The Structure of Secure System for Collection, Storage and Processing of Telemetric Information on the Slate of Aircraft Subsystems

V.V. Berkholts
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: torina4@yandex.ru

A.M. Vulfin
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vulfin.alexey@gmail.com

M.B. Guzairov
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: guzairov.murat@gmail.com

A.I. Frid
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: frid46@mail.ru

K.V. Mironov
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: mironovconst@gmail.com

Abstract[1]

The problem of aircraft subsystems state identification and data transmition to enterprise-developer is highly actual. Enterprise-developer can give recommendations for quick eliminate defects during aircraft operation and analyze the causes of faults. The intruder can interfere with process of collection, storage and processing of telemetric information. In the paper the structure of secure system for collection, storage and processing of telemetric information on the state of aircraft subsystems is proposed.

1. Introduction (style CSIT-Title2)

The arising malfunctions and pre-failures of the on-board equipment of the aircraft can be diagnosed on the basis of the processed telemetric information (TMI). This allows specialists of ground technical services to plan repair and preventive measures based on an assessment of the current state of the equipment.

Collected and processed TMI will allow Enterprise-manufacturer (EM) experts to provide support to ground services engineers in decision-making in the event of technical failure of the aircraft units and modules.

The ability to transmit information about the actual state of the on-board subsystems in the process of operation to the manufacturing enterprises will make it possible to increase the operational efficiency of the aircraft in the regular mode. As well, it will greatly assist in the investigation of incidents, failures and cyberattacks.

The purpose of the research is to increase the protection of the automatic system for collecting, storing and processing TMI on the state of on-board airborne subsystems. The increase in security is planned through the analysis of the application of modern (including intelligent) technologies for the protection and processing of TMI. It is based on the analysis of modern technologies for the protection and processing of TMI.To achieve this goal, it is necessary to provide a structural diagram of a secure system for the collection, storage and processing of telemetric information on the state of the aircraft subsystems on the basis of the modular principle

2. Analysis of the problem of secure collection, storage and processing of TMI in distributed information system

Automated information system (AIS) of ground maintenance services is a set of software and hardware needed to receive, store and process information about the state of aboard complex technical device (CTD) on board the aircraft. AIS is a territorially distributed system. It combines the infrastructure of information systems of ground-based service stations and the information system of the EM through secure communication channels. The TMI acquisition is realized by reading the CTD status log on board the aircraft during technical inspection and

Proceedings of the 20th international workshop on computer science and information technologies CSIT'2018, Bulgaria, Varna, 2018

maintenance at ground stations using wireless and / or wire sensor networks.

system (SAS) capable of detecting errors in the network configuration, possible routes of cyberattacks of various categories of violators determining critical network resources and ensuring the selection of an adequate security policy.he projected system of TMI collection, storage and processing is a platform for modelling possible actions of violators in the form of attack graphs. Subsequent checking of graph properties and calculation of security metrics forms one of the components of the integral indicator of the system's overall dependability.

3.Development of a structural diagram of a secure system for collecting, storing and processing TMI on the state of the on-board subsystems of an aircraft

The generalized structure of the territorially distributed hierarchical system for the collection, storage and processing of TMI is presented in Figure 1. TMI comes from the sides of aircraft based on ground service stations.

The level of TMI collection by the systems of ground service stations is the realization of the sensor network of the primary TMI collection from the output interfaces of the on-board aircraft systems using wire and wireless sensors.

Preliminary storage of accumulated data at the level of primary accumulation and preparation of TMI for transmission to a part of AIS EM is implemented.

The creation of a secure channel through global communication networks and the transfer of TMI to a part of the AIS EM is realized at the transmission level of accumulated data. Organization levels of reception and distribution of information at the enterprise are realized according to the three-layer CISCO model. [4].

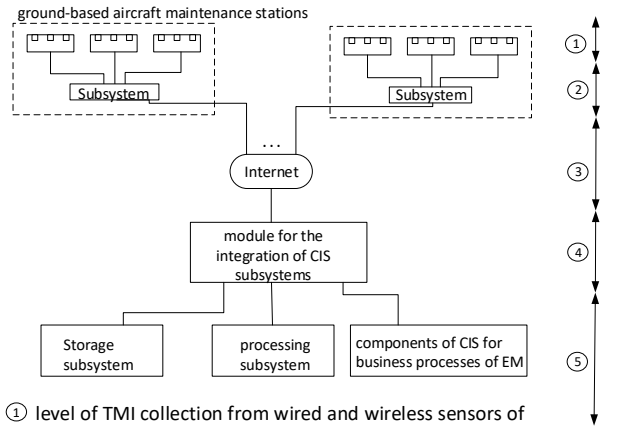
There is a level in the corporate information network of EM. It includes subsystems for storage and processing of TMI. Also, there is a segment designed to support and implement the business processes of the enterprise.

