electronics

MDPI

Article

Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management

Xin Lu *, Ruochen Dong, Qing Wang and Lizhe Zhang

School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China
* Correspondence: 2018071030@cauc.edu.cn

Abstract: With the continuous expansion of air traffic flow, the increasingly serious aviation network security threats have a significant and far-reaching impact on the safe operation of the aviation industry. The networked air traffic management (ATM) system is an integrated space–air–ground network integrating communication, network, satellite, and data chain technology, which adopts a network-centric structure to provide network-enabled services and applications for the air transportation system. In view of the serious network threats faced by networked ATM, this paper studies the basic theories and key technologies of ATM information security assurance and designs a credible security architecture to provide comprehensive and systematic security assurance for networked ATM. Starting from the problems and development trend of ATM security assurance, this paper investigates the dynamic and complex data processing process of ATM system, analyzes the complex interaction between its cyber and physical system, and then constructs the networked ATM cyber–physical fusion system model and threat model. Furthermore, the causal relationship between ATM security threat alert information is mapped into a Bayesian network, and the game model of networked ATM is proposed using Bayesian Nash equilibrium strategy. At last, the information security assurance architecture of networked ATM system based on blockchain technology is formed by establishing a distributed co-trust mechanism and multi-chain storage structure. We expect this paper to bring some inspiration to the related research in academia and aviation so as to provide useful reference for the construction of ATM safety and security system and the development of technology.

Keywords: air traffic management (ATM); cyber–physical system (CPS); blockchain; cyber security; information security assurance

Citation: Lu, X.; Dong, R.; Wang, Q.; Zhang, L. Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management. *Electronics* **2023**, *12*, 1665. https://doi.org/10.3390/electronics12071665

Academic Editor: Andrei Kelarev

Received: 4 March 2023
Revised: 26 March 2023
Accepted: 29 March 2023
Published: 31 March 2023

1. Introduction

The Global Air Navigation Plan (GANP) [1] developed by the International Civil Aviation Organization (ICAO) specifies that the future development trend of air traffic management (ATM) system is a network-centric intelligent sensor network that provides network-enabled services and applications to form a networked ATM system, as shown in Figure 1. It integrates cyberspace (airborne communication/navigation satellite networks, airborne self-organizing networks, and ground-based system wide information management) with the physical environment (airlines, airports, and ATM operation centers/departments) through communication, network, satellite, and data link technologies to form a multi-dimensional and complex intelligent system, a cyber-physical system (CPS) [2].

As early as 1996, the ICAO Working Committee on Aeronautical Telecommunications Network (ATN) clearly stated that "ATM messages transmitted over the data chain are at risk of Modification, Replay and Masquerade attacks", and emphasized that "All aviation communication, navigation and surveillance network/air traffic management (CNS/ATM) applications are vulnerable to Distributed Denial of Service (DDoS) attack". Therefore, the networked ATM is bound to face serious information security threats, and the security

situation is not optimistic. With the development of networked ATM, the number of intrusions and attacks that take advantage of the vulnerabilities and security risks of networked ATM is increasing year by year. Experts from European Organization for the Safety of Air Navigation (EuroControl) and the European Aviation Safety Agency (EASA) say aviation security is facing unprecedented challenges. Statistics show that in the first quarter of 2019 alone, aviation networks were hacked as many as 30 times, and each attack on aviation networks caused an average economic loss of approximately USD 1 million [3]. In addition, the statistics for 2020 show that the number of hacking attacks against civil aviation systems (including airlines, airports, ticket sales, etc.) reached a staggering 1000 worldwide. After 9/11, Ron Dick, then director of the National Infrastructure Protection Center, said that "if the terrorists of 9/11 had combined a physical attack (crashing planes into buildings) with a cyber-attack (hijacking U.S. ATM), the result would have been a much worse disaster than 9/11" [4]. Therefore, information security for networked ATM is critical and significant in terms of ensuring national security and preventing air transportation security incidents, as well as in reducing the social impact of security incidents and property damage.

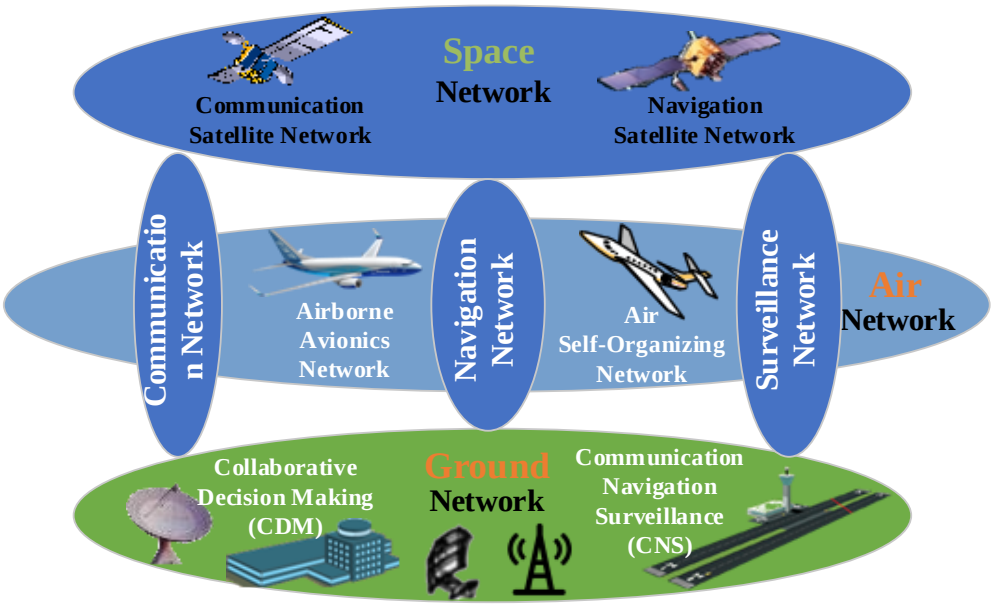

Figure 1. Networked ATM system with space–air–ground structure.

2. Related Work

While focusing on the construction of the future air transportation system, the international community attaches great importance to the research and construction of civil aviation information security assurance. The Civil Aviation Cyberspace Security Strategy [3], developed by ICAO in October 2019, sets development goals for the construction of networked ATM information security assurance.

2.1. Aviation Industry

On 20 February 2019, the United States released the latest version of the National Strategy for Aviation Security [5], focusing on new security threats posed by emerging disruptive technologies and developing strategic action and support plans. The Federal Aviation Administration (FAA) has developed a rigorous Information System Security (ISS) program since 1999 [6] to build the U.S. ATM information security assurance system. The ISS structural model has a five-layer structure and two supporting functions across the five layers that form a trusted system to assure the U.S. ATM system with regard to policy, management, technology, and engineering.

The U.K. Civil Aviation Authority developed the Aviation Cyber Security Strategy [7] in order to secure the U.K. air transport system. It designed an information security assur-

ance framework with resilient mechanisms to defend against deliberate cyber intrusions and attacks in response to cyber security incidents.

For the development of the next generation ATM, the FAA and National Aeronautics and Space Administration (NASA) developed the Next Generation Air Transportation System (NextGen) and the Aeronautics Strategic Implementation Plan (ASIP), respectively. Europe developed the Single European Sky ATM Research (SESAR). Japan developed the Collaborative Actions for Renovation of Air Traffic Systems (CARATS). China proposed the Civil Aviation ATM Moderation Strategy (CAAMS) construction program, which is "centered on flight operations, with collaborative decision-making as a means and supported by new technologies".

Around the development of next-generation air transportation systems, the U.S. and EU countries proposed information and cyber security research programs for the development of networked ATM, providing theoretical bases and technical support for information security assurance of networked ATM.

- The Air Traffic Control Cyber Security Project (ACSP) [8], an air traffic control (ATC) information security project led by the U.S. Cyber Security Forum Initiative (CSFI) organization, aims to uncover and identify cyber security vulnerabilities in ATC system and airborne system in the NextGen project, which is currently being upgraded and promoted, and to minimize the risk of such vulnerabilities. They conducted penetration tests for scenarios in which attackers exploit ATC system vulnerabilities with a collaborative approach to launch cyber attacks on U.S. airports.
- The Global ATM Security Management (GAMMA) project in Europe [9] conducted a systematic study of cybersecurity management issues in SESAR program. The project, funded by the European Union's Seventh Framework Program project, conducts a comprehensive assessment of possible serious security threats and vulnerabilities in ATM, and studies effective solutions to improve the security performance of the system.
- The German project Air Traffic Resilience (ARIEL) [10], based on the research results of the European SESAR project, provides an overall risk assessment of potential cyber attack threats to the critical infrastructure of the aviation system. At the same time, with the help of air traffic simulators, a scenario-oriented approach is used to analyze the risk of different cyber attack scenarios and ultimately achieve the goal of improving flight safety.

2.2. Academic Community

The U.S. Government Accountability Office (GAO) concluded that the U.S. ATM system has significant security control vulnerabilities that threaten the safe and uninterrupted operation of the National Airspace System (NAS) [11]. The GAO recommended measures such as system boundary protection, encryption of sensitive data, and implementation of access controls to reduce security risks due to security flaws and system vulnerabilities.

Boeing presented its views on a framework towards improving ATM critical infrastructure cybersecurity for the future of networked ATM [12]. Boeing believes that various U.S. aviation companies and departments should collaborate to share cyber threat information and best practices to develop and deploy a more secure information infrastructure. Furthermore, it can prevent, detect, and defend cyber attacks, and recover quickly from disasters caused by attacks.

Professor Timothy B. Holt et al. [13] from Embry-Riddle Aeronautical University studied the High-Level Safety Risk Assessment (HSRA) methodology for the NextGen program. Their study showed that there is a high security risk in data exchange due to the lack of strong information security measures in the ground–air data link system and aircraft access System-Wide Information Management (SWIM).

A study by Bart Elias [14], a U.S. aviation strategist, showed not only the security risks of airborne networks but also the access and frequent data exchange between airborne networks and the separate resource system devices in ATM, creating inherent security vulnerabilities in ATM. He emphasized that the increasingly tight interconnectivity between air vehicles

and ATM makes them vulnerable to unauthorized remote access attacks. He concluded with recommendations for protecting civil aviation networks against cyber attacks.

Tim H. Stelkens-Kobsch [15] from the Flight Instruction Institute of the German Aerospace Center considered the ATM as a whole and divided the CNS and automation systems into separate subsystems for security assessment. He described a possible methodology for security prototype validation and aimed to enhance the security of ATC voice communication system by adapting to security prototypes. In addition, Meilin Schaper and Tim H. Stelkens-Kobsch [16] from this institution evaluated several new systems involving several security prototypes developed in the European Aviation Security Research Program. The specific validation efforts of the selected methods were detailed for complex ATM with wide area distribution. Their research was funded by the EU Seventh Framework FP7 program project.

Lanka Bogoda et al. [17] from RMIT University studied the security risks faced by aviation assets and analyzed the security vulnerabilities in the aviation system. Aimed at six key aviation systems, such as CNS/ATM system, avionics system and airport management system, they used analytic hierarchy process and fuzzy logic system to analyze the impact of eight important attack types on the system and assess the system security risk. By improving the consistency and accuracy of risk attributes, the risks faced by the system can be better managed.

K. Sampigethaya from Boeing and R. Poovendran from University of Washington [2,18,19] proposed a novel CPS framework for aviation systems applicable to aircraft, aviation users, airports, and ATM and analyzed its challenges and solutions. Their research showed that data communications and networks that guarantee the safe flight of air vehicles were key enablers for civil air transportation systems to meet the aviation needs in the next 20 years and beyond, and they analyzed the security threats and challenges faced by aviation communication networks and the open problems in security authentication in aviation communication networks.

Professor Sathish A.P Kumar et al. [20] from Coastal Carolina University proposed a framework for vulnerability assessment of aviation CPS, which was used to assess and prevent security threats and vulnerabilities in the computer system and network of aviation CPS. They used vulnerability analysis and penetration testing tools to test and evaluate the vulnerabilities of aviation systems, including data loaders, and to develop corresponding solutions to improve the information security of aircraft.

Xenofon Koutsoukos et al. [21] from Vanderbilt University considered security and resilience as system properties and proposed an integrated platform for modeling and simulation of CPS for evaluating system security and resilience using intelligent transportation system as an application domain.

