JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 통신 기술

J. Adv. Navig. Technol. 21(6): 633-637, Dec. 2017

항공기 디지털 네트워크 시스템 보안 문제점과 사이버 대응 전략

Security Problems in Aircraft Digital Network System and Cybersecurity Strategies

임 인 규 · 강 자 영*
한국항공대학교 대학원 항공운항관리학과

In-Kyu Lim · Ja-Young Kang*
Aviation Management, Graduate School, Korea Aerospace University, Gyeonggi-do, 10540, Korea

요 약

항공기와 항공 네트워크에 대한 사이버 공격은 일반적으로 지상 산업에서 흔히 볼 수 있는 사이버 공격과 크게 다르지 않다. 항공 교통 인프라스트럭처(infrastructure)는 항공 교통 자원 확보를 위해 디지털 기반 구조로 전환되고 있다. 다양한 종류의 통신 환경과 정보 통신, 항법, 감시 및 기내 엔터테인먼트 시스템이 사이버 테러 위협에 노출될 위험을 가중시키고 있다. 또한 무인항공기의 출현은 사이버 테러에 의해 통제될 수 없는 위험을 내포하고 있다. 차세대 데이터 네트워크 시스템 환경에서 항공기 시스템 및 항공 기반의 인프라스트럭처에 대한 사이버 위협의 취약점을 인식하고 항공 선진국의 사이버 보안 표준과 대응 전략을 분석했다. 그리고 국내 항공 환경에서 고려해야 할 사이버 보안 정책에 대한 포괄적인 방안을 논의하고, 보안 환경에 대한 개념과 신속한 대응 전략 수립 등을 논의하였다.

[Abstract]

Cyber attacks on aircraft and aeronautical networks are not much different from cyber attacks commonly found in the ground industry. Air traffic management infrastructure is being transformed into a digital infrastructure to secure air traffic. A wide variety of communication environments, information and communications, navigation, surveillance and inflight entertainment systems are increasingly threatening the threat posed by cyber terrorism threats. The emergence of unmanned aircraft systems also poses an uncontrollable risk with cyber terrorism. We have analyzed cyber security standards and response strategies in developed countries by recognizing the vulnerability of cyber threats to aircraft systems and aviation infrastructure in next generation data network systems. We discussed comprehensive measures for cybersecurity policies to consider in the domestic aviation environment, and discussed the concept of security environment and quick response strategies.

Key word : Cybersecurity, Communication, Navigation, Surveillance/Air Traffic Management, Aircraft.

https://doi.org/10.12673/jant.2017.21.6.633

Received 29 November 2017; **Revised** 7 December 2017
Accepted (Publication) 15 December 2017 (30 December 2017)

***Corresponding Author; Ja-Young Kang**

Tel: +82-2-300-0081
E-mail: jaykang@kau.ac.kr

I. 서 론

항행 시스템의 백본으로서 통신 네트워크는 데이터 통신의 기술 발전으로 기존 음성 무선 통신 방식에서 무선 IP(internet protocol) 통신 방식으로 전환되고 있다. 또한 항공기 내 항행 지원을 위한 네트워크 뿐 아니라 항공사 이용 업무용 네트워크, 그리고 기내 승객의 편이를 위한 서비스 네트워크를 이용한 데이터 통신이 지상의 COTS(commercial off the shelf) 기술력이 바탕이 되어 이용자가 더 많아지고 있다. 이에 따른 항공기 시스템 및 지상의 항행 네트워크로 침입하는 사이버 보안 위협은 더욱 가중되고 하고 있다[1].