The protected system for collecting, storing and processing TMI on the state of the on-board subsystems of the aircraft is based on the modular principle and contains rather large subsystems with a high degree of connectivity of components inside and a sufficient degree of autonomy at the level of interaction of the subsystems themselves. Each level and subsystems is built on the basis of organizational principles, specific to each task and are regulated by existing documents.

4.Development of the subsystem's structure for TMI collection and storage at ground-based aircraft service stations

In modern practice industrial networks are not isolated they use common information transfer technologies. Most Industrial Ethernet protocols do not have built-in security mechanisms. As a result, any simple cyberattack can lead to negative consequences.

Therefore, the problem of the industrial networks security is actual.



① level of TMI collection from wired and wireless sensors of ground-based aircraft servicing systems
② level of primary surveillance and preparation of TMI for transmission to the AIS of the manufacturer's enterprise (AIS EM)
③ the level of data transmission over secure channels through global data networks in the AISEM
④ level of organization of reception and distribution of TMI on EM
⑤ level of storage and processing of TMI in the CIS

Fig. 1. - Generalized structural diagram of a protected system for collecting, storing and processing TMI

It is necessary to be guided by the normative documents of the international and federal standards to ensure the security of subsystems implementing the first two levels of the proposed structure. It is necessary to take into account the requirements [5, 6] to design the subsystem of the wireless sensor network for collecting TMI.

These documents provide detailed information about the reference system of ensuring information security and contain recommendations for identifying and analyzing network security risks, a review of measures and tools of control. Also, these papers summarize the issues related to the implementation and operation of the measures of network security monitoring and management tools.

It is necessary to implement methods of protection of industrial monitoring systems considered in [7,8,9]. These documents provide a detailed description of the information protection organization to carry out industrial activities using industrial monitoring systems.

The physical architecture of the TMI collection and storage subsystem at the ground-based aircraft maintenance stations is constructed in accordance with [10] and is shown in Fig. 2.

Mechanisms for collecting and storing a large size of TMI about the state of individual units and elements of an aircraft should take into account the actively developing concept of the industrial Internet of things (IIot). IIoT is deployed network consisting of a large number of devices provided with a set of sensors that communicate with

each other by means of thin and short wireless connections. The first step is to collect data from the sensors. One of the most promising solutions is the low-power and low-transmission protocol IEEE 802.15.4 or IEEE 802.15.4e. The IEEE 802.15.4 and IEEE 802.15.4e protocols and their architecture layers are subject to IETF standards [11]. A small effective range is sufficient to transmit data within the ground-based service station.

It is proposed to use heterogeneous wired (physical interface RS-485) and wireless sensor networks (IEEE 802.15.4, IEEE 802.15.4e) for the collection of TMI based on protocols using the built-in mechanisms of Modbus over TCP to protect the transmitted data (stream encryption)

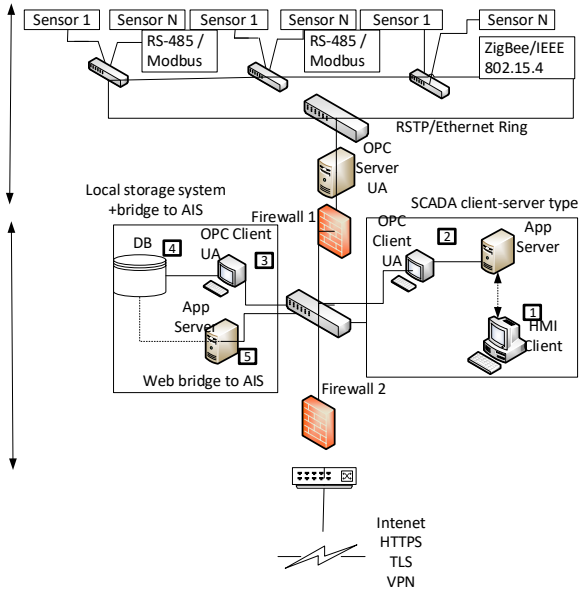


Fig. 2. - The subsystem of data collection and storage at aircraft service stations

The heterogeneous industrial network includes communication lines, switches, interface converters. The least reliable elements of this system are communication lines, so redundancy is necessary.

Reservation methods based on the improved RSTP protocol have too long switchover time [12]. The basis of modern industrial solutions is the use of networks with a ring topology (Ethernet ring) [12].