Professor Malan [22] from Civil Aviation University of China studied ATM information security assurance method based on System Security Engineering (SSE) theory during her Ph.D. study at Tianjin University. She applied the theory of SSE to the information security assurance and evaluation of ATM system and combined the idea of Dynamic System Control (DSC) to propose a method for information security assurance of ATM system. As the editor-in-chief, Prof. Malan published the academic monograph "Information Security Assessment for Air Traffic Management" [23] to share her research experience in ATM information security.

In summary, as shown in Figure 2, current relevant research focuses mainly on the security assurance schemes of the ATM system, but there is little research on the model design and security assurance scheme of the ATM-CPS. As a typical CPS, it is necessary to design its system model and ensure the safe operation of the system. At present, international information security assurance schemes for ATM have matured and started to be implemented and applied. The research for ATM-CPS has completed the integration of cyber space and physical space of ATM and designed the interaction between them. However, business interactions among ATM infrastructure layer, communication layer, and decision layer have not been addressed. Moreover, there are no international standards

proposed for ATM-CPS information security research. Due to the great differences in ATM configuration and requirements and the wide variety of configured system network equipment and different standards, it is difficult to directly draw on the experience of existing general information security assurance. Therefore, more adaptable ATM-CPS and its information security assurance solutions need to be researched and developed on the basis of the actual situation and the specific requirements of ATM.

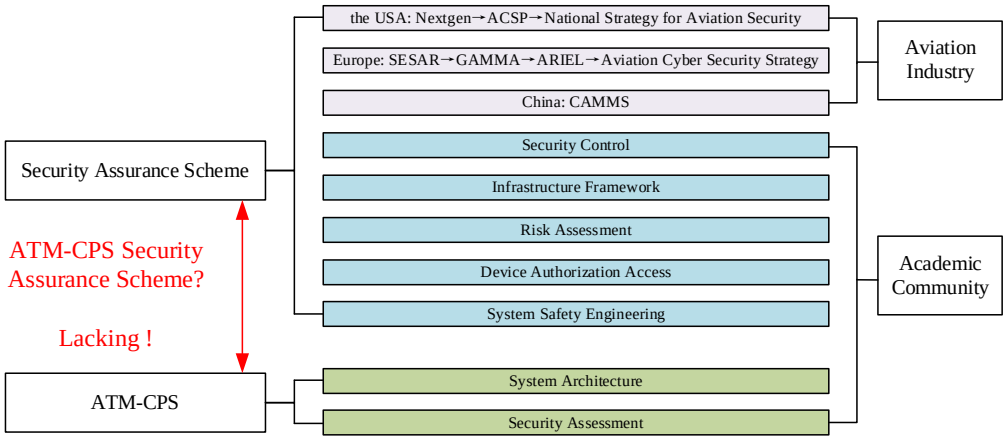

Figure 2. Deficiencies in related work.

2.3. Contribution and Organization

According to the "Civil Aviation Cyberspace Security Strategy" formulated by ICAO and the "Civil Aviation Net-work Information Security Management Regulations (Provisional)" promulgated by the Civil Aviation Administration of the Ministry of Communications of China, the key tasks of this paper are "to strengthen the information integration of civil aviation networks, analyze the security threats, comprehensively grasp the development situation of civil aviation network information security, and build a civil aviation network information security assurance system". This paper formulates four research contents on the basis of the four key tasks, and their relationships are shown in Figure 3.

The Civil Aviation Cyberspace Security Strategy released by ICAO points out that the main threat to networked ATM is the prevention of information spoofing, data injection, entity masquerading, and DDoS attack, which lead to inaccessibility or normal use of ATM services. On the basis of the ATM-CPS model and its game model, this paper uses blockchain technology to establish a trustworthy model of ATM from the key technical dimensions of security protection, security assessment, and situational awareness. The information security assurance architecture of networked ATM based on the trustworthy model is proposed, and a systematic research plan is proposed for the information security problems of networked ATM security.

The thought behind the research in this paper is to perform cyber–physical fusion for space units (communication and navigation satellite networks), air units (air surveillance networks and airborne networks) and ground units (ATC operation centers, data centers, ATM departments, airlines, airports, and ground stations) to form ATM-CPS (Figure 4). Further, for the security threats of ATM-CPS, the information security properties of networked ATM are determined by special analysis based on the SSE theory, the security properties satisfied by ATM are mathematically proved, the potential attacks faced by ATM are mined using the formal verification method, and various optimization objectives and optimization functions are designed to establish the ATM-CPS threat model. Then, using Bayesian game theory, we simulate the attack characteristics of the attack mode in the real ATM-CPS and the defense characteristics of the networked ATM on the basis of the security baseline strategy to form a non-cooperative game with incomplete information and establish the ATM-CPS game model on the basis of Bayesian Nash equilibrium. Finally, blockchain technology is used to establish a trustworthy mechanism for ATM-CPS, and

cryptographic algorithms are used to implement access authentication among data chains and networks, and then an integrated ATM-CPS space–air–ground security assurance architecture is constructed on the basis of the blockchain trustworthy model.

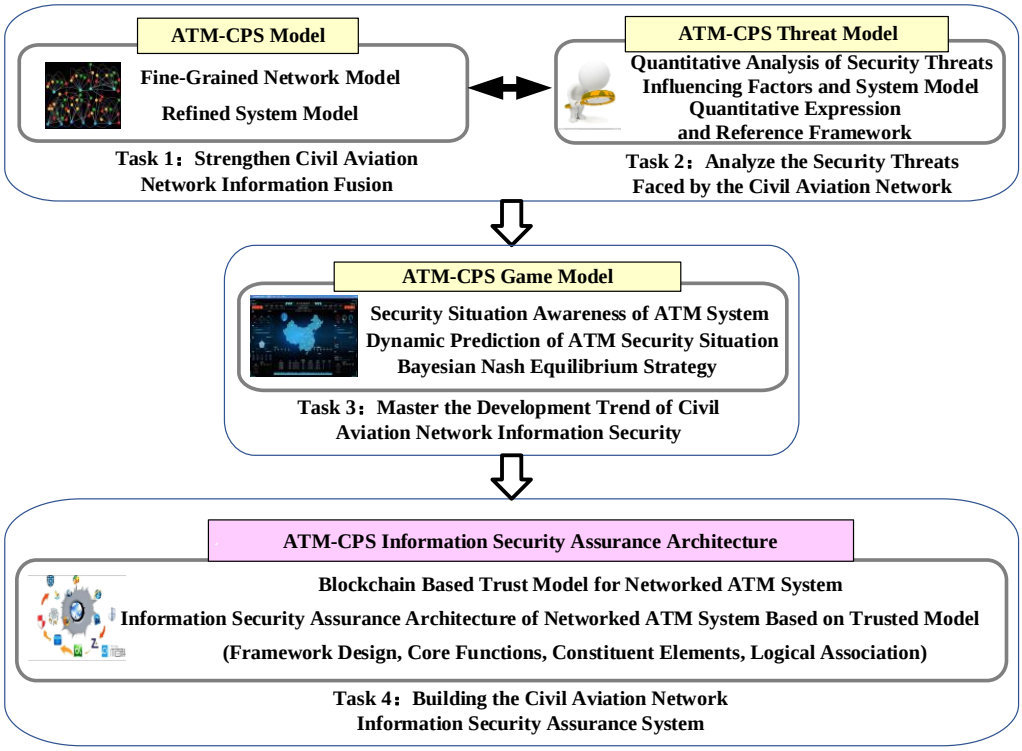

Figure 3. Research contents and the relationships among them.

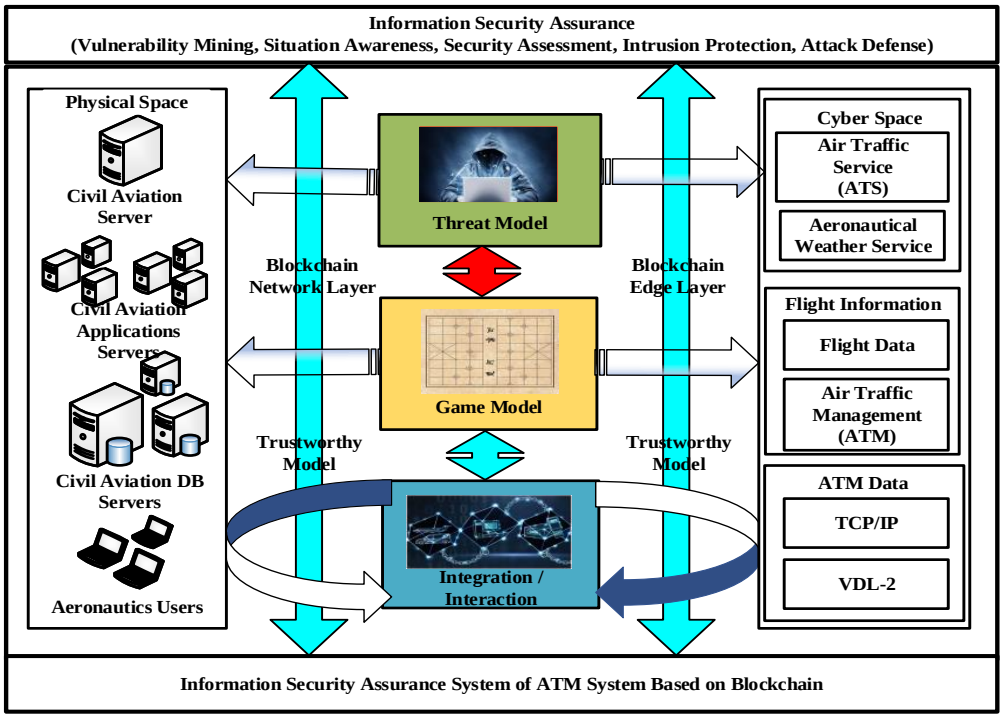

Figure 4. The overall research proposal.

This paper is organized as follows. Section 3 outlines the current issues and trends in ATM security according to the actual needs. Section 4 presents the networked ATM-CPS model and its threat model. Section 5 introduces the networked ATM-CPS game model. Section 6 describes the networked ATM-CPS security assurance architecture. Section 7 provides the scientific problem solved by networked ATM-CPS and the implementation deployment route. Finally, Section 8 draws conclusions.

3. ATM Security Concerns and Trends

The ATM is an important part of the integrated space–air–ground defense system in various countries around the world. With the rapid growth of airspace density and air vehicle types, the degree of informationization, automation, and integration of networked ATM is increasing, and different components are deeply integrated to form a complex CPS [18]. Among them, the cyber system completes the information-based decision support function; the physical system supports the state change of the air vehicle. The middleware for the interaction between the cyber system and the physical system is an important component for data acquisition, control command generation, and command execution of the complex system of ATM-CPS. While the deep integration of multiple components enhances the intelligence of networked ATM, the dimension of attacks on ATM is extended, and, thus, the potential threats to ATM are further exacerbated by cross-domain attacks that penetrate from the cyber domain to the physical domain.

3.1. Security Concerns

At present, the main problems in information security of civil aviation ATM system are as follows.

(a) Simple information security product stacking.

The information security products of ATM are single. The existing ATM information security is still at the stage of simple information security product stacking, i.e., the deployment of firewall and intrusion detection products in the computer network used in ATM. Moreover, no technical measures have been taken for the core system equipment of ATM, and the deployment of network probe equipment has been very rare. Thus, networked ATM lacks systematic protection design and measures.

(b) The scope of information security protection and evaluation is limited.

At present, ATM information security protection covers only the computer networks of ATM departments, airlines, and airports interconnected with ATM, while security protection for core ATM system equipment (e.g., ACARS, ADS-B, radar networks, satellite communications, and navigation networks) is almost blank. The security protection does not even involve the core of ATM automation system, and at most, some simple protection is carried out for the boundary and interface of the automation system (e.g., modem), which cannot form a systematic and effective protection. In addition, most of the assessment of civil aviation information security is limited to the computer networks of airlines and airports, and few information assessment activities are carried out for the core ATM networks and systems.

(c) Lack of systematic security assurance system structure.

There is a lack of research on security assurance framework for large-scale complex networks such as networked ATM. Two key issues need to be explored and solved: first, to build a scalable and robust security assurance system; second, to improve the effectiveness, accuracy, and efficiency of security assurance method.

