Information Security Risks in Civil Aviation Network: Classification, Identification and Preventive Strategies

Lian Ran
Civil Aviation flight University of China, School of Air Crew, 618307, Guanghan, China

Abstract. Information security of civil aviation network is an important issue in national cyberspace security governance. Based on the ISO27001 information security management system, the main contribution of this paper is to build a classification and identification framework to identify key sources and specific factors of information security risks in civil aviation network through generalization and summary approaches. The detected risk sources mainly include management subject, management process, technology, laws and regulations, and infrastructure. In accordance with the attributes of different risk sources, systematic preventive strategies are proposed in this paper to serve as references for preventing and resolving information security risks in civil aviation network.

1 Introduction

As a strategic and proactive industry of great significance for a country, civil aviation is closely related to national security, economic operation, social order and public interests as a key industry under national information security protection. Currently, civil aviation, together with banking, securities, railway, telecommunications, and radio and television, has been incorporated as seven industries whose networks and information systems are subject to national protection due to their close relationship with the national economy and people’s livelihood. With the development and application of emerging network technologies like blockchain, big data, artificial intelligence, and cloud computing, the civil aviation industry in China is increasingly information-based, a process represented by visualization, intelligence, and interactive and sharing development. The application of “smart airports”, “mobile service processing” and “big data analysis” shows the increasing dependence of the civil aviation industry on network information development. However, information security risks in civil aviation network follow under this context. Information security of civil aviation network is becoming a more and more serious issue. Once the civil aviation information system is attacked or encounters malicious interference, risk sources like leakage of important information and information system failure will seriously affect flight safety and passenger information security, and even directly threaten social stability and national security in more serious cases. Therefore, under the complex context where new situations, new technologies, and new social dissemination paths converge, we need to examine the sources of information security risks in civil aviation network and come up with preventive strategies to effectively prevent and deal with possible political, social, and
economic risks and consequences. This meets imminent reality needs and is also a key issue to ensure the sustained safety of civil aviation.

2 Literature review

The general trend towards ubiquitous networking has reached the realm of airplanes, and airplane safety may be heavily dependent on the security of network information. Related researches on the information security of civil aviation networks in foreign academic circles mainly focus on the technical application and evaluation of aviation network information security. Data networks have well-known security vulnerabilities that can be exploited by attackers to corrupt and/or inhibit the transmission of airplane assets, i.e., software and airplane generated data [1]. Many scholars have realized the threat of aviation information security vulnerabilities to aviation security. Thanthry Nagaraja (2004) reviewed the existing aircraft data network standards, security provisioning, and the security threats associated with the aircraft data networks [2]. Krishna Sampigethaya (2008) believed that the use of unregulated information technology and wireless technology creates loopholes that could allow unauthorized access to airborne aeronautical information systems and hinder their operation [3]. In order to deal with the threat of aviation network information security, some scholars have proposed corresponding technical measures. Sampigethaya Krishna (2013) proposed a new framework for cyber physical systems (CPS) in the field of applications and aviation [4]. In addition, some scholars focused their research on aviation cybersecurity risk assessment. Sathish A.P.Kumar (2017) presented a vulnerability assessment framework [5]. Jurgen Ziegler (2016) proposed a model-based approach for aviation cybersecurity risk assessment in support of holistic understanding of threats and risk in complex interconnected systems [6].

Compared with foreign scholars, the researches of Chinese scholars mainly focus on the construction of civil aviation network information security system and technology application. Gang Li (2010) proposed to construct a civil aviation network information security management system from the aspects of concept system, team system, legal system, and responsibility system [7]. Jianzhao Zhang (2019) proposed to use intrusion detection technology, network monitoring technology, file encryption technology, identity authentication technology and other technical means to strengthen the security construction of civil aviation network information systems [8].