항공기 시스템과 기내 혹은 지상의 네트워크 사이에서 불법 접속에 의한 사이버 침입은 일반적인 산업에서 나타나고 있는 사이버 테러나, 그 위협이 크게 다르지 않다고 본다. 따라서 본 논문에서는 항공기 보안 위협 사례를 알아보고 시스템 보안의 취약성에 따르는 항공기 디지털 통신 시스템 보안 문제점을 파악하였고, 이에 대한 대응 전략으로 항공 선진국인 유럽과 미국의 차세대 항공 디지털 통신 네트워크 구축에 따르는 사이버 보안의 대응책을 분석하였다. 그리고 국내 환경에서 사이버 보안 적용 방안에 대하여 논의하였다.

II. 항공기 디지털 통신 시스템 보안 문제점

2-1 항공기 시스템의 보안 위협 사례

최근 한국에서 일어난 GPS JAMMING 공격은 위치 기반의 모든 시스템을 무용지물로 만들었고, DDOS(distributed denial - of service)의 공격은 네트워크의 과부하로 인하여 시스템 서버의 비정상적 성능으로 인하여 많은 불편을 초래 하였다. 또한 최근에는 중요한 데이터 손실을 주는 랜섬웨어와 같은 형태의 사이버 공격도 급증하고 있다. 표 1은 보고된 사이버 공격 및 침입에 의하여 영향을 받은 항공 관련 주요 사례이다[1].

보안사건의 위협에 대한 유형을 보면 주로 특정 시스템을 기만하거나 가짜 정보를 제공하는 방법으로 공격하여 시스템의 부 작동을 야기한다. 지상에서 무선으로 제어하는 드론 같은 무인기의 위치정보에 대한 스푸핑(spoofing, 기만) 공격과 드론에서 송신하는 정보를 가로채는 등 사이버공격 사례이다.

2-2 시스템 보안의 취약성

통신 기술의 발달과 더불어 안전운항에 필수적인 항행지원 시스템과 항공사의 필요에 따라 사용하는 지상 시스템과 항공기간의 데이터 통신, 그리고 기내 승객 혹은 승무원의 편의를 위한 통신 네트워크가 있다. 그림 1는 최근 항공기에서 적용되는 디지털 환경의 데이터 통신 인프라스트럭처를 보여 준다[2].

표 1. 보안 사건과 위협 사례
Table 1. Security Incident and Threats.

No	Year	Subject	System
1	2013	Attacking the Flight Management System (FMS)of Aircraft	FMS
2	2012	Attacking Mission-Critical Systems via In-Flight Entertainment Systems Vulnerabilities in Commercial-Off-the-Shelf-Based Electronic Flight Bags(EFB)	EFB
3	2012	Spoofing Aircraft with Faked Automatic Dependent Surveillance-Broadcast Messages Tracking of Hidden Blocked Aircraft Registration Request Aircrafts	ADS-B
4	2012	Spoofing Global Positioning System Navigation of Civilian Drones	GPS
5	2011	Attacking Aircraft via Compromised Information Technology Infrastructures	AIRCRAFT
6	2011	Spoofing Global Positioning System Navigation of United States RQ-170 Sentinel Drone	GPS
7	2009	Intercepting Video Feeds of Drones	NETWORK

항공기와 VHF, HF, SATCOM, Broad Band(LTE, 3G), Wifi 등 다양한 무선 네트워크의 접속으로 데이터 통신이 증가되고, 새로운 복합적인 항공기 아키텍처와 시스템이 개발되고 상용 H/W(hardware)나 S/W(software)에 그 의존성이 증가되고 있다. 표 2는 무선 접속으로 항공서비스에 사용되는 데이터 서비스와 응용 프로그램 시스템을 제시 하였다. 이러한 다양하고 복잡한 시스템의 활용은 WiFi, 광대역(broadband) 접속을 경유하여 승객이나 승무원의 휴대전자장비(PED, portable electronic device)를 가지고 기내 네트워크에 접속이 가능한 하게 하므로

표 2. 항공기 응용 시스템의 무선 접속
Table 2. Wireless Connectivity for aircraft Application.