To organize TMI collection in conditions of the possibility of horizontal scaling and use of heterogeneous network, it is necessary to use an open standards-based OPC (Openness, Productivity and Connectivity) infrastructure. Infrastructure defines a set of programming interfaces for several logical (program) objects as well as the methods (functions) of these objects. It is proposed to use the unified architecture of OPC Unified Architecture (OPC UA) [13].

This architecture is a platform-independent service-oriented architecture that combines all the functionalities that exist in the OPC Classic specification and is compatible with OPC Classic. The choice of this architecture is due to the possibility of efficient transport of high-level structured data and the ability to securely access OPC servers through firewalls. Particular importance is the built-in implementation of TMI protection mechanisms using encryption and authentication mechanisms at the level of interacting devices in the industrial network.

Client-server implementation of the mechanism of access and operational storage of TMI implies the use of dedicated application servers and web clients that allow to administer the subsystem. The Web application deployed on the application server provides secure access to the AIS EM. To build a secure web application you need to use two-way authentication at the web server level. Currently, the most secure two-way authentication technology is authentication using the TLS protocol. Interaction at the web application level allows creating a secure channel for transferring the accumulated telemetry data to the AIS EM for further analysis. In detail these questions were considered in the previous works of the authors [14].

The security of the first two levels of the proposed structure is ensured by the introduction of protective measures and the use of architectural templates conditioned by normative documents of the international and federal standard in the field of information and industrial safety. A distinctive feature is the use of service-oriented architecture and client-server implementation of the mechanism for accessing and storing TMI with the help of a set of web-applications.**F**

5.Development of the subsystem structure for receiving, storing and processing TMI in AIS EM

The organizations of reception and distribution of TMI at the enterprise are realized according to the three-level CISCO [4] model and correspond to core layer level and distribution layer of the network, which are a complex of network devices (routers and switches) providing redundancy of channels and high-speed Data transmission between different segments of the distribution level (Figure 3).

Protection of network infrastructure is an important part of the IS architecture.

The use of the CISCO model in the design of the Security Architecture for Enterprise (SAFE) architecture allows to take into account the modern experience of designing and deploying secure networks based on the defense in depth principle against external and internal attacks [15].

As a part of the corporate information network a level is distinguished that includes subsystems for storing and processing TMI as well as a segment designed to support and implement business processes of the EM (Figure 4).

To ensure storage of TMI and efficient access to accumulated volumes of data it is necessary to build a fault-tolerant storage system using MySQL replication

mechanisms such as Master-Master and Master-Slave with the introduction of a caching proxy server and a separate server that performs cluster monitoring functions.

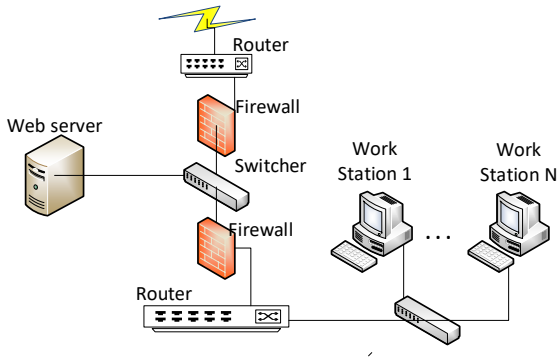


Fig. 3 - Structure of the subsystem for receiving, storing and processing TMI in AIS EM

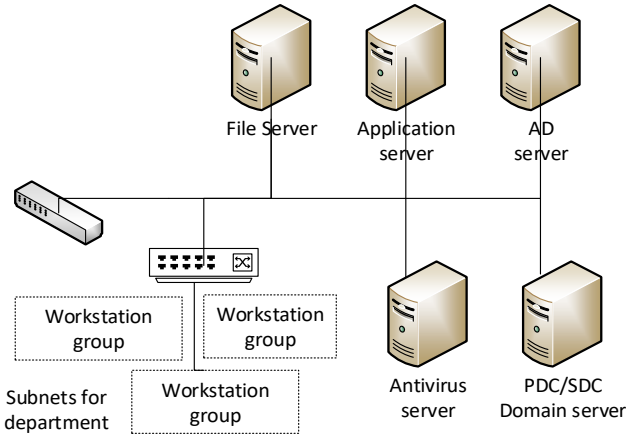


Fig. 4 - Structure of the segment of the corporate information network support and implementation of business processes EM

Such a scheme (Figure 5) allows to distribute the load on the database between several servers, increases the fault tolerance of the system as a whole and provides the deployment of a platform for efficient processing and analysis of accumulated TMI data [16].