3.2. The Trends

Networked ATM is a typical large-scale CPS with serious network security threats, and its serious impact on ATM safety has not yet received the attention of management and technical departments at all levels of the ATM field. The analysis of the relationship

between network security and system safety is not deep enough, and the analysis of ATM network security is still scattered and not systematic; in particular, the effective threat model has not been established. The basic theories and key technologies for ATM information security need further in-depth research.

(a) Networked ATM faces the control challenges of proliferation of flight density and diversification of air vehicle types, and its cyber security is under serious threat.

In ATM, the threat to data security of ATM posed by cyber attacks presents a serious challenge to flight safety. Securing ATM data requires effective CPS modeling of ATM based on the networked ATM architecture and information flow analysis and as a basis to study its information security performance. Unlike traditional information systems, the physical and cyber processes of CPS systems are closely coupled with each other, and the existing computing and communication model are quite different from the actual CPS physical process model. The granularity of ATM-CPS modeling in existing research results is relatively coarse, and formal CPS modeling of specific functional subsystems has not yet been performed. In particular, the existing models have not been able to portray the information transmission flow among the nodes of various elements in ATM and to quantify the interaction between the cyber system and the physical system. Research results that abstractly map ATM into CPS and then use CPS security theory to analyze ATM security are not yet available.

(b) With the development of software-defined radio technology and the high versatility of ATM devices, the scope of cyber attacks against ATM is expanding, cyber attack modes are emerging, threat models are evolving, yet a unified and effective cyber threat model has not yet been constructed.

Due to the openness of the networked ATM wireless channel and security flaws in the protocol design, various important parts of ATM are subject to potential attack threats to varying degrees. For example, ATM uses Global Navigation Satellite System (GNSS), either GPS or Beidou, as a data source for aircraft position and velocity status. Since GNSS civil navigation message (CNAV) is susceptible to jamming and attacks [24], it may directly affect the accuracy of airspace posture in ATM. The CNAV messages of GNSS transmit the messages out in the signal format specified by the GNSS protocol standard, which are not encrypted and authenticated, and the access to the wireless channel is not associated with an anti-collision mechanism. The open nature of wireless propagation determines that it is easy for attackers to eavesdrop, modify, inject, and delete GNSS messages [25]. Meantime, GNSS receivers continuously receive location or timing information from outside input, which may contain malicious code carefully constructed by attackers. If there is a remote execution vulnerability in the receiver, an attacker can control the GNSS receiver by wireless injection. For airborne GNSS receivers, an attacker could take control of the airborne receiver by sending erroneous data to the on-board surveillance isolation processor, generating conflicting trajectories that could lead to an incident.

(c) Due to the lack of effective and credible theoretical research results on the intrinsic connection between information security and flight safety, the analysis of the propagation path of the impact of cyber attacks in the ATM is still largely lacking, resulting in a gap in the understanding of the importance of ATM cyber security between the cyber security field and the ATM field.

Although, in several recent hacker conferences (DefCon and Black Hat), technicians in the field of network security have used inexpensive, generic software radio platforms to demonstrate cyber attacks on ATM surveillance systems, clearly believing that cyber security will pose an important threat to flight safety. However, ATM professionals are not fully aware of the changes in the ATM cyber security threat model and the serious threat that cyber security poses to flight safety. ATM professionals have a weak and vague understanding of the "important impact of cyber security on flight safety" and usually believe that the traditional approach based on backup and emergency procedures

is sufficient to ensure flight safety in the event of a cyber attack, thus placing cyber security at a lower priority for development. Therefore, the important impact of cyber security on flight safety in the field of ATM needs to be further explored and studied. The study of the propagation path of cyber attack impact in ATM and the quantitative analysis of the impact of cyber attack on core ATM performance (e.g., the impact on flight interval control and anti-collision algorithm) can complete an effective and credible cyber security assessment of ATM, thus drawing the attention of professionals in ATM field to cyber security and promoting the future development of ATM security.

(d) ATM has special cyber security needs, and it is urgent to build a complete networked ATM cyber security defense solution to ensure the operational efficiency and flight safety of the system.

At present, security solutions for different components of ATM are built separately, lacking effective interaction among them, and security solutions of different component bring fragmentation and incompatibility of system security. Therefore, it is difficult to meet the security needs of networked ATM. By building a complete networked ATM security solution, integrating the security protection of different components, and deploying a defense-in-depth solution, we can realize the basic reinforcement, accurate detection, and fast response capability of ATM security, avoid the spread of damage caused by attacks, and ensure the overall security of ATM.

In summary, the development trend of networked ATM information security is to establish a systematic and deep defense system. Relying only on the engineering security protection mechanism of the physical system and the information security technology of the cyber system, it is difficult to achieve the requirements of comprehensive security of ATM-CPS. In turn, it is necessary to study new ATM-CPS information security solutions from ATM service data fusion, system model fusion and system defense ideas.

4. Networked ATM-CPS Model and Its Threat Model

We perform CPS modeling for ATM, analyze the deep inter-action relationship between ATM cyber domain and physical domain, model the fine-grained network of air traffic network using the relevant theories of graph theory and complex network, and construct a refined system model of networked ATM using CPS theory to provide model support for ATM security analysis, cross-domain security analysis, and security assessment. In addition, networked ATM consists of key resource subsystems with different security requirements, which have complex hinge relationships, potential security hazards, and system vulnerabilities and face diverse security threats.

4.1. Networked ATM-CPS Model

The degree of informationization, automation, and integration of the networked ATM is increasing, and different components are deeply integrated to form a complex CPS. The cyber system completes the information-based decision support function, and the physical system supports the state change of the aircraft. The middleware for the interaction between the cyber system and the physical system constitutes an important component for data collection, control command generation, and command execution of the complex system. As a typical complex CPS, the networked ATM based on CNS/ATM architecture will integrate the sensing system, computing system, communication system, and control system, highly integrate the three functions of control, computing, and communication, deeply couple the physical entity with the cyber domain, and effectively realize information sharing and resource optimization.

To address the information security threats in networked ATM, sensor-spoofing attack models, such as ADS-B false data injection and Beidou civil navigation message spoofing, are used to uncover CPS security vulnerabilities in ATM which may affect flight safety. On the basis of the security threats faced by the networked ATM, a fine-grained system model of the ATM critical infrastructure (communication, navigation, surveillance, and automation systems) is constructed using complex network theory and CPS theory, focusing

on the in-depth analysis of the interaction between the cyber domain and the physical domain to construct a fine-grained CPS model of the networked ATM, as shown in Figure 5. The correlation from the ATM cyberspace (cyber system—SWIM) to the physical space (physical systems—airlines, airports, and aircraft maintenance) and its discrete components (ATM/CNS resource subsystems, e.g., radar, navigation satellites, ground-to-air data chains, and ADS-B) is established in the process of interaction between the aviation operations and maintenance department and between the ATM infrastructure (sensors) and ATM application service delivery departments (actuators). They interact with each other through seamless and frequent interactions between the physical domain (aircraft, airports, and airspace, as well as ground handling, crews, passengers, and flights), between the cyber domain (networks, software, computing, policies and information, and network-enabled services and applications), and between the physical and cyber domains, clearly outlining the physical risks (weather and sunrays, etc.) and cyber risks (system failures and attacks, etc.) facing networked ATM. Define the ATM-CPS as a multivariate group.

$$CPS_{ATM} = \langle S, \sum, T, X, P, F \rangle \tag{1}$$

S represents the set of states in the ATM-CPS for different operational models, e.g., normal, fault, and alarm; $\sum$ represents the set of events, e.g., events caused by various risks in cyberspace and physical space; X refers to parameters and metrics that can be quantified in the ATM-CPS, which is a set of real-valued variables; P is a protection function that is assigned to each transition state and is used to indicate the discrete changes that occur in the ATM state; $T \subseteq S \times \sum \times G \times S$ is a set that characterizes the transition states between ATM states; and F represents the continuous physical operation of the system.

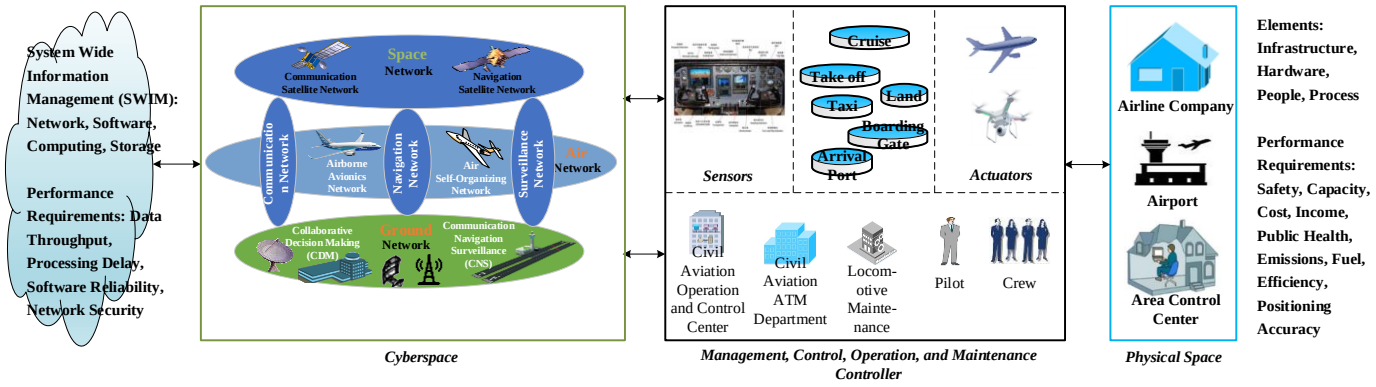

Figure 5. Networked ATM-CPS model.

In the proposed ATM-CPS model, its state evolves continuously under different business models according to the business processes. Therefore, the evolution process of these states is illustrated by the research methods of graph theory and complex network model of ATM system based on matrix operation. Classical network models, such as small-world network model and scale-free network model, cannot fully reflect the characteristics of real networked ATM, and new strategies need to be used for analysis. The adjacency matrix and association matrix reflecting the networked ATM cyber system and the physical system are another form of representation of the complex network; therefore, starting with the analysis of the adjacency matrix or association matrix of the network, the adjacency matrix of ATM graphs and the association matrix of the hypergraphs are represented by graph theory. The complex network is constructed by matrix operation of the adjacency matrix based on graph and hierarchical graph and association matrix of hypergraph and hierarchical hypergraph. At the same time, the degree distribution polynomial is introduced to analyze the degree distribution characteristics and other characteristics of the networked ATM. Specifically, five steps are included.

First, the classical theories, such as graph theory, fractal theory, and stability theory, are used to analyze the ATM network model on the basis of matrix operations. Second, the average path length of the ATM network is measured as a basis for determining the actual ATM reachability. Third, the cluster structure (association structure) of the complex network is used to analyze the robustness of the network when the nodes or edges of the ATM network are subject to accidental and deliberate attacks (fault tolerance). Fourth, on the basis of the flow of the actual ATM service and the characteristics of the network traffic, the meshing number of the complex network is used to determine the distribution state of its service traffic to avoid cascade failure (avalanche phenomenon) in the ATM-CPS. Fifth, the clustering points in the ATM-CPS are identified by combining the efficiency parameters in the complex network. By identifying the agglomeration points, prevention strategies are proposed to ensure the stability and risk resistance of the networked ATM-CPS.

4.2. Networked ATM-CPS Threat Model

Networked ATM consists of key resource subsystems with different security requirements in the space, air, and ground, with complex hinge relationships, potential security hazards, and system vulnerabilities, and diverse security threats (Figure 6). To address the security threats faced by networked ATM, vectors of sensor-spoofing attacks, such as ADS-B false data injection and Beidou civil navigation message spoofing, are constructed to guide the generation of attack data through robustness, coverage, and other metrics and then uncover potential security risks and system vulnerabilities of networked ATM to construct a networked ATM-CPS threat model.