Item	Application
Air Traffic Control	CPDLC(controller-pilot data link communications)
Airline Operation Control	ACARS(aircraft communications, addressing and reporting system), EFB, 3G/LTE
Airport Connectivity	Terminal Area Network(Gatelink)

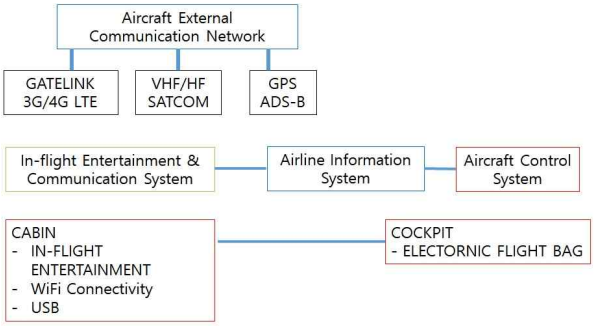

그림 1. 항공기 데이터 통신 인프라
Fig. 1. Aircraft Data Network & Interface.

사이버 보안에 취약한 위험성을 갖고 있다.

기내에서 혹은 지상에서 항공기의 시스템을 제어하거나 방해 할 가능성과 제한된 기내 내부 공간에서 무선 인트라넷 사용이 허용되어 사용자 상호간의 개인정보 악용이나 서버의 해킹 등 시스템 보안의 위험성을 갖고 있다.

미래의 항공통신 시스템은 IP 기반으로 광범위한 데이터통신 링크를 수용할 것이다. 이를 위해 미국의 FAA와 유럽의 EUROCONTROL에서 추진하고 있는 시스템으로 NextGen(next generation air transportation system)과 SESAR(single european sky ATM research)가 있다. 여기에서 SWIM(system wide information management)은 CNS/ATM(communications, navigation and surveillance/air traffic management) 환경에서 항공 교통정보 관련 모든 응용프로그램과 서비스를 통합 관리하는 백본으로 공항운영, 항공사운영, 기내 승무원, 기내 승객, 지상 이동승객의 모든 보안과 서비스가 포함되는 것으로 네트워크 중심 운영 개념으로 서비스 지향 아키텍처(SOA; service oriented architecture)로 설계되었다. 따라서 서비스 및 메시지 기반의 보안정책으로 시스템의 기밀성, 무결성 그리고 가용성

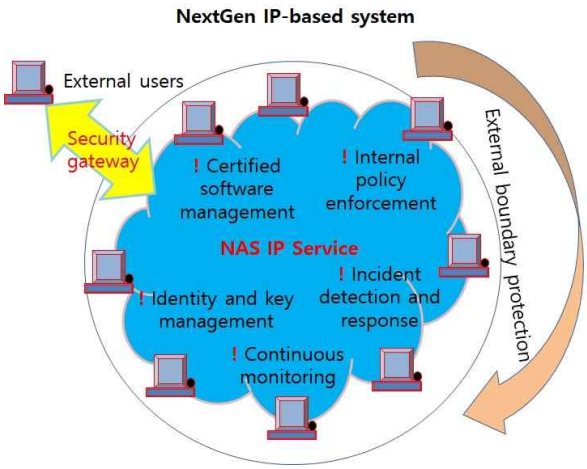

그림 2. NextGen IP Network
Fig. 2. NextGen IP Network(GAO-15-370).

표 3. 보안관련 절차 및 규정
Table 3. Document of Security.

Item	Subject
ICAO Annex 17	Security
RTCA DO-178	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254	Design Assurance Guidance for Airborne Electronic Hardware
RTCA DO-236	Security Assurance and Assessment Processes for Safety-related Aircraft Systems

을 가지는 표준 보안 모델을 가지고 있다[3].

미국의 NAS(national airspace system)에서는 그림 2에서 보여 주듯이 사이버보안의 도구를 가지고 내부 정책의 강화, 인가 S/W 관리, ID 및 Key 관리, 사건의 검출 및 대책, 지속적인 모니터링 또한 보안 게이트웨이를 가지고 외부의 침입을 보호하고 있다[3].