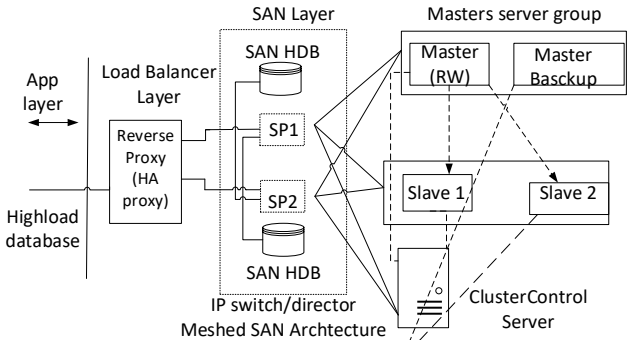


Fig. 5 - Structure of the storage subsystem TMI with fault tolerance functions

Accumulated volumes of TMI are proposed to be located on external storage devices (disk arrays) and to organize a storage area network (SAN) of the "meshed fabric" type. This architecture includes a set of cells where each switch is connected to all the others. If one of the inter-commutator links (ISL) fails the connectivity of the network is not violated. SANs are characterized by the provision of network block devices (via Fiber Channel protocols) [18].

Implementation of TMI processing algorithms requires solving a number of tasks related to the design and deployment of an appropriate infrastructure for the processing of accumulated data. There are many tools for distributed processing of large amounts of accumulated data (frameworks: Hadoop, Apache Spark, ClickHouse, ElasticSearch, Splunk Free) [18, 19, 20, 21, 22]. The proposed structure of the TMI distributed processing subsystem is shown in Figure 6.

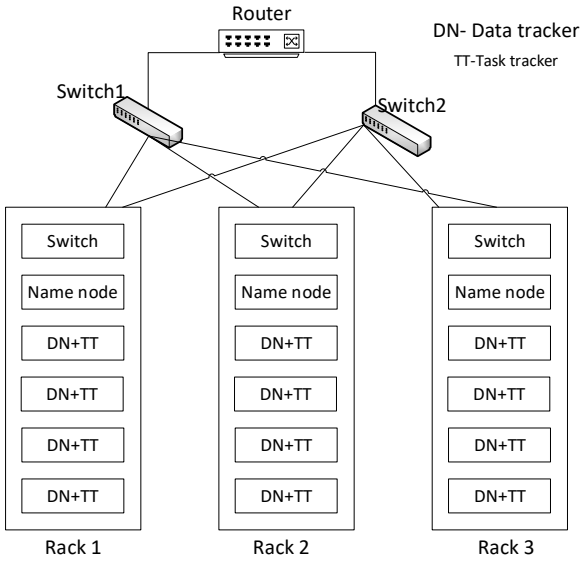


Fig. 6 - Structure of the distributed processing subsystem TMI

The main element of the distributed processing system of TMI is the distributed file system. The most popular is HDFS [18]. Additional measures to ensure the confidentiality of stored data is encryption at the level of individual columns of the database. To audit access to large data you must use the Database Activity Monitoring [DAM] solutions.

The next element of the large data processing system is the distributed programming and machine learning infrastructure. [18]. The structure of this infrastructure includes the machine learning tool MLLib which allows to implement tools for intellectual analysis of accumulated TMI data.

The network infrastructure of the CIS segment and the data distribution segment are designed taking into account the requirements of the enterprise security architecture (SAFE) and allows the implementation of defense in depth from external and internal attacks.

Fault tolerance of the storage subsystem is ensured by using MySQL replication mechanisms such as Master-

Master and Master-Slave. This allows you to additionally solve the task of load balancing on the database. It also provides the ability to deploy a site for efficient implementation of processing and analysis of accumulated TMI.

Conclusion

A block diagram of a protected system for the collection, storage and processing of telemetric information on the status of aircraft subsystems based on the modular principle is proposed. A distinctive feature of the proposed solution is that it contains sufficiently large subsystems with a high degree of connectivity of components inside and a sufficient degree of autonomy at the level of interaction of the subsystems themselves. Each subsystem is built on the basis of organizational principles that are specific to the problem being solved and is regulated by existing regulatory documents to ensure certain aspects of the system's dependability.

The TMI collection, storage and processing system is a platform for modeling possible actions of violators in the form of attack graphs with subsequent verification of graph properties and calculation of security metrics. This approach allows us to solve complex problems of ensuring trouble-free operation, fault tolerance, availability, security, serviceability, observability of the TMI transmission system from the aircraft.

