission and reception of telemetric information on the status of individual elements of the aircraft system.

In the work of the authors [3], the problem of providing secure access to the existing database containing critical information about the parameters of the life cycle of complex technical products (CTD) using the example of gas turbine engine control system was considered.

Thus, increasing the security of access to a database containing critical information about an exploited product is based on the development of a secure WEB application architecture. It serves as an isolating layer for external AIS clients, which allows for the provision of the ability to transmit and analyze at ground service stations and to provide remote access to the required data. Prevention of vulnerabilities in the WEB-application is carried out by implementing measures to develop secure software, established by GOST R ISO / IEC 12207 [4].

Modeling security threats and identifying vectors of possible attacks, as well as their analysis, allowed to formulate countermeasures for each of the vectors at different architectural levels of the WEB application.

The growth in the volumes of telemetric information forces the aviation industry to consider new approaches to collecting and analyzing a large amount of data on the condition of aircraft nodes and elements. The concept of an industrial Internet of things is developing actively (IIoT). This is a deployed network consisting of a large number of devices equipped with a set of sensors that exchange data with each other through low-power and short wireless connections. The first step is to collect data from the sensors. One of the most promising solutions is a protocol with low power consumption and low transmission radius IEEE 802.15.4 IEEE 802.15.4e [5]. A short range is sufficient to transmit data within the ground service station. The IEEE 802.15.4 and IEEE 802.15.4e protocols and their architecture layers are subject to IETF standards [6].

The question of analyzing the security of the system for collecting, transmitting and receiving telemetric information on the status of individual elements of aircraft systems during data transmission through the first two channels remains an open question. The violation of the information security of the TMI collection and transmission system under consideration can be caused by a variety of

different reasons: vulnerabilities in operating systems and server and client applications; incorrect configuration of hardware and software; access control settings errors, and so on.

External and internal violators can implement various strategies to attack the system. The attacker can use combinations of available vulnerabilities and network configuration and security policy (PB) deficiencies. These strategies can be designed to access a database that contains critical information about STI. Strategies can also include multi-step chains of attacking actions to implement security threats. This arises the task of verifying the provision of the necessary level of security The level of security of the system is determined by a set of parameters for the configuration of the data transmission network, security policy and protection mechanisms.

The initial data for analyzing the security of the TMI collection and transmission system are its specifications and security policies. The task of developing the architecture of the security analysis system (SAS) is due to the high complexity of the TMI collection and transmission system. This increases the number of vulnerabilities and potential errors of the software and hardware components. The SAS of the TMI collection and transmission system should detect errors in the transmission network configuration, possible routes of attacking actions of various categories of violators (for implementing various security threats), identify critical network resources and ensure the selection of adequate security policy threats. The core of the CAS are algorithms for assessing the level of security of the system, it is based on the construction of possible actions of violators in the form of attack graphs. The properties of the attack graph are checked and the system security metrics are calculated [7].

The system for analyzing the security of the transmission of telemetric information includes the implementation of a set of models:

• behavior model of an attacker;

• simulation of the graph of attacking actions aimed at the implementation of information security threats taking into account attacker's qualification;

• vulnerability model of the system;

• calculation of security metrics system and assessment of the overall level of security.

The security analysis system is a software package implemented as a hierarchical set of client-server applications. AIS enterprise interaction is carried out by means of a Web application with remote TMI transmission modules: a secure channel, single-board microcomputers with a set of required wired and wireless network interfaces, intermediate switching equipment, a client and server computer. Input data for security analysis are:

• specification of the configuration of the information system for data collection and transmission of TMI;

• specification of the planned security policy;

• hardware and software vulnerabilities;

• model of the intruder;

• requirements to the security of the information system.

The output of the CAS are:

• identified vulnerabilities of the system;

• graphs of possible attacks; • security metrics;

• evaluation of the overall level of security of the system and its components. The obtained results provide the development of well-founded recommendations on elimination of identified bottlenecks and strengthening of the system's security.

The simulation stand is a software implementation of the system for analyzing the protection of the transmission of telemetric information on the state of airborne systems. The generalized architecture of the proposed CAS is shown in Figure 4.

The module for configuring the security analysis model allows the security specialist to manage the operation of all system components, specify the input parameters of the analysis process, the requirements for the level of security, and review security analysis reports and receive recommendations for enhancing the security of the TMI transmission system. The management and administration module provides access to external vulnerability databases and configuration settings

for other modules (modeling of IS nodes, simulating an attacker and its actions, as well as updating the DB and the Knowledge Base (KB)).