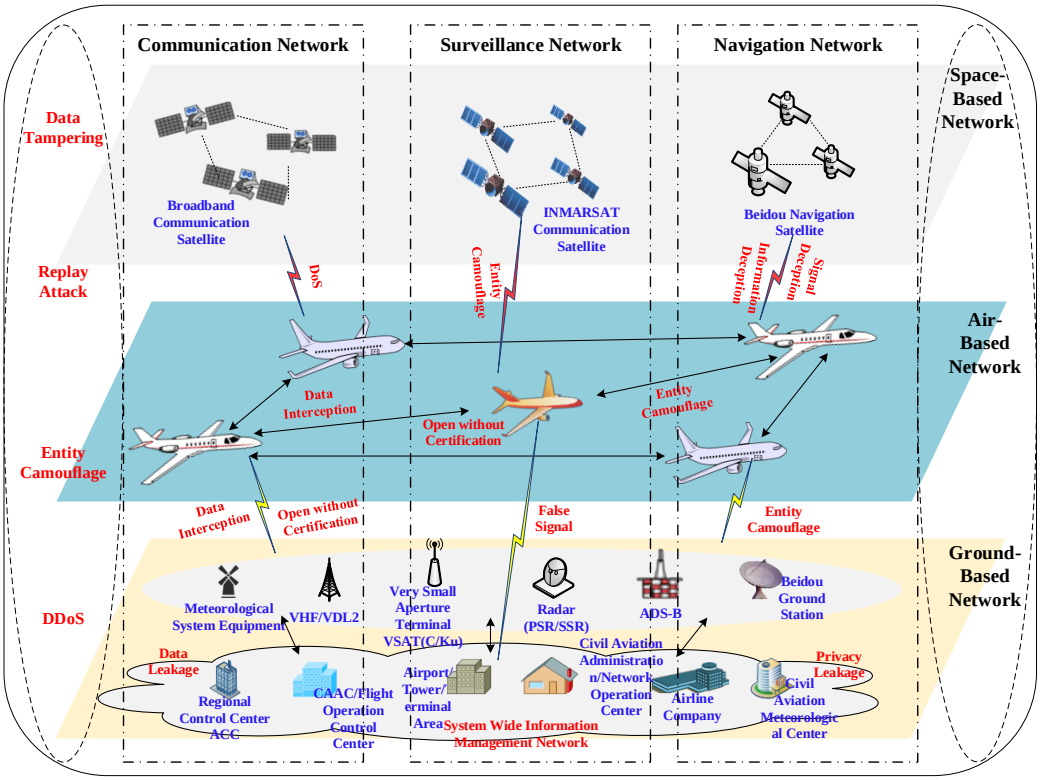

Figure 6. Networked ATM-CPS threat model.

(a) Quantitative analysis of the impact of security threats on the core performance of ATM system.

It is necessary to study the quantitative assessment mechanism of the destructive ability of attack techniques due to ATM-oriented security threats, studying mainly the quantitative analysis of the impact of network attacks on ATM core performance, including the analysis of the concealment mechanism of various attacks, the analysis of the impact on

different security features and service performance, the scalability of attack techniques, the mechanism of chain reaction of security events, and other quantitative assessments.

- Security hazards. There is a need to analyze and study the openness and lack of authentication issues for ADS-B system links, ground and air data link systems, and Beidou civil navigation messages in networked ATM.
- System vulnerabilities. The system vulnerabilities, such as explicit data transmission (without encryption/decryption processing) of networked ground–space data link and VSAT network (C/Ku-band) in ATM, as well as the modem of ATM automation system (especially when its port is open), are to be identified and excavated.
- Security threats. The security threats faced by the networked ATM are dissected individually, such as entity masquerading to generate fake signals in ADS-B systems, data tampering in ACARS systems, location information spoofing in Beidou civil navigation messages, entity masquerading, and DDoS attack.

(b) Establishment of influencing factors and system model of networked ATM system security metrics.

On the basis of the networked ATM-CPS model, we study the propagation paths of typical network attacks in ATM, seek quantitative analysis methods for the impact of network security on ATM core performance, and investigate the correlation between "Security" and "Safety" in ATM to provide a quantitative basis for networked ATM security assessment and threat modelling. It is necessary to research the effectiveness assessment methods of various security mechanisms, system vulnerability evaluation methods, attack threat models, and attack impact calculation methods, as well as the time-varying rules and mutual influence mechanisms of the above factors.

(c) Quantitative reference framework and expression method for studying safety characteristics of ATM.

It is further necessary to research the quantitative reference framework and expression method of networked ATM security characteristics, including the definitions of various security characteristics, constraint relationships, and quantitative expression methods of service impact and performance impact. For the analysis of real attack and defense history events of ATM, as well as for typical application scenarios, the summary of attack technology and defense technology development trend and its impact on the security degree of network system, the reference operation process, and the reference system of indicators for security metrics should be studied.

5. Networked ATM-CPS Game Model

In this section, we introduce the game modeling approach based on Bayesian Nash equilibrium strategy from the game modeling of networked ATM-CPS.

5.1. Game Modeling of Networked ATM-CPS

The establishment of the CPS game model for the networked ATM system is necessary (hereinafter referred to as "the ATM-CPS game model"; note: this model is different from the "networked ATM-CPS model"). The security situation of each resource subsystem in the ATM system is comprehensively evaluated from both attack and defense perspectives, and the development trend of the security situation of the entire networked ATM system is obtained by using the quantitative evaluation method of network security situation. On the basis of the ATM-CPS game model, Bayesian game theory is used to analyze the impact of security threats (such as data tampering and privacy leakage) and attacks (such as ADS-B counterfeit signals and Beidou civil navigation message information deception) on the ATM system, and a Bayesian sequential game model of ATM-CPS is established. According to Bayesian Nash equilibrium security protection strategy, it can comprehensively master and control the security status of ATM-CPS.

(a) ATM-CPS information security situation assessment.

In view of the wide area distribution of location, multi-source heterogeneity of data, multiple communication protocols and inconsistent interface standards of networked ATM system, the main research contents are as follows.

- Design the architecture of security situational awareness system of ATM system based on multi-sensor. For the processing mode of distributed collection and acquisition of ATM business data by ATM system equipment, the resource equipment and system mesh physical structure of ATM system and the hierarchical model of equipment layer, transmission layer, and application layer should be designed.
- Design a solution for eXML format of multi-source heterogeneous security information in ATM. The system structure framework of security situation awareness of the ATM system is divided into information collection layer, element extraction layer, and situation decision-making layer from bottom to top, including three steps: detection data fusion, establishment of threat propagation network (TPN), and evaluation of CPS game model. The CPS game model is used to comprehensively evaluate the security situation of each subsystem of the ATM system from the perspectives of attack and defense, and the development trend of the security situation of the entire networked ATM system is obtained through the quantitative evaluation method of network security situation, thus providing a reference for the security situation prediction of the ATM.

(b) ATM-CPS information security situation prediction.

According to the huge composition and complex hinge relationship of networked ATM system, the deep learning model is used to predict the security situation of networked ATM system. It includes two main contents.

- Security event embedding method. The security events faced and suffered by networked ATM should be sorted out, and the security event embedding method should be investigated to represent them as dense vectors using Neural Tensor Network (NTN) and train them for security events.
- Dynamic prediction model of security situation based on deep convolutional neural network. The deep convolutional neural network should be used to model the impact of security incidents in the networked ATM; thus, a dynamic prediction model of the security situation of the networked ATM based on the deep convolutional neural network is established. Genetic algorithm should be used to optimize the model and realize the nonlinear time series prediction of the security situation of networked ATM.

(c) Bayesian Nash equilibrium security protection strategy for ATM-CPS.

On the basis of the established ATM-CPS model and its threat model, starting from the physical space of the ATM-CPS, it is possible to reduce the damage caused by the cyber space intrusion event of the ATM-CPS due to malicious attacks and protect the safe operation of the physical entities in the CPS system. The security research of ATM-CPS is abstracted as a game process, and the dynamic game model of ATM-CPS is established on the basis of the scenario that the ATM-CPS is attacked by the time sequence of data packets. It includes two main contents.

- A dynamic Bayesian game model is proposed to determine the type of attackers, the equilibrium strategies of both sides of the game are obtained according to the process of repeated game, and the incomplete information game is converted into the complete information game to obtain the Bayesian Nash equilibrium solution.
- The game tree is established through reverse induction, and the attack process facing the ATM-CPS is analyzed to obtain the equilibrium path of the game tree. According to the known attack types faced by the ATM-CPS determined by the threat model and the unknown attack types determined by the Bayesian game strategy, the best protection measures are selected. It provides decision-making for ATM-CPS information security protection, and lays a foundation for building a systematic ATM-CPS information security assurance architecture.

5.2. A Game Modeling Method of Networked ATM-CPS Based on Bayesian Nash Equilibrium Strategy

The information security assurance of ATM-CPS is actually a game between attackers and defenders in cyber space and physical space. When both sides of the game reach the dynamic equilibrium state, the ATM-CPS alternates between the initial normal state and the penetration state, and there is a Bayesian Nash equilibrium with mixed strategies. Therefore, the game modeling of ATM-CPS is to evaluate and predict the security status of ATM-CPS on the basis of security situation awareness and then determine the Bayesian Nash equilibrium strategy and establish the game model according to the evaluation and prediction results.

(a) Security situation assessment method of networked ATM-CPS based on Bayesian game theory.

The quantitative evaluation method based on naive Bayes is adopted to evaluate the security situation of networked ATM-CPS. The naive Bayesian quantitative evaluation method considers the fusion of multiple information sources and multi-level heterogeneous information in the ATM system, which can effectively handle uncertain factors and complete the quantitative evaluation of the security situation of the ATM system. The security situation assessment method of networked ATM based on Bayesian game theory is shown in Figure 7.

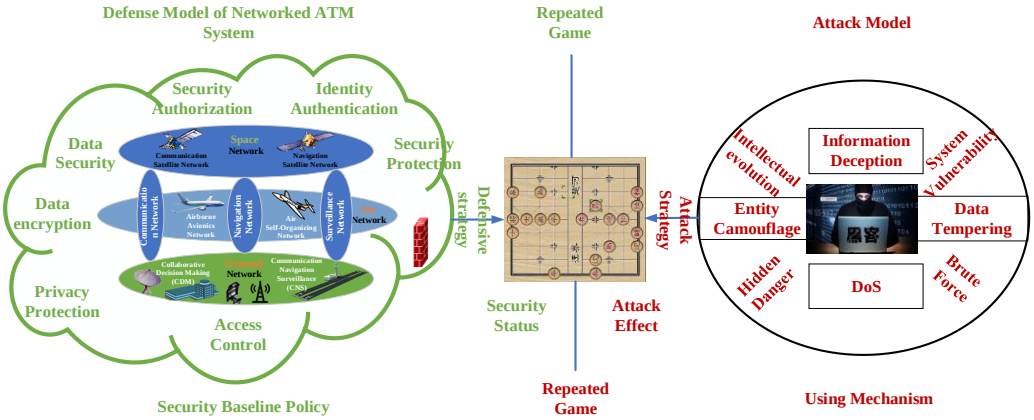

Figure 7. A security situation assessment method for networked ATM system based on Bayesian game theory.

In Figure 7, a networked ATM system defense model based on security baseline strategy and a hacker attack model based on utilization mechanism are established. According to Bayesian rule and game theory, the information security situation prediction method of networked ATM system is proposed. This method maps the causal relationship between alarm information to the Bayesian network in advance, establishes the information security situation prediction model of networked ATM system on the basis of Bayesian game, and then identifies the attacker's invasion or attack intention and predicts the threat degree according to the alarm information. Then, according to the intrusion or attack behavior that has been implemented by the attacker, the probability value on the ATM resource subsystem where the intrusion or attack behavior occurs is continuously revised according to Bayesian law. Finally, based on this probability value, the attack effect and security status of the attacker and the networked ATM information security assurance system are analyzed, and the probability of the attacker choosing the attack mode in the next game stage and the probability of the networked ATM information security assurance system choosing the defense in the next game stage are predicted.

The steps of security situation assessment of networked ATM system based on Bayesian game theory are as follows.

- Using Bayesian game theory to simulate the attack characteristics of the attack modes (deception attack and DDoS attack) in the real networked ATM system and the defense characteristics of networked ATM system based on security baseline strategy, forming a non-cooperative incomplete information game.
- Analyzing the attack behavior of the networked ATM system and using Bayesian law to continuously modify the probability value of the resource subsystem or network containing malicious intrusion tendency in the networked ATM system.
- Predicting the networked ATM system and attackers according to the information they have obtained and quantitatively describing and depicting the change trend of the networked ATM system.
- Predicting the hacker's behavior according to the security status of the current networked ATM system to make a prediction and evaluation of the security situation of the networked ATM system.

(b) Constructing the ATM-CPS game model based on Bayesian Nash equilibrium strategy.