The security of the subsystems of the first two levels is realized by the introduction of protective measures and the use of architectural templates, fixed by normative documents of the international and federal standard in the field of information and industrial safety. A distinctive feature is the use of service-oriented architecture and client-server implementation of the mechanism for accessing and storing TMI with the help of a set of web-applications.

The network infrastructure of the CIS segment and the data distribution segment is designed taking into account the requirements of the enterprise security architecture (SAFE) and allows the implementation of defense in depth from external and internal attacks. Fault tolerance of the storage subsystem is ensured through the use of MySQL replication mechanisms such as Master-Master and Master-Slave which allows additional solve the tasks of load balancing on the database and provides the ability to deploy the site for efficient processing and analysis of accumulated TMI data.

Recommendations for the development of architecture and the selection of solutions at various levels of the proposed secure system for collecting, storing and processing TMI will allow specifying the methodology for constructing protected systems of this type.

Acknowledgments

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

References (style CSIT-Title2)

1. Frid A.I., VulfinA.M., Zakharov D. Ju, Berkholts V.V., Mironov K.V.Architecture of the security access system for information on the state ofautomatic control systems of aircraft // Proceedings of the 19thInternational Workshop on Computer Science and Information Technologies (CSIT'2017), Germany, Baden-Baden, October 8-10,2017, T.№2, P. 21-27
2. Frid A.I., VulfinA.M., Zakharov D. Ju, Berkholts V.V., Mironov K.V. Architecture of the security access system for information on the state of automatic control // Proceedings of the 19thInternational Workshop on Computer Science and Information Technologies (CSIT'2017), Germany, Baden-Baden, October 8-10,2017, T. №1, P. 16-19
3. Frid A.I., VulfinA.M., , Berkholts V.V. Analysis of the methods of constructing information attack models for the system of telemetric information transmission, Proceedings of the Information Technology Intelligent Decision Support (ITIDS2018), Russia, Ufa URL: [http://itids.ugatu.su/index.php/itids/itids2018/paper/view/50]
4. Cisco 3 layer Hierarchical Network Model | Core |Distribution | Access URL [http://w7cloud.com/cisco-3-layer-hierarchical-network-model-core-distribution-access/]
5. ISO / IEC 27033-1-2011 "Information technology (IT)" Methods and means of ensuring safety. Network security. Part 1. Overview and concepts "and ISO / IEC 27033-3-2014" Information technology (IT);
6. ISO / IEC 27033-1-2011 "Information technology (IT)" Methods and means of ensuring safety. Network security. Part 3. Reference network scenarios. Threats, design methods and management issues
7. Order FSTEC of Russia of March 14, 2014 No. 31 "On the approval of the requirements for ensuring the protection of information in automated control systems of production and technological processes in critical facilities, potentially hazardous facilities, as well as objects posing an increased risk to life and health of people and environmental protection »
8. Order FSTEC of Russia of 23 March 2017 No. 49 "On Amending the Composition and Content of Organizational and Technical Measures to Ensure the Safety of Personal Data when Processing in Personal Information Systems approved by the Order of the Federal Service for Technical and Export Control of February 18, 2013 No. 21

9. Requirements to ensure the protection of information in automated control systems of production and technological processes in critical facilities, potentially hazardous facilities, as well as objects posing an increased risk to life and health of people and the environment, approved by the order of the Federal Service for Technical and Export Control March 14, 2014 No. 31 »
10. NIST 800-82 and ISA / IEC 6244
11. 802.15.4e-2012: IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LRWPANs) Amendment 1: MAC Sublayer, IEEE Std., Apr. 2012.].
12. Encyclopaedia of ACS TP , Reservation of industrial networks URL [http://www.bookasutp.ru/Chapter8_3.aspx]
13. OPC Unified Architecture URL: [https://opcfoundation.org/about/opc-technologies/opc-ua/]
14. Guzairov M.B., Frid A.I., Vulfin A.M., Berholts V.V. Protected access to the database on the status of automatic control systems (ACS) by aviation GTE via the web application // Information and Security. 2017 Vol. 20 No. 3 (4). P.410-413
15. CISCO URL [http://www.cisco.com/go/ safe]
16. MySQL Repication URL: [https://severalnines.com/resources/tutorials/mysql-replication-high-availability-tutorial]
17. Data Center Storage Evolution URL [https://www.siemon.com/us/white_papers/14-07-29-data-center-storage-evolution.asp]
18. Hadoop Apache URL [http://hadoop.apache.org/]
19. Apache Spakr URL [http://spark.apache.org/]
20. ClickHouse URL [https://clickhouse.yandex/]
21. Elastic URL [https://www.elastic.co/]
22. Splunk Free URL [https://www.splunk.com/en_us/software/features-comparison-chart.html]