Generally speaking, certain theories, opinions and approaches have been proposed on the basis of the existing research findings about the information security of civil aviation network from the academic circle to provide references. However, there are still some shortcomings. The main contribution of this paper is content and perspective innovation, that is, to construct a classification and identification framework for civil aviation network information security risks from a management perspective, and systematically summarize the various sources of risks facing civil aviation network information security management.

3 Classifying and identifying the information security risk sources of civil aviation network—an analysis framework based on ISO27001

This paper attempts to analyze and identify the information security risk sources of civil aviation network caused by human beings based on ISO27001. The ISO27001 information security risk management covers all security related aspects to realize and maintain the confidentiality, integrity and usability of information systems. An ideal security risk standard should be an integrated, consistent, analyzable, practical and cost-benefit balanced
approach. The definition of information security risk management suggests that information security risks involve security policy, standard and consciousness strategies, in addition to security and technical risks [9]. The classification of information security risks has to allow for not only the probability of risks and the possible consequences, but also the interaction between different risks on the basis of individual risks in order to further analyze and evaluate the comprehensive security risks. From the perspective of information security science, this paper classifies such information security risks in civil aviation network as subject risk, management risk, technical risk and legal risk based on the ISO27001 risk classification standard and after systematically allowing for environmental, human resource, management, technical, legal and economic risks (as shown in Fig.1).

3.1 Identifying sources of subject risk

3.1.1 Imperfect management agencies of network information security in civil aviation administration

Management agencies is an important organizational guarantee for the construction of information security system in civil aviation network. Imperfect management agencies can directly restrict effective regulation of information security of civil aviation network, thereby entailing certain security hazards. Firstly, an authoritative and effective management agency is needed. Currently, there is no authoritative functional agency in the field of civil aviation information security to put information security of civil aviation network under unified and effective management. Secondly, the existing information security management agencies perform poorly in coordination. Managing information security of civil aviation network involves communication and coordination between different organizations, including the government, airlines, and network technology companies. However, the existing management agencies of information security of civil aviation network are not able to contact and coordinate various parties, and a multilevel and interdepartmental coordination mechanism has not been established.

3.1.2 Weak awareness towards network information security among civil aviation units

Information security awareness mainly includes dimensions of organization, public, social politics, computer ethics, etc. [10]. Nowadays, there is a sharp contrast between the weak awareness toward network information security among civil aviation units and the wide
application of information and intelligence technologies in civil aviation. This contrast is manifested in the following aspects. Firstly, management departments in the industry are not fully aware of the relationship between network information security and flight safety. Some civil aviation management departments pay more attention to factors directly influencing flight safety, such as crew, aircraft maintenance, and air traffic control. They tend to assume that network information security has no significant effect on flight safety. Secondly, airlines have low awareness toward preemptive prevention against network information security risks. Frequent reports of airline employees disclosing passenger information and of hackers attacking the information systems of airlines point to the fact that airlines do not pay due attention to preemptive prevention against risks and fail to take effective preventive measures against information security risks. Thirdly, airport groups need to further enhance their network information security awareness. With the continuous promotion and deepening of the construction of smart airports, airports become more and more information-oriented. However, their employees, management and technical maintenance personnel need to further enhance their security awareness in order to adapt to the increasing dependence of airports on information technology.

3.2 Identifying sources of management risks

3.2.1 Imperfect management regulations and certification system for information security of civil aviation network

Currently, China has not put in place perfect management practices and certification systems for information security of civil aviation network. On the one hand, the management regulations for information security of civil aviation network in China need to be specific. Early in 2012, the Civil Aviation Administration of China issued the Specification for Civil Aviation Network and Information Security Management. However, security management regulations are simply generalized guidelines in a sense, while what is needed is specific, operable and detailed regulation documents. On the other hand, the certification system for information security management of civil aviation network needs to be improved. At present, the civil aviation field needs an authoritative, unified and internationally recognized certification system for information security of civil aviation network. An incomplete security certification system can further increase the risks of data abuse and privacy disclosure.