Combined with the networked ATM-CPS model, the security threats (hidden dangers and vulnerabilities) and attack methods facing the ATM system are classified. Using temporal logic and model checking methods, the security threats of networked ATM system are studied at a higher level of abstraction. Further, the security requirements of ATM can be explored and the security requirements modeling method based on CPS features can be studied. Use the CPS system model and security requirements of the previously constructed networked ATM system to match all potential attack modes and establish a dynamic Bayesian ATM-CPS game model on the basis of the ATM-CPS security threat model, as shown in Figure 8.

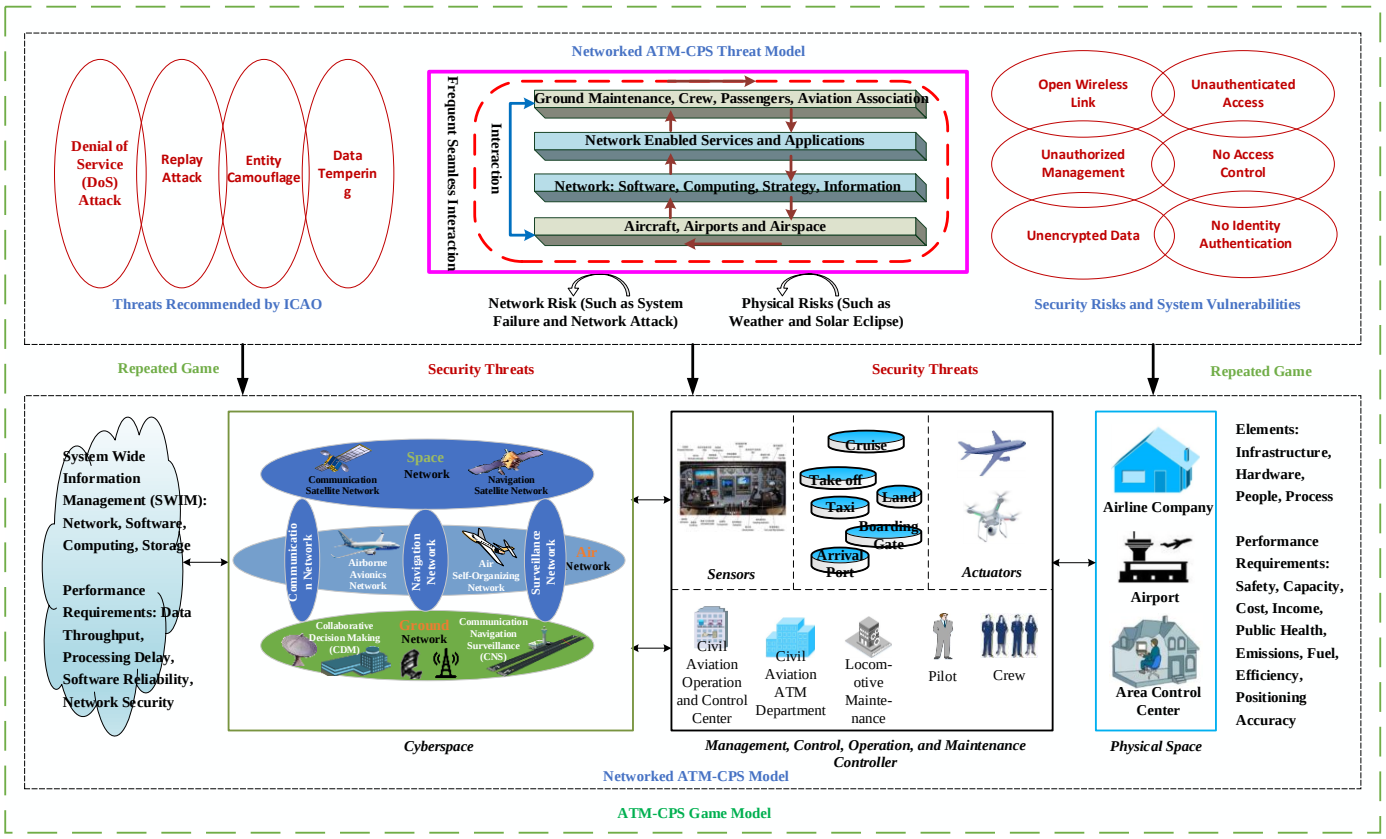

Figure 8. The ATM-CPS game model.

From the perspective of security threats, attacks on the ATM-CPS may have different consequences. For example, the equipment of ATM system is damaged (including overloading of equipment and violation of safety restrictions) or operation loss is caused (i.e., service quality and operation efficiency are reduced). Attackers use the security risks and system vulnerabilities of the ATM-CPS to carry out network hijacking and even some network crimes. Therefore, the security of the ATM-CPS must be evaluated, including the following points.

- Simulate the dynamic behavior of the ATM-CPS under normal conditions and the behavior under network attacks.
- Study the difference parameters based on ATM and attacker. For example, detection frequency, attacker's understanding of the system, physical damage parameters, and attacker's punishment attack detection results may affect the security of CPS.
- Use game theory to study the Bayesian Nash equilibrium strategy of attackers and ATM systems under different interdependence conditions and estimate the attack and detection probability according to special defensive and antagonistic parameters (known and unknown attacks can be detected and identified using intelligent algorithms).
- Evaluate the security indicators of the ATM-CPS on the basis of the threat model (e.g., availability, failure time).

ATM-CPS game model:

$$CPS - G_{ATM} = \langle S, \sum, T, X, G, F, P, A, R \rangle \quad (2)$$

where $S = \{N, P, W, E, NE, S, R, F\}$ is a set of system states. Among them, $\boldsymbol{N}$ is the initial normal state; $\boldsymbol{P}$ is the penetration state; $\boldsymbol{W}$ is the warning state; $\boldsymbol{E}$ is an emergency; $\boldsymbol{NE}$ is a non-emergency state; $\boldsymbol{S}$ is the stop state; $\boldsymbol{R}$ is the recovery state; $\boldsymbol{F}$ is the failure status.

$F = \{F_{ATM}, F_{Attack}\}$ is a set of players, F_{ATM} is the ATM-CPS, and F_{Attack} is the attacker.

$P = \{P_{Attack}, P_{ATM}\}$ is the action set, P_{Attack} represents the attacker, and P_{ATM} represents the ATM-CPS.

$R = \{R_{Attack}, R_{ATM}\}$ is a practical program function. R_{Attack} is used for attackers and R_{ATM} is used for ATM-CPS.

$T \subseteq S \times \sum \times G \times A \times S$ is a finite set of transitions among states, adding actions of both players to the transition function.

According to the current state of the players and the model, the model can be transferred to a new state. Therefore, the ATM-CPS game model is a random mixed model.

6. Networked ATM-CPS Security Assurance Architecture

In this section, we introduce the information security assurance construction method based on the blockchain trustworthy model from the networked ATM information security assurance construction.

6.1. Construction of Networked ATM Information Security Assurance

Based on the fine granularity CPS model of networked ATM, combined with the business characteristics and processes of ATM, the design of point-to-point network for networked ATM application is completed. In addition, blockchain technology is used to implement trustworthy mechanisms and design the information security assurance architecture of networked ATM. The following is the specific research content.

(a) The blockchain-based trust model of networked ATM.

The blockchain network is designed as a trusted management institution (for example, the Civil Aviation Administration or the Civil Aviation ATM Administration), which can provide a trust mechanism which runs a finite state machine model for the processing of the corresponding networked ATM system and makes reliable and credible records of its operating data (record behavior). In this way, we can use blockchain technology to establish

a trusted mechanism to ensure the integrity and authenticity of the cyber system processing process and application of the networked ATM system. It consists of the following steps.

- Digital signature technology and edge protection network are used to design a trust access verification mechanism to enable real-time monitoring of the networked ATM system and promote resource sharing and collaboration among various subsystem entities in the ATM system.
- An anonymous evaluation model based on Bayesian network is proposed to solve the anonymity problem in the ATM blockchain and ensure the authenticity of ATM management institutions and departments, airlines, airports, and other ATM users.
- Based on zero knowledge verification technology, using the account model of ATM system service providers and users and the multi resource model of ATM system, this paper proposes a privacy protection scheme for ATM system service providers and users based on blockchain, as well as a protection scheme for shared data security and sensitive information of ATM system.

(b) The information security assurance architecture of networked ATM system based on trusted model is designed.

The research adopts domestic cryptographic algorithm, designs a trusted ATM information security assurance architecture on the basis of blockchain technology, and specifies the relationship between the elements of the ATM system infrastructure and resource subsystem from the top level. It includes ATM system infrastructure assurance capability system, information security assurance system architecture, technical system, application mode, etc., and develops the framework of ATM system information security standard specification system. It includes the following two aspects.

- Research the blockchain platform of networked ATM system and design the smart contract required for its operation. Among them, the blockchain helps the cooperation between business service providers and users in the ATM system, manages crowd sensing tasks on the basis of smart contracts, and uses distributed algorithms based on smart contracts to achieve trusted services between ATM business service providers and users.
- Research the information security assurance architecture of networked ATM system on the basis of blockchain technology. This includes such key technologies as high fidelity and fast reproduction of ATM business process, replication of ATM user behavior, automatic configuration and fast release of ATM resources, system security isolation and trusted interaction, engine construction for ATM business tasks, and playback of real communication and transmission data flow for each subsystem of ATM system.

6.2. The Method of ATM-CPS Information Security Assurance Based on Blockchain Trusted Model

The equipment and system resources in the networked ATM system are characterized by decentralization (all types of communication, navigation, and surveillance equipment are distributed in different places in a wide area in the form of sensors), and information is directly transmitted and served among CNS equipment (sensor nodes). When the networked ATM system is faced with malicious attack and network deception, it shows a certain vulnerability and must establish a trust model to ensure its security. Blockchain technology can support secure data sharing and privacy protection [26–30]. Zhe et al. [26] put forward the block share system, which can effectively verify any part of the shared data record by introducing a new authentication data structure scheme. At the same time, based on zero-knowledge verification, it supports the privacy protection of users. In addition, blockchain technology increases the timeliness while ensuring the authenticity of stored data, and transaction data need to be verified by most nodes before entering the chain, which provides a unified data source for the trust model. As blockchain technology continues to improve, security, such as session keys and message integrity, continues to improve, and communication and computing costs continue to decrease. Kuljeet Kaur [27] proposed a framework based on software defined network and blockchain for privacy protection of

smart grid cyber–physical system. Aimed at the complex interaction, communication protection, and mutual identification among different subsystems, software-defined network, smart contract, and elliptic curve encryption are combined with blockchain, respectively, to ensure the privacy protection and power safety of smart grid cyber–physical system. Wang et al. [28] used blockchain technology and smart contracts to build a reliable and efficient lightweight certificateless signature scheme, providing protection for the security and privacy transmission of Industrial Internet of Things data. Their solutions not only provide more reliable security for Industrial Internet of Things data but also greatly reduce computing and communication costs. Therefore, this research uses the blockchain technology to build the trust model of the networked ATM system, establish a trusted mechanism among the resources of the networked ATM system, and then realize the information security assurance architecture of the networked ATM system. It regards the blockchain network as a server that provides trust, runs a finite state machine model for the corresponding processing process on it, and records the historical behavior reliably. Digital signature technology and edge computing network are used to design a trust access verification mechanism, which can monitor the networked ATM system in real time and promote resource sharing and collaboration among entities in the system.

The trusted model of information security assurance of networked ATM based on blockchain is shown in Figure 9. The design idea of this model is to jointly participate in and maintain the distributed ledger by Civil Aviation Administration of China (CAAC), CAAC ATM Bureau, ATM departments, airports, and airlines. The trust relationship between nodes is established through peer-to-peer network, password, and distributed consensus mechanism. In Figure 9, the blockchain network layer records mainly the data information related to the ATM system. In the decentralized environment, blockchain technology, as a trust creation machine, ensures its authenticity and reliability by technical advantages of its distributed structure (the ledger in the blockchain is distributed on multiple nodes in the network, each node has a complete ledger, and the transaction bookkeeping is completed by multiple nodes distributed throughout the network), trust mechanism (the blockchain uses the principles of cryptography and authorization technology to establish a consensus mechanism to achieve the openness and transparency of the system so as to establish a good trust relationship between all trading parties in the system), and the tamper-proof time sequence (the consensus mechanism and encryption algorithm ensure that the ledger data cannot be tampered with. At the same time, the timestamp in the chain storage structure ensures the data stored in the block have strong traceability and verifiability). As a trust access mechanism, the blockchain edge layer monitors the ATM in real time. The digital signature algorithm of domestic password SM9 (a Chinese national standard cryptographic algorithm) is adopted to realize the digital signature function. Therefore, all nodes of the blockchain edge layer and the ATM layer need to submit identity tags to the blockchain network layer to generate private keys. Therefore, there is a certain foundation of trust among them.