표 3는 NextGen(next generation air transportation system)과 SESAR(single european sky ATM research)에서 언급하고 있는 보안관련 문서를 보여주고 있다. 이들 규정은 항공기 보안에 대한 설계, 평가, 환경 그리고 운영에 대하여 기술하고 있다[4].

2-3 국내 사이버 보안 적용 방안

대표적인 항공통신 매체인 VHF/HF 통신과 위성통신(SATCOM)은 위성기반의 차세대 항행 시스템과 더불어 IP 기반의 데이터 통신으로 정보의 안전성, 무결성, 그리고 가용성을 확보한 항공통신 서비스를 추구하고 있지만, 항공기가 공항 지역 혹은 지상에 있을 때는 COTS 기반의 WiFi, 3G, LTE, Gate Link , WiMax(AeroMax) 등 대용량의 고속 데이터 통신을 사용하고 있다. 또한 최근 증가 되는 무인항공기의 대두는 국제적인 C2(command control) 네트워크 환경에서 위협적인 항공 교통의 안전 요인이 될 수 있으며, 불특정 다수의 위협에서 발생할 수 있는 사이버 공격에 대한 위험을 직시하여 설계, 제작, 운용, 유지, 그리고 관리 측면의 적절한 규정과 대비책이 준비 되어야 한다.

항공기의 네트워크 보안 환경은 다양한 무선 시스템의 통신과 자동화 되어가는 시스템의 복잡한 결합으로 보안의 관리가 더 취약해지고 있다[2]. 따라서 국내에서도 항공 사이버 보안(aviation cyber security)에 대한 종합적이고 체계적인 법체계 수립이 요구된다.

1) 가용성 관리

리스크의 예로 항공기 내부 주요 시스템의 네트워크 연결이 일시적으로 접속 불가 상태가 되어 시스템이 정상 동작이 되지

표 4. 보안 가이드
Table 4. Security Guide.

RTCA (radio technical commission for aeronautical) Document	Subject	ED (eurocae document)
DO-326A Airworthiness Security Process Specification	[Development] • Risk assessment process with a generic set of activities • Security development activities • Interfaces with the safety assessment process	ED-202A
DO-355 Information Security Guidance for Continuing Airworthiness	[Operation/Maintenance] • Airborne Software • Aircraft Components • Aircraft Network Access Points • Ground Support Equipment • Ground Support Information Systems • Digital Certificates • Aircraft Information Security Incident Management	ED-204

않도록(원격제어, 혹은 대 단위 트래픽 양성, 신호정보의 위변조) 하여 항공기의 운항에 영향을 주는 예상 시나리오를 고려해 보았다.

변화하는 환경에서 사이버 보안은 위협을 미리 방지하는 것과 이미 위협에 노출 된 경우 실시간 탐지와 신속한 대응이 무엇보다 중요하다. 따라서 시스템은 지속적으로 다음과 같이 관리 되어야 한다.

- 시스템이 악성코드에 감염되었는지,
- 사이버 해킹 여부 인지,
- 신속한 대응 방안은 있는지,
- 보안 지침과 암호화 기술을 이용한 보안 통신,
- 각 개별 장치의 상호 인증,
- 사용자에 대한 유지관리,
- 가용성의 관점에서 secure계정관리,
- 서버접근 통제와 네트워크 서비스 사용자 로그관리 등,

지속적인 취약점 점검과 보안 패치로 유효한 네트워크 서비스가 되도록 해야 한다[5].

2) 시스템 개발단계에서의 보안개념

항공기 시스템의 사이버 보안은 시스템설계 개발 단계에서 강력한 보안 개념이 포함되어야 한다. 소프트웨어 개발, 분배, 디지털 데이터의 기능, 리소스 관리 및 운용을 위한 항공기 내부 / 외부 접근제어 보안 개념을 수립해야 한다.