3.2.2 Incomplete prevention and control system against network information security risks

The construction of a prevention and control system against information security risks in civil aviation network lags far behind that in finance and telecommunications industries. Out of consideration to their own interests, few information departments at airlines can meet the ISO27001 and NIST standards in information security management. On the one hand, information security risk assessment is mostly done by airlines independently, and the mechanism of engaging third parties such as consulting firms for risk assessment has not be established. On the other hand, civil aviation departments do not share coordination practices and effective processes for coordinated emergency response to information security risks. Considering that information security of civil aviation network is an issue which involves multiple units and departments, once a network system breaks down, huge losses will inevitably result if there is no mechanism for coordination among multiple departments.
3.3 Identifying sources of technical risks

3.3.1 Bugs in the operation of information technology systems in civil aviation network

With the stable computerized development of civil aviation, many vectors of network attack are not protected by the state-of-the-art technologies [11]. Nowadays, most civil aviation enterprises and institutions do not pour sufficient investments in the operation and maintenance of network information technologies; instead, they pay more attention to functions of information systems and ignore the development of information security technologies, which is the cause of many security risks and bugs. These technical security risks and bugs mainly include that: Firstly, vulnerabilities of network hardware equipment (such as security problems of servers and network equipment) can harm the reliability and availability of the network; secondly, vulnerabilities and bugs of operating platforms (such as operating systems, database systems, and general software systems) may constitute system hidden hazards; thirdly, vulnerabilities of application software systems, bugs of application systems, code errors, execution modes of unsafe codes or unsafe designs may entail security risks.

3.3.2 Dependence on outsourcing for network information technologies and lack of independent development

As the trend of intelligent civil aviation gains momentum, the operation and maintenance of network information technologies in civil aviation becomes increasingly difficult. Currently, outsourcing is the prevailing solution for the operation and maintenance of network information technologies in civil aviation, and independent management of technical operation does not exist. For example, many automatic information systems for air traffic control and operation control software of airlines are purchased from foreign producers, because there are no alternative producers of such large advanced software systems in the country and foreign producers have to be engaged to provide maintenance and remote debugging services. At the same time, some high-end information equipment imported by domestic aviation enterprises are not managed by professional maintenance personnel. To a large extent, the operation and maintenance of such equipment is commissioned to producers, and independent authority is lacked.

3.4 Identifying sources of legal risks

3.4.1 Backward legal construction for network information security in the field of civil aviation

Information security is a systematic project. Authoritative industrial laws and regulations are needed to guarantee the information security of various network systems in civil aviation. Currently, the legal construction of regulations on information security in the field of civil aviation is relatively backward. The regulations available now are mostly issued to provide measures and guidelines. These measures and guidelines have not been elevated to the height of legal regulations and are not authoritative and restrictive enough. With the absence of imperative laws and regulations in the industry, enterprises and institutions are at their discretion when it comes to the importance of information security. No due attention is paid to it from the height of the industry.
3.4.2 Poor connection and interaction between domestic regulations and international civil aviation laws

In the field of international civil aviation, as countries will come into frequent cooperation in network information security, cooperation is an irresistible trend. Safeguarding civil aviation is one of the highest priorities for International Civil Aviation Organization, in order to prevent illegal interference in civil aviation. With the deepening of the “Belt and Road Initiative”, civil aviation will be more and more international. To effectively reach international conventions and strengthen legislative cooperation is a major challenge confronting the information security of civil aviation network in China. At present, the regulations on civil aviation information security in China are not connected with international civil aviation regulations well enough. In particular, the formulation of civil aviation network regulations does not extensively draw on and absorb the theories and practical experience of international civil aviation legislation. A multilateral, democratic and transparent network governance system has not been established.