(a) Blockchain network layer.

The block node is responsible for generating private keys for each node in the edge layer and each node in the ATM system layer. The Key Generation Center (KGC) ring replaces a single KGC in the SM9 standard algorithm. Let the number of nodes in the blockchain network layer be n, and all nodes agree on a random number $ks \in [1, N-1]$ as the signature master private key to calculate the signature master public key $p_{pub-s} = [ks]p_2$. In addition, each member generates a random number $ke_i \in [1, N-1]$ to calculate the element $p_{pub-i} = [ke_i]p_2$ in G2. Then, sum $p_{pub-e} = \left[\sum_{i=1}^{n} ke_i\right] p_2$. Among them, ks, p_{pub-s} and p_{pub-e} are jointly held by the members in the ring, and each member keeps its ke_i secret while disclosing its public key p_{pub-i} to the members in the ring. If a KGC_i in the ring generates a key for node A, its private key is ke_i, the set of public keys in the ring is

$R = \left\{ p_{pub-1}, p_{pub-2}, \cdots, p_{pub-n} \right\}$, and the node A is identified as ID_A. Now, it needs to ring sign the message M and perform the following steps (Algorithm 1).

Algorithm 1: Ring signature is performed on message M.

start
Calculate $g = e\left(p_1, p_{pub-s}\right)$ // in group G_T
Generate $r \in [1, N-1]$
Calculate $w = g^r$
Calculate $h = H_2(M||R||w, N)$
Calculate $t_1 = H_1(ID_A||hid, N) + ks$
Calculate $S = [t_2]p_1$ // $t_2 = (t_1 r)^{-1}(r-h) \cdot ke_i \mathrm{mod} N$
Calculate $l = ks \cdot r \cdot {ke_i}^{-1}$;
$\sigma = (h, R, S, l)$ // the ring signature of message M.
end

Receiver A verifies the received message M' and ring signature (h', R', S', l') as follows (Algorithm 2).

Algorithm 2: Verification.

start
Calculate $g = e\left(p_1, p_{pub-s}\right)$
$t = g^{h'}$
Calculate $p_{3'} = [h_1]p_2 + p_{pub-s}$ //$h_1 = H_1(IDA||hid, N)$
$p_3 = [l]p_{3'}$
Calculate $u = e(S', p_3)$
Calculate $w' = u \cdot t$
Calculate $h_2 = H_2(M'||R'||w', N)$
if $h_2 \neq h'$
Verification failed
else
$d_i = ke_i \cdot {t_1}^{-1} \mathrm{mod} N$ // for each KGC
Sends d_i to node A through a secure channel
Calculates $ds_A = \sum_{i=1}^{n} \left[d_j\right] p_1$ // as the signature private key.
end

In the identity-based cryptographic algorithm SM9, a single KGC generates a user signature key through the master private key and user identity, which has the problem of key escrow. However, by introducing the certificateless digital signature system, multiple KGCs can generate part of the user's private key in the form of ring signature, which not only solves the problem of key escrow but also reduces the pressure of a single KGC.

(b) Blockchain edge layer.

Blockchain edge layer is responsible for collecting data information of ATM system and submitting it to blockchain network layer. By using digital signature technology, the obtained information is written into a new block to complete the successful chaining of information. The specific access process is shown in Figure 10.

According to the process shown in Figure 10, the specific steps are as follows.

Step 1: ATM system node B reports information to edge node A, uses its own private key to sign the collected information, and uses the public key of edge node A to encrypt the information;

Step 2: After receiving the information, edge node A will decrypt and verify the signature. After the information is approved, edge node A will sign all the obtained information and submit it to the block node/KGC_i;

Step 3: Block node/KGC_i writes the information submitted by edge node A into the new block and broadcasts the information after it is signed with the ring private key ks;

Step 4: Other nodes verify the new block and send confirmation information to the block node/KGC_i if the block is accepted. When all nodes are confirmed, the block node/KGC_i encapsulates the new block into the historical blockchain.

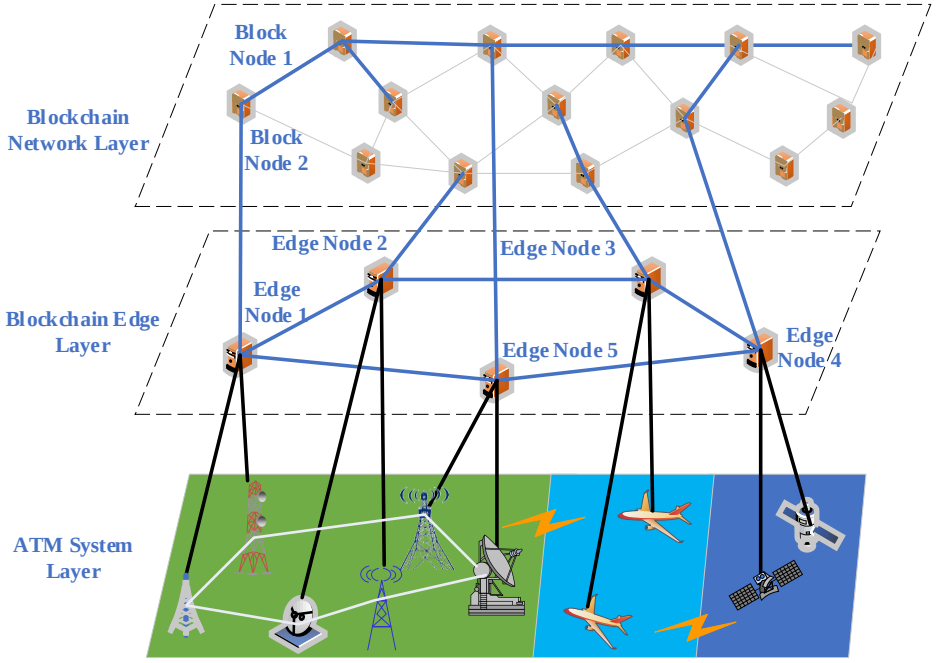

Figure 9. Blockchain-based trustworthy model for information security assurance of networked ATM system.

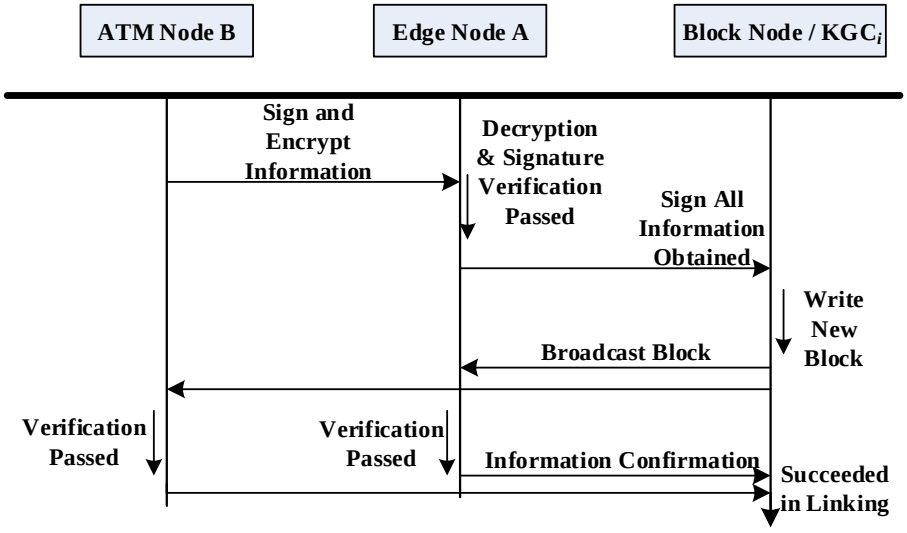

Figure 10. Block into blockchain process.

(c) ATM system layer.

Entities that provide their own data information use blockchain technology to achieve the sharing and collaboration of overall resources. Whenever a new node joins the ATM system layer, it needs to submit its own identity to the blockchain network layer so as to obtain part of the private key and calculate it locally, and then it generates the signature private key. Because the ATM network layer uses the form of ring signature to generate the private key, it can also verify the signature without knowing the specific situation of the signer, which also ensures the anonymity of the network layer nodes.

On the basis of the trustable model established by the blockchain, this paper proposes a networked ATM-CPS information security assurance architecture based on the trustable model, as shown in Figure 11. The networked ATM-CPS has many cooperative subject resources, wide information sources, large data volume, and long business chain, realizing cross regional, multi-agent, and full process space–air–ground integration and multi-dimensional sharing and cooperation. Therefore, taking advantage of the characteristics of the distributed data records of the blockchain, such as certificate storage, traceability, sharing, trust, and cooperation and combining them with the basic theory and key technology of information security assurance oriented to the networked ATM system, a systematic space–air–ground integration and all-round networked ATM system information security assurance architecture is formed. This structure supports and accommodates the information security assurance technologies of ATM system, such as vulnerability mining, intrusion prevention, situation awareness, and attack defense.

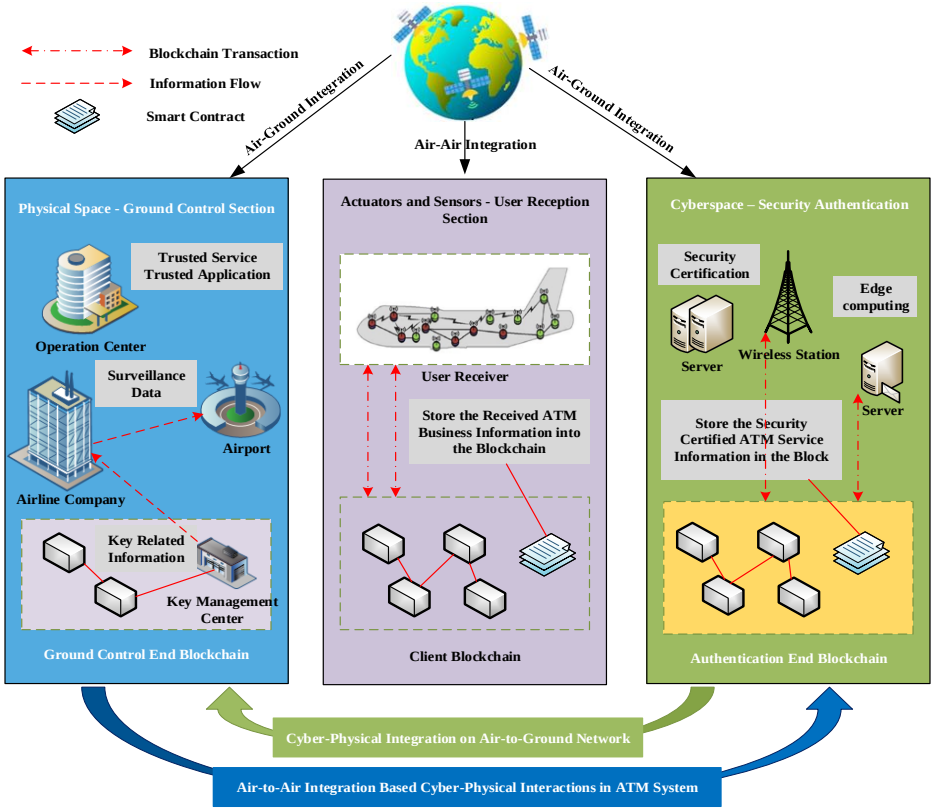

Figure 11. Information security assurance architecture of networked ATM system based on trustworthy model.

(d) The example scenario.

Suppose there is a flight Flight(X) from Beijing to Shanghai, which needs to pass through Tianjin, Xuzhou, Suzhou, and other places on the way. The following will consider flight plan management as an example to illustrate the application of the security architecture designed in this paper from the three stages of the flight.

Before the flight: Pre-made flight plan. Flight(X) needs to formulate the flight plan and corresponding access strategies of this flight and then submit them to the information broadcasting layer. The broadcasting layer packages the information collected over a period and sends it to the blockchain terminal layer (here, the blockchain terminal layer acts as a flight plan approver). The terminal layer determines whether to approve the flight plan and provides feedback about the flight on the basis of the collection of external information (such as weather information, ground conditions, and traffic flow at the destination airport).