독립된 시스템 컴퓨터에 접근하는 물리적인 공격에 대한 대응이나 EMI(electromagnetic interference)/RFI(radio frequency interference), HIRF(high intensity radiated fields)등 전자적 공격에 대하여 시스템의 면역성과 데이터 정보 보호 수준에서 최소한의 안전성 확보를 위한 검증과 인증의 절차가 포함되어 설계되어야 한다[2].

3) 네트워크 보안정책

점 대 점(Point to Point) 환경의 시스템 네트워크에서 IP 기반의 항공기 네트워크로 전환됨으로써 각각의 부 지역 네트워크(LAN, Domain) 에 대한 항공기 시스템의 위험에 대한 심각한 정도에 따라 위험 요소를 구분하여 우선순위에 따른 네트워크를 분리 운영 설계함으로써 사이버 위협에 대한 위험성과 시스템 결함에 대한 안전성을 확보하고 있다. 따라서 디지털 네트워크에 대한 취약성을 고려한 보안 정책으로 각각의 분리된 시스템 네트워크 간의 상호 운용성과 기술적인 보안을 기반으로 물리적 부분뿐만 아니라 소프트웨어적으로 강인한 시스템이 필요하다.

지상과 항공기간 및 항공기내의 복잡하고 다양한 통신 네트워크 환경에서 안전한 항공 운항서비스를 위한 공통의 사이버 보안 인프라스트럭처를 위한 표준이 있어야 한다. 이것은 원칙성 있는 비전과 전략의 프레임 워크로 진화하는 위협요소를 해결하기 위한 로드맵이 적용 되어야 한다. 또한 위협과 리스크가 동일한 원칙에 따라 관리되고 시스템의 상호작용을 이해하는 지속적인 평가 프로세스가 있어야 한다.

항공 사이버 위협은 국제적 파급효과가 크고 민감한 항공 보안 문제이기 때문에 국가적인 상황인식의 보장과 위협에 대한 충분한 소통이 요구된다. 또한 운영의 원칙은 사이버 문화, 탄력성, 중요 데이터 분리, 공격 탐지 등 연구 개발에 리소스를 집중해야 하고, 사고에 대한 대응의 적시성, 방어 시스템의 강화, 그리고 사이버 보안 위협 정보의 공유는 위협 대응 설계의 기본 원칙으로 산업체 간의 상호 협력과 정부 주도의 적극적인 협력이 요구된다[5].

4) 보안기술과 규정

보안기술을 안전기술(safety engineering)관점에서 보면,

- 보안 우선순위를 설정하고,
- 보안 취약점을 분석하고,
- 보안이 요구되는 곳을 선정하여 보호 관리하고,
- 그 보호 수단의 효과성을 평가하는 것이다.

따라서 적절한 감항당국의 규정 절차에 따라 항공기 시스템 운영 및 항공 산업의 안전평가에 사이버보안위험평가(cyber security risk assessment)을 적용하여 관리 할 수 있도록 해야 한다[5].

표 4는 보안 가이드를 보여준다. 항공기 제작 단계에서는 RTCA DO-326A “Airworthiness Security Process Specification” 가이드에 의거 사이버보안(cybers security) 이 관리되어야 하고, 운용 및 유지보수(maintenance) 단계에서는 RTCA DO-355, “Information Security Guidance for Continuing Airworthiness” 가이드에 따라 사이버보안 관점에서 항공기의 감항성이 유지될 수 있도록 관리 적용해야 한다.

항공기내의 시스템 아키텍처는 시스템의 안전 우선순위에

따라 그 보안 수준이 정의되고 독립된 통신 환경 및 관리 비용으로 자원을 분배하여 운영함으로써 시스템 방화벽(firewall)과 소프트웨어 운영으로 최적의 보안 시스템을 구축하고 있다. 하지만 비행중인 항공기 시스템에 대한 사이버 테러는 그 결과가 상당히 치명적일 수 있기 때문에 적극적인 사이버테러의 대비가 수립되어 관리되어야 한다.