4 Preventive strategies against information security risks in civil aviation network

4.1 Preventive strategies against subject risk: strengthening safety awareness, improving management agencies, and recruiting professionals

Firstly, set up and improve management agencies in charge of information security of civil aviation network. On one hand, information management agencies in civil aviation units at different levels should be further integrated, and a network security and information work leading group should be set up to guide the formation of an authoritative and unified management agency of civil aviation information security to coordinate subordinates in different civil aviation units; on the other hand, the responsibilities and authorities of management agencies in charge of information security in civil aviation enterprises and institutions should be further rationalized. Civil aviation enterprises and institutions should elevate network information security to the height of strategic development, designate technical professionals to be responsible for information security management on a full-time basis, clearly define the basic authorities and work of the professional management personnel, and pay particular attention to the supervisory responsibilities of department heads to practically carry out information security work.

Secondly, speed up the training and team building of management professionals in charge of information security of civil aviation network. It is urgent to train management professionals in charge of information security of civil aviation network among all tasks in the management of information security in civil aviation. On the one hand, the recruitment policy targeted at information security professionals should be reasonably optimized. Supporting policies for the recruitment of network information security professionals should be formulated to further open up “green channels”; on the other hand, the training system of professionals in information security of civil aviation network should be improved. The management of human resources invested in information security work should be strengthened, and high-quality professionals and teams engaged in this field should be trained in terms of performance management, promotion channels, training and development, career planning, and team building.
4.2 Preventive strategies against management risk: developing management plans, improving management systems and strengthening safety supervision

Firstly, improve the management system for information security risks in civil aviation network. Improving the management system that adapts to the rapid information-based development of the civil aviation industry is an important objective of the management work around information security of civil aviation network. One strategy is to refine and specify regulations on information security risk management. The Regulations on Managing Civil Aviation Network and Information Security should be further refined and specified level by level so that the regulations are operable, and the management responsibilities should be specified and implemented. Another strategy is to strengthen and improve the information security certification system. Prestigious information security certification agencies inside and outside the industry should be commissioned to create and improve an information security certification system to prevent computer viruses and intrusion of illegal users. The final strategy is to improve the prevention system for information security risks in civil aviation network. On the one hand, a regular risk evaluation mechanism that involves third-party evaluation agencies should be established. On the other hand, the ability of different units to coordinate with each other in emergency response to information security incidents should be enhanced and an emergency response linkage process should be regulated for long-term response to information security risks.

Secondly, information security risks in civil aviation network should be strictly monitored and controlled. Strict audit on information security of civil aviation network should be practiced. The information security management by civil aviation units should be audited in strict accordance with ISO27001 and NIST standards. Online public opinions and security incidents should be fully monitored in real time. A complete security early warning and emergency response system should be created to ensure safe operation of information system.

4.3 Preventive strategies against technical risk: mending technical bugs and strengthening safety research

Firstly, focus on mending technical bugs in network information technologies. To begin with, bugs in software and hardware technologies should be targets to be mended in daily system maintenance and troubleshooting. Damaged system hardware equipment should be replaced in a timely manner to optimize the operating environment of the systems and ensure normal and sustained operation of hardware equipment in computers. Next, professional technicians should be organized to check the operating platforms one by one, especially to scan core operating systems, database systems, and general software systems to detect vulnerabilities and bugs, and remedial measures should be taken. Last but not least, application software used in information security systems of civil aviation network should be subject to intensified testing and inspections. Vulnerability scanner should be used to test and inspect application software and detect safety bugs by checking their settings and other parameters. Based on the testing results, technical remedies should be taken.

Secondly, research on key technologies applied for information security of civil aviation network should be substantially strengthened. Strengthening research on the independent development of advanced security technologies is the fundamental solution to reduce the dependence on technical outsourcing and reinforce independent technology development power. On the one hand, fundamental research on information technology security should be strengthened. In particular, more cooperation among research institutes inside and outside the industry should be encouraged, and efforts should be made to promote the R&D
of and breakthroughs in key technologies applied for information security of civil aviation network. Civil aviation units should reserve a budget used for information technology development to support forward-looking and innovative research on applied information security technologies. On the other hand, China Civil Aviation Administration should organize and work with multiple parties to lead the formation of a strategic alliance for innovation of civil aviation information security technologies. Aviation organizations, information technology enterprises, institutions of higher education, and research institutes should join hands to found collaborative innovation laboratories dedicated to exploring independent technologies applied for information security of civil aviation.