If the plan is approved, the blockchain terminal layer will record and store once to complete the generation of new blocks.

During the flight: Modify the flight plan on the basis of external information. The blockchain terminal layer continues to collect updated external information. In the event of severe weather or changes in current airspace flow, the flight route needs to be changed for safety reasons, and the blockchain terminal layer will modify the flight plan and return it to the crew. If the flight agrees to the modified flight plan, the previous block generation operation will be repeated. The blockchain terminal layer is also responsible for recording this modification information and the related operations in the block.

After the flight: Ensure the correctness and completeness of the modification record. The blockchain terminal layer must ensure that compared with the original flight plan, any changes to the flight plan are reported and recorded during the flight. Components such as time stamps and underlying cryptography in the blockchain are used to ensure reliable traceability and strong confidentiality of flight data.

(e) The storage structure.

Due to some unexpected circumstances and restrictions (such as bad weather around the destination airport), these factors will cause the delay or cancellation of the flight, and it is usually necessary to rework the flight plan to solve the ATFMP (Air Traffic Flow Manage Problem) [31]. In the scenario in general, starting before Flight(X) takes off, the blockchain terminal layer will continuously collect external information and feedback key information to the flight. This information is finally generated by the blockchain terminal layer to generate blocks and merge them into the chain (the specific steps have been explained in the previous sections). In addition to the flight schedule, the uploaded information includes the current location of the flight, flight altitude, and other parameters. The storage structure of the block is shown in Figure 12.

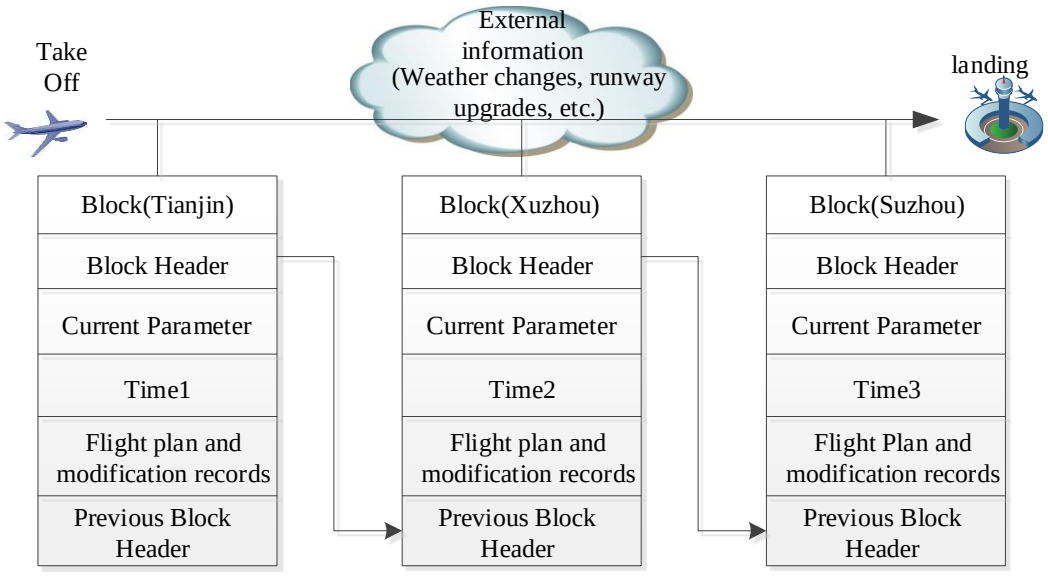

Figure 12. The storage structure of the blockchain.

7. Scientific Issues and Deployment Implementation Routes

Three aspects are highlighted in the "Civil Aviation Cyber Space Security Strategy" formulated by ICAO and the "Civil Aviation Network Information Security Management Regulations (Provisional)" issued by the Civil Aviation Administration of the Ministry of Communications of China: first, identify the security threats faced by the aviation network; second, master the security status of aviation network operation; and third, build a complete aviation network information security assurance system.

7.1. The Scientific Issues

According to the three key points, three scientific issues that to be solved are summarized.

(a) Scientific Issue 1: Complex game relationship of networked ATM-CPS.

This scientific issue aims to solve the first key point—finding the security threats faced by the aviation network and studying the source and extent of threats to aviation network security. Networked ATM system is a multi-dimensional complex system integrating network, computing, and equipment physical environment. Through the organic combination and deep cooperation of aviation communication, statistical calculation, and automatic control technology, it faces the management and control challenges of soaring flight density and diversified types of aircraft and realizes the safe and efficient operation of air transportation. Therefore, the networked ATM system is a complex intelligent management system with CPS characteristics, which is a deep integration of cyber system and physical system. Therefore, solving the CPS model of the networked ATM system is beneficial to:

- Master the security threats and degrees faced by the networked ATM, and build a unified and effective threat model;
- Analyze the requirements of information security assurance of ATM system, design the technology of information security assurance of ATM system, and build a systematic information security assurance architecture of ATM system.

(b) Scientific Issue 2: Networked ATM-CPS information security situation awareness.

This scientific issue aims to solve the second key point—to master the security status of aviation network operation. According to the operation of the networked ATM system, the prediction and evaluation of its network security situation will help to timely adjust its information security assurance strategies and measures. It includes two processes:

- Security situation prediction. The change of security situation of networked ATM system is a complex nonlinear process. An intelligent prediction model based on neural network is established by using deep learning method. Nonlinear time series prediction is conducted for time-based sequence actions in ATM operation. The depth neural network model is used to calculate the nonlinear time series data, and the security situation of the networked ATM system is obtained through approximation and fitting;
- Security assessment. According to the requirements of the National Security Classification Protection Guide, an approach based on security baseline strategy is adopted to conduct a multi-dimensional security assessment of the networked ATM system from three dimensions: static (functional design and technical measures), dynamic (operation status and development trend), and status (security status and security attributes).

(c) Scientific Issue 3: Systematic ATM-CPS information security assurance mechanism.

This scientific issue aims to solve the third key point—building a complete aviation network information security assurance system and establishing a lasting and effective security mechanism. It is necessary to establish the security threat model of the networked ATM system and propose a complete network security defense solution for the networked ATM system according to the SSE theory. It includes:

- Analyzing the characteristics of the ATM system and the demand for information security assurance, formulating the information security assurance strategy of the ATM system, launching the ATM-CPS information security assurance plan, and building a systematic information security assurance architecture of the ATM system;
- Specifying the requirements, guidelines, and specifications for ATM-CPS information security assurance and designing specific core algorithms, special methods, and key technologies for information security assurance.

7.2. The Key Technologies

According to the above three key scientific issues to be solved, the following three key technologies should be adopted.

(a) Information security modeling technology of networked ATM-CPS based on game theory.

The cyber system and physical system of ATM-CPS seem to be independent of each other, but they are closely coupled with each other in the entire operation process. Because the standards and specifications of transmission protocols and communication interfaces used by each independent resource subsystem of the ATM are varied and not uniform, and the existing calculation models and communication models are quite different from the actual physical process models of the ATM-CPS, it is impossible to describe the information transmission flow among the various element nodes of the ATM system to quantify the interaction between the ATM cyber system and the physical system. Therefore, the ATM is abstractly mapped to CPS, and then the security of the ATM system is analyzed by using the CPS security theory. On the basis of analyzing the architecture and information flow of networked ATM system, the fine-grained CPS modeling of ATM is realized. The main tasks to be completed include:

- Model the dynamic behavior of CPS under the normal operation and network attack of ATM system;
- Study the system parameters (detection rate, defense effect, physical interruption time, etc.) and attack parameters (attack intensity, attack duration, attack mode, etc.) that affect CPS security, accurately predict the performance of both players in the game, and reduce the impact on normal operation of ATM system in the game with attackers;
- Study the strategy selection of attackers and ATM system under different situations in the mutual game according to game theory and estimate the attack performance and detection probability according to the defensive and antagonistic parameters of ATM-CPS;
- Use the security evaluation algorithm to calculate the security indicators, such as mean-time-to-shutdown (MTTSD) and availability of ATM-CPS, and obtain an accurate evaluation of ATM-CPS security through the comprehensive evaluation of the indicator system;

(b) Networked ATM information security situation awareness technology based on ATM-CPS game model.

The information security situation of networked ATM system is the operation status and change trend of the entire network, which is composed of various system equipment operation conditions, network traffic behavior, aviation user behavior, and other factors. Various pieces of system equipment in the ATM are independent of each other and are connected through the network. However, after a certain aeronautical communication, the navigation, surveillance, and automation system equipment in the system is successfully attacked, and the threat can spread to other equipment connected to the equipment through the network (for example, ADS-B system networking; when one of the ADS-B systems is attacked, the attacker can use the ADS-B system as a springboard to attack ADS-B systems in other networks). This renders these devices subject to security threats. The networked ATM information security situational awareness technology based on CPS game model analyzes the impact of security threats (network intrusion, data tampering, and privacy leakage) and attacks (ADS-B counterfeit signals and Beidou navigation information deception) on the ATM system, which can accurately and comprehensively evaluate and predict the information security situation of the ATM.

- Situation assessment. In the networked ATM system, various resource subsystem devices—all of which are data sensors used for receiving (collecting) and sending (transmitting) ATM business data—are distributed in different locations in a wide area and are connected by different communication protocols and interfaces to form

a typical sensor network. Aimed at the processing mode of distributed collection and acquisition of ATM business data by ATM system equipment, the structure framework of security situation awareness system of ATM system based on multi-sensor is studied (divided into three levels from bottom to top: information collection level, element extraction level, and situation decision-making level), and the network physical structure of ATM system and the hierarchical model of equipment layer, transmission layer, and application layer are designed. On the basis of the structural framework of the security situation awareness system of the ATM system, the eXML format solution for multi-source heterogeneous security information of the ATM system is proposed. It includes three steps: detection data fusion, establishment of threat propagation network (TPN), and evaluation of CPS game model. The CPS game model is used to comprehensively evaluate the security situation of each resource subsystem of the ATM system from the perspectives of attack and defense, and the development trend of the security situation of the entire networked ATM system is obtained through the quantitative evaluation method of network security situation, thus providing a reference for timely adjustment of the system security strategy.

- Situation prediction. The deep learning model is used to predict the security situation of networked ATM system. First, we sort out the network attack events suffered by the networked ATM, study the method of event embedding, express the security events as dense vectors using neural tensor network (NTN), and conduct security event training. Then, the deep convolutional neural network is used to model the impact of security incidents, and a dynamic prediction model of networked ATM system security situation is established on the basis of the deep convolutional neural network. Genetic algorithm is used to optimize the model and realize the nonlinear time series prediction of the security situation of networked ATM system.

(c) Building trust mechanism technology of networked ATM based on blockchain.

On the basis of the open-source licensing blockchain framework and in combination with the business characteristics and processes of the ATM, the point-to-point network design, the application of cryptographic technology, the implementation of distributed algorithms, and the development of data storage technology for the networked ATM are completed. The goal is to establish a blockchain-based trust model for the networked ATM, study the information security assurance architecture of the networked ATM based on the trusted model, and realize the data security and privacy protection of the ATM. Meanwhile, secure communication among the ATM departments, airlines, airports, and other operation support units or other authorized entities in the space–air–ground integrated ATM network can be guaranteed. The functions realized include:

- Adopt the characteristics of blockchain decentralization, asymmetric encryption, distributed storage, etc., and realize point-to-point communication in the ATM system through the distributed accounting method of the underlying public chain so as to ensure that all devices in the ATM system can securely exchange data in a trusted environment;
- Adopt smart contract technology to convert and write the registered network access information of all component resource subsystem equipment in the ATM into the blockchain. The characteristics of blockchain technology ensure that the entire process of storage, reading, and execution of business data of ATM is transparent, traceable, and tamper-proof. It can solve the trust problems among the equipment of the ATM, airlines, airports, and ATM departments and between the ATM operators and the ATM;
- Establish a tamper-proof intelligent trust mechanism in the networked ATM system by using the blockchain network; this can resist the tampering of core data by internal personnel of the ATM, identify false data injection, and resist the deceptive attack facing satellite navigation information. On the basis of the blockchain, design the technology of building the trust mechanism of the networked ATM with the functions of certificate authorization, smart contract support, and aviation sensitive information

protection, and realize the sharing and information security of ATM big data according to the terms specified in the form of a smart contract.