Ⅲ. 결 론

본 논문에서는 항공기의 디지털 네트워크의 다양한 시스템 리스크로 인한 사이버 위협 노출 사례와 시스템의 취약성의 문제점을 알아보고, 항공 선진국의 차세대 항공 디지털 통신 네트워크 구축에 따르는 사이버 보안의 대응책을 분석하였다. 그리고 국내 환경에서 사이버 보안 적용 방안에 대하여 논의하였다. 사이버 보안에 대한 조직, 보호, 모니터링, 조치 및 회복 등에 대한 종합적이고 독립적인 네트워크 보안정책 수립과 변화하는 다양한 보안 환경에서의 관리 가용성, 항공기 시스템 개발 단계에서의 검증과 인증해야 할 보안 개념, 그리고 사이버보안의 보호 수단에 대한 평가 관리를 위한 정책과 기술에 대하여 강조하였다.

사소한 원인으로 항공통신 시스템이 손상되면 많은 승객 및 항공 업계에 큰 불편을 초래하게 되고, 고의로 항공기 및 항공 시스템을 위협하는 것에 대하여 적절히 대처하지 못하면 커다란 국가적 경제적 손실을 감수 할 수밖에 없다.

사이버 보안은 과거의 방화벽이나, 소프트웨어 제어 인증(authentication) 만으로는 충분하지 않다. 시스템을 모니터링하여 비정상적인 상태를 검출하여 침입자를 확인하고 시스템을 보호해야 하며 주기적인 시스템 검사와 검증으로 무결성과 가용성을 확인해야 한다. 그래서 차세대 데이터기반의 항공통신네트워크 시스템이 사이버 보안 위협에 신속하게 대응 할 수 있도록 사이버 보안전략 인프라스트럭처의 구축이 요구된다.

Acknowledgments

본 연구는 국토교통부 항공안전기술개발사업 (과제번호: 16ATRP-C108186-02)의 지원을 받아 수행되었습니다.

References

[1] M. Wolf, M. Minzlaff, and M. Moser, “Information technology security threats to modern e-Enabled aircraft: A cautionary note,” Journal of aerospace information systems, Vol. 11, No. 7, July 2014

[2] P. Skaves, FAA AIRCRAFT SYSTEMS INFORMATION SECURITY PROTECTION OVERVIEW, FAA

[3] GAO-15-370 AIR TRAFFIC CONTROL FAA needs a more comprehensive approach to address cyber security as agency transitions to NextGen, Apr. 2015

[4] CSFI ,CSFI ATC(air traffic control) cyber security project July 16, 2015

[5] AIAA, “The connectivity challenge; protecting critical assets in a networked world,” Aug.2013

임 인 규 (In-Kyu Lim)
2002년 08월 : 한국항공대학교 정보통신공학과 (공학석사)
2015년 08월 ~ 현 재 : 한국항공대학교 대학원 항공운항관리학과 박사과정
1991년 12월 ~ 현 재 : 대한항공 정비본부 항공기 정비
※관심분야 : CNS/ATM, 시험평가인증, 공항운영 및 관리, 항공보안공학

강 자 영 (Ja-Young Kang)
1992년 06월 : 미국 Auburn Univ, AE/Ph.D.
1979년 03월 ~ 1984년 08월 : 국방과학연구소 연구원
1992년 06월 ~ 2002년 03월 : ETRI 책임연구원/팀장
2002년 03월 ~ 현 재 : 한국항공대학교 항공운항학과 교수
2011년 12월 ~ 2015년 12월, 2017년 08월 ~ 현재 : 한국항공대학교 부설 항공체계시험인증연구센터장
※관심분야 : CNS/ATM, 항공체계공학, 시스템 V&V, 위성시스템 응용