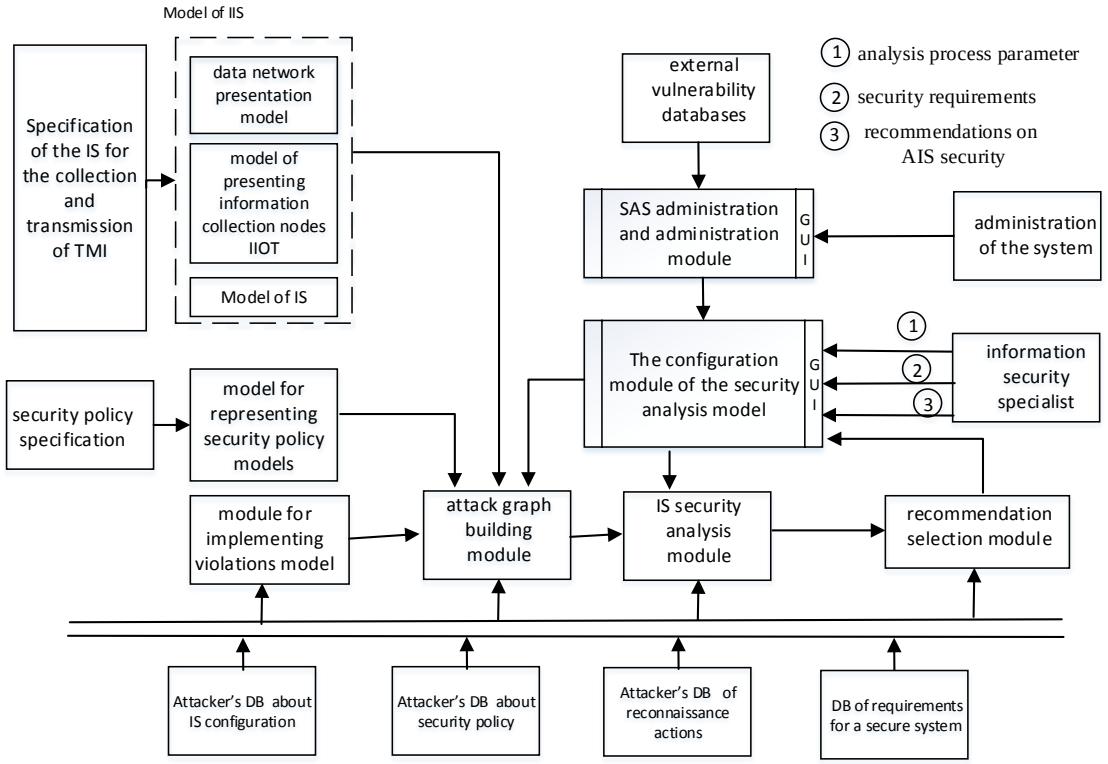



**Figure 4.** Architectures of the TMI transmission security analysis system on the status of individual elements of the aircraft systems.

The module for forming the internal representation of the analyzed network and the security policy converts the data about the analyzed network and the implemented security policy into an internal representation.

The security systems and security policies introduced in the SAS should describe the components of the protected system (network) with the necessary degree of detail - the software used (in the form of software product names and versions) must be specified The data warehouse consists of the following databases and knowledge bases:

(1) knowledge base on the structure and configuration of the TMI transmission network and the implemented security policy;

(2) an attack database;

The knowledge base group consists of four bases:

(1) knowledge base on the configuration of the analyzed system;

(2) knowledge base on the security policy (SP) implemented in the information system;

(3) knowledge base of the intruder about the configuration of the analyzed network;

(4) knowledge base of the offender on the network security policy implemented in the network.

The network configuration database and the security policy database contain information about the architecture and specific parameters of the network and the rules that describe its operation. The action database group consists of the following bases:

(1) DB of actions using vulnerabilities. It is built on the basis of an external database of vulnerabilities.

(2) The intelligence database contains actions aimed at remote retrieval of information about the host or network.

The security requirements database contains predefined sets of values of security metrics, each of which corresponds to the requirements for systems of a certain security class [8].

The database update module and the knowledge base downloads open vulnerability databases [9,10] and updates the database of attacking actions.

The attack graph module simulates possible actions of the intruder in the analyzed network, using information about available actions of various types (attacking, reconnaissance), network onfiguration and the used security policy.

The module for the implementation of the intruder's model provides a definition of the initial position of the offender, the level of knowledge and skills, the primary knowledge of the analyzed computer network. The level of knowledge and skills determines the set of actions used by the offender.

The security analysis module forms a set of composite objects of the attack graph. It also calculates security metrics related to these objects, estimates the overall level of security of the computer network. Algorithms for the intellectual analysis of large volumes of transmitted TMI using Big Data technologies use preprocessing methods with highlighting useful information about the hidden actions of the attacker. The selection in the sequence of values of the observed parameters of TMI, features, repetitive processes, hidden anomalies and patterns in automatic mode underlies the procedure for detecting an attack of an attacker and replenishing the corresponding BR. Technologies of intellectual analysis of large volumes of accumulated data have proved themselves in the tasks of technical diagnostics of complex control objects [11,12] and detection of fraudulent activities in information systems. The results of the analysis are processed in the advisory module based on the application of methods and algorithms for data mining. The analysis results are compared with the requirements determined by the information security specialist, and recommendations are made to improve the overall level of security of computer networks.