4.4 Preventive strategies against technical risk: improving safety regulations in the industry and strengthening international cooperation

Firstly, develop and improve industry laws and regulations on network information security. To defend the information security of civil aviation network depends on the fundamental support of complete and targeted laws and regulations. At present, there is an urgent need for Regulations on Managing Information Security of Civil Aviation Network (hereinafter referred to as “the Regulations”) in the field of aviation. The formulation of the Regulations should be based on and refer to the Cyber Security Law of the People’s Republic of China. The cyber security law at the national macro level should be used to guide regulations that are developed to solve network security issues in civil aviation. In this way, national regulations and industry regulations can be positively connected and interacted.

Secondly, draw on and refer to international conventions extensively and strengthen cooperation in information security legislation. Convention on International Civil Aviation (Chicago Convention) clearly states that each Contracting State develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation [12]. Legislation concerning information security of civil aviation network should extensively refer to the Convention on International Civil Aviation and standard laws and regulations in other countries. On one hand, it is essential to absorb useful theories and practical experience from foreign countries. To formulate industry regulations, different departments should identify problems from reflection and apply internationally applicable regulations to the formulation process. On the other, all stakeholders should strengthen legislative cooperation, boost effective communication with the International Air Transport Association, enhance connection and interaction between industry regulations with international benchmarks and interaction in the legislative process, and jointly promote the construction of an international governance system for information security of civil aviation network.

This article was funded by the following research funds:
1. The 2019 annual scientific research project of Civil Aviation Flight University of China: Research on Civil Aviation Safety Quality Management System(Project Number: J2019-035).
2. Research Project of Cabin Safety Management Institute of Civil Aviation Flight University of China(Project Number:2019-31)

References

1. R. Robinson. et al. Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety. Computer Safety, Reliability, and Security, 26th International Conference (2007).
2. N. Thanthry & R. Pendse. Aviation data networks: security issues and network architecture. *IEEE Aerospace and Electronic Systems Magazine* **20**, 6 (2005).

3. K. Sampigethaya, R. Poovendran & L. Bushnell. Secure operation, control, and maintenance of future e-enabled airplanes. *Proceedings of the IEEE* **96**, 12 (2008).

4. K. Sampigethaya & R. Poovendran. Aviation cyber-physical systems: foundations for future aircraft and air transport. *Proceedings of the IEEE* **101**, 8 (2013).

5. S.A.P. Kumar & B. Xu. Vulnerability Assessment for Security in Aviation Cyber-Physical Systems. *IEEE International Conference on Cyber Security & Cloud Computing* (2017).

6. J. Ziegler, T. Kiesling, J. Niederl & M. Krempel. A Model-Based Approach for Aviation Cyber Security Risk Assessment. *International Conference on Availability. IEEE* (2016).

7. G. Li. Strong engine of "continuous security": building a solid defense line of civil aviation information security (in Chinese). China Information Security, 5 (2010).

8. J.Z. Zhang. Analysis of Civil Aviation Network Information Security and Its Protection Strategy (in Chinese). Digital Communication World, 4 (2019).

9. K.J. Farna, S.K. Lina, R.W. Funga. A study on information security management system evaluation-assets, threat and vulnerability. Computer Standards & Interfaces **26**, 6 (2004).

10. M. Siponen. Five dimensions of information security awareness. Computers and Society. **31**, 2 (2001).

11. M. Wolf, M. Minzlaff, M. Moser. Information Technology Security Threats to Modern e-Enabled Aircraft: A Cautionary Note. *Journal of Aerospace Information Systems* **11**, 7 (2014).

12. R. Abeyratne. Cyber terrorism and aviation-national and international responses. *Journal of Transportation Security* **4**, 4 (2011).