7.3. The Technical Route

According to the general research idea, the CPS model of networked ATM system is established at first. The next step should be to determine the security risks and vulnerabilities of the networked ATM system on the basis of the model, identify the security threats faced by the networked ATM system, and study the threat model of the ATM-CPS. The Bayesian Nash equilibrium strategy is used to design the ATM-CPS game model, and the blockchain technology is used to realize the trusted model so as to build the architecture of the ATM-CPS information security assurance. The specific research technical route and measures are shown in Figure 13. According to the decomposition of the research content in this paper, the design of the technical route is based on the research of the content in each stage. The specific steps are as follows.

(a) ATM-CPS model.

The establishment of the networked ATM-CPS model is based on the study of the business information data flow of the ATM and the composition of the ATM, including three steps:

- Determine the dynamic weighting network of the ATM system;
- Establish fine granularity network model of the ATM system;
- Establish the refined CPS model of the ATM system.

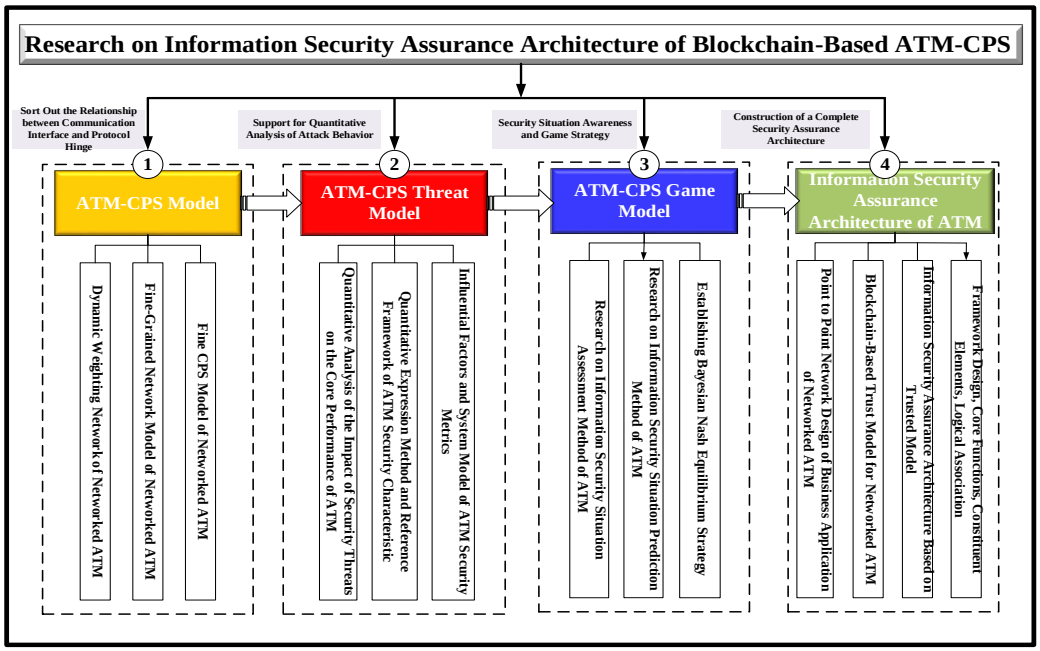

Figure 13. Technical route and measures of the research.

(b) ATM-CPS threat model.

Aimed at the complex composition and heterogeneous structure of the networked ATM system, the network traffic super fusion probe technology is used to conduct deep packet analysis and flow analysis for the traffic of different communication protocols and interfaces so as to realize the comprehensive and effective detection of various security threats faced by the networked ATM system. Then, it is found that the purpose of discovering system security risks and mining system vulnerabilities is achieved, the identification method of information security risks of ATM system is studied, and the information security threat model of ATM is established. The specific implementation steps are as follows:

- Carry out quantitative analysis on the impact of security threats on the core performance of the ATM system;
- Design the quantitative expression method and reference frame of the ATM system security characteristics;
- Establish the influencing factors and system model of the ATM system security measurement.

(c) ATM-CPS game model.

The four aspects of ATM-CPS security situational awareness capability construction, security indicator extraction, situational prediction, and situational visualization are used to strengthen the situational awareness capability of ATM, thus laying the foundation for the establishment of ATM-CPS game model based on Bayesian Nash equilibrium strategy. The specific steps include:

- Study the information security situation assessment method of the ATM system;
- Study the information security situation prediction method of the ATM system;
- Establish Bayesian Nash equilibrium strategy.

(d) Information security assurance architecture of the networked ATM system.

On the basis of the security hidden danger and system vulnerability mining of the networked ATM, the security threats are clarified, and the information security model of the ATM-CPS is established. In addition, from the perspective of the relationship among the elements of ATM infrastructure from the top level, we design the architecture of ATM information security assurance system on the basis of blockchain trust model. The specific steps include:

- Study the point-to-point network design of the business application of the networked ATM system;
- Establish the blockchain-based trust model of networked ATM system;
- Design the information security assurance architecture on the basis of the trusted model;
- Complete the design of information security assurance framework of the networked ATM system, including core functions, constituent elements, and logical associations.

8. Conclusions

The highly integrated information and real-time data sharing of networked ATM has become a necessary means to ensure the safety of air traffic. With the application of artificial intelligence and other information network technologies in the ATM, while improving the performance and efficiency of the existing system, various vulnerabilities in the information network have seriously affected the safe operation of the ATM-CPS. Therefore, the information security assurance of the networked ATM must consider mining its security risks and system vulnerabilities on the basis of cyber–physical integration, establishing a systematic assurance system, and realizing an all-round information security assurance of the networked ATM system. To summarize, the research of this paper has application value and prospects in the future.

Author Contributions: Conceptualization, X.L. and R.D.; methodology, X.L.; validation, R.D., Q.W. and L.Z.; investigation, X.L.; resources, R.D.; writing—original draft preparation, X.L.; writing—review and editing, R.D.; visualization, X.L.; supervision, Q.W.; project administration, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the joint funds of National Natural Science Foundation of China and Civil Aviation Administration of China (U2133203), the National Natural Science Foundation of China (62172418), the Natural Science Foundation of Tianjin, China (21JCZDJZ00830), the Scientific Research Project of Tianjin Municipal Education Commission (2019KJ117), and the Fundamental Research Funds for the Central Universities of China (ZXH2012P004, 3122021026).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ATM	Air Traffic Management
CPS	Cyber-Physical System
ATC	Air Traffic Control
CNS	Communication, Navigation, and Surveillance
ICAO	International Civil Aviation Organization
GNSS	Global Navigation Satellite System
ADS-B	Automatic Dependent Surveillance-Broadcast
SWIM	System-Wide Information Management
DDoS	Distributed Denial of Service
KGC	Key Generation Center

References

1. ICAO. *Global Air Navigation Plan. ICAO Doc 9750*, 6th ed.; ICAO: Montréal, QC, Canada, 2019.
2. Sampigethaya, K.; Poovendran, R. Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport. *Proc. IEEE* **2013**, *101*, 1834–1855. [CrossRef]
3. ICAO. *Security and Facilitation Strategic Objective: Aviation Cyber-Security Strategy*; ICAO: Montréal, QC, Canada, 2019.
4. Arthur, P. A Systems Approach to Protecting the U.S. Air Traffic Control System Against Cyber-Terrorism. Presentation PPT. 2012. Available online: https://www.federalregister.gov/documents/ (accessed on 2 December 2022).
5. Homeland Security. *National Strategy for Aviation Security of the United States of America*; Homeland Security: Washington, DC, USA, December 2018.
6. Mehan, D.J. Systems Security—The Federal Aviation Administration's Layered Approach. *TR News* **2000**, *211*, 8–13. Available online: https://www.nstl.gov.cn/paper_detail.html?id=c4f0fcec6bb53e1a2cd5d1d3349d2638 (accessed on 2 December 2022).
7. Aviation Cyber Security Strategy. *Department for Transport and Civil Aviation Authority*; Aviation Cyber Security Strategy: London, UK, 12 July 2018.
8. Thompson, K.H.; Tran, H.T. Application of a Defender-Attacker-Defender Model to the U.S. Air Transportation Network. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018; pp. 1–5.
9. Hird, J.; Hawley, M.; Machin, C. Air Traffic Management Security Research in SESAR. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 486–492.
10. Montefusco, P.; Casar, R.; Koelle, R.; Stelkens-Kobsch, T.H. Addressing Security in the ATM Environment: From Identification to Validation of Security Countermeasures with Introduction of New Security Capabilities in the ATM System Context. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 532–541. [CrossRef]
11. United States Government Accountability Office. *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems. Report to Congressional Requesters, GAO-15-221*; United States Government Accountability Office: Washington, DC, USA, January 2015.
12. The Boeing Company. *Views on the Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 9 February 2016.
13. Holt, T.B.; Moallemi, M.; Weiland, L.; Earnhardt, M.; McMullen, S. *Aircraft Cyber Security and Information Exchange Safety Analysis for Department of Commerce*; Report; Embry-Riddle Aeronautical University: Washington, DC, USA, 2 June 2016.
14. Elias, B. *Protecting Civil Aviation from Cyberattacks*; CRS Insights: Watford, UK, 18 June 2015.
15. Stelkens-Kobsch, T.H. *Security in ATM—A Validation Methodology for Security Prototype*; Report; Deutscher Luftund Raumfahrtkongress (DLRK): Sacramento, CA, USA, 13–15 September 2016.
16. Schaper, M.; Stelkens-Kobsch, T.H.; Carstengerdes, N. From preparation to evaluation of integrated ATM-security-prototype validations. In Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 17–21 September 2017; pp. 1–8. [CrossRef]
17. Bogoda, L.; Mo, J.; Bil, C. A Systems Engineering Approach to Appraise Cybersecurity Risks Of CNS/ATM and Avionics Systems. In Proceedings of the 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 9–11 April 2019; pp. 1–15. [CrossRef]

18. Sampigethaya, K.; Poovendran, R. Cyber-physical Integration in Future Aviation Information Systems. In Proceedings of the 2012 IEEE/AIAA 31st Digital Avionics Systems Conference (DASC), Williamsburg, VA, USA, 14–18 October 2012.
19. Sampigethaya, K.; Poovendran, R.; Shetty, S.; Davis, T.; Royalty, C. Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond. *Proc. IEEE* **2011**, *99*, 2040–2055. [CrossRef]
20. Kumar, S.A.; Xu, B. Vulnerability Assessment for Security in Aviation Cyber-Physical Systems. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 145–150.
21. Koutsoukos, X.; Karsai, G.; Laszka, A.; Neema, H.; Potteiger, B.; Volgyesi, P.; Vorobeychik, Y.; Sztipanovits, J. SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber–Physical Systems. *Proc. IEEE* **2017**, *106*, 93–112. [CrossRef]
22. Lan, M. The Information Assurance of Air Traffic Management System Based on SSE Theory. Ph.D. Thesis, Tianjin University, Tianjin, China, 2011. (In Chinese)
23. Lan, M.; Zhijun, W. *Air Traffic Management Information Security Assessment*; Science Press: Beijing, China, 2015. (In Chinese)
24. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A Survey and Analysis of the GNSS Spoofing Threat and Counter-measures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [CrossRef]
25. Bian, S.; Ji, B.; Hu, Y. Research status and prospect of GNSS anti-spoofing technology. *Sci. Sin. Inf.* **2017**, *47*, 275–287. [CrossRef]
26. Peng, Z.; Xu, J.; Hu, H.; Chen, L.; Kong, H. BlockShare: A Blockchain Empowered System for Privacy-Preserving Veri-fiable Data Sharing. *IEEE Data Eng. Bull.* **2022**, *45*, 14–24.
27. Kaur, K.; Kaddoum, G.; Zeadally, S. Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5178–5189. [CrossRef]
28. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Sig-nature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7059–7067. [CrossRef]
29. Wang, H.; Xu, C.; Zhang, C.; Xu, J.; Peng, Z.; Pei, J. vChain+: Optimizing Verifiable Blockchain Boolean Range Queries. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 1927–1940.
30. Wu, H.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. VQL: Efficient and Verifiable Cloud Query Services for Blockchain Systems. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 1393–1406. [CrossRef]
31. Ali, K.M.; Alexandre, S.; Nidhal, R. A Flight Plan Rescheduling in Air Traffic Management Problem: A Time Discret Event System Approach. *IFAC Proc. Vol.* **2012**, *45*, 285–290. [CrossRef]