Ensuring the reliability of systems for transmitting telemetric information about the state of aircraft using artificial intelligence methods.

Assurance (dependability) allows to solve complex problems of ensuring trouble-free operation, fault tolerance, availability, security, serviceability, observability of the TMI transmission system from the aircraft. The SAS being developed allows one to estimate one of the parameters of the overall integral index of the system's reliability. It is showed in figure 5.

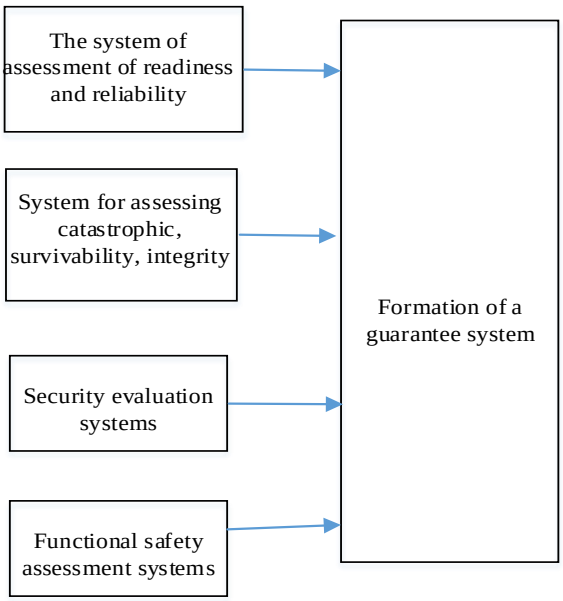



**Figure 5.** Architectures of the TMI transmission security system on the status of the individual elements of the aircraft systems.

Therefore, it is necessary to build a hierarchy of models that allow to comprehensively assess various aspects of the TMI transmission system and develop a methodology for assessing the overall integral index of the system's overall security.

## 3. Conclusion

The structure of an imitation stand for testing a system for transmitting telemetric information about the state of airborne systems to a ground station for processing telemetric information and control is proposed to improve the efficiency of modeling and analysis of system security. A block diagram is proposed for the collection, transmission and reception of telemetric information on the status of individual elements of the aircraft systems of the aircraft. The architecture of the security analysis system of the TMI transmission system on the status of individual elements of the aircraft system is developed. To assess the overall integral index of the system's overall security, it is necessary to build a hierarchy of models that allow for a comprehensive assessment of various aspects of the TMI transmission system and develop a methodology

## 4. References

[1] *Internet of Aircraft Things: An Industry Set To Be Transformed* (Access mode: http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-betransformed) (02.01.2016)
[2] *Aircraft Hacking Practical Aero Series* (Access mode: https://conference.hitb.org/hitbseccon f2013ams/materials/D1T1%20-20Hugo%20Teso%20-20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf) (23.02.2016)
[3] Guzairov M B, Frid A I, Vulfin A M, Berkholts V V, Zakharov D Ju and Mironov K V 2017 The architecture of the web application for protected access to the informational system of processing critically important information *Proceedings of the 17st Computer Science and Information Technologies Conference* **1** 16-19
[4] GOST R ISO / IEC 12207-2010 *Information technology. System and software engineering* (Software life cycle processes)
[5] Palattella M, Accettura N, Vilajosana X, Watteyne T, Grieco L, Boggia G and Dohler M 2013 Standardized Protocol Stack for the Internet of (Important) Things *IEEE Communications Surveys & Tutorials* **15(3)** 1389-1406
[6] *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture* (Access mode: http://ieeexplore.ieee.org/document/6847097) (23.04.2012)
[7] Kotenko I V, Stepashkin M V and Bogdanov V S 2006 Analysis of the security of computer networks on various stages of their life cycle *Priborostroenie* **49(5)** 3-8
[8] The Russia FSTEC order dated March 14 2013 N 31 *On the requirements approval for the information security that is not a state secret contained in government information systems* (Access mode: http://fstec.ru) (14.04.2013)
[9] *NVD. National Vulnerability Database* (Access mode: http://nvd.nist.gov)
[10] *OSVDB* (Access mode: https://blog.osvdb.org/)
[11] Vulfin A M and Frid A I 2011 Neural network model for the analysis of time series process in the methodology Data Mining *Information-Control Systems* **5** 31-38

**Acknowledgments**
This article is supported by RFBR grant № 17-07-00351.