



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0107914
(43) 공개일자 2014년09월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) G06F 21/60 (2013.01)
(21) 출원번호 10-2013-0022113
(22) 출원일자 2013년02월28일
심사청구일자 없음
기술이전 희망 : 기술양도, 실시권허여, 기술지도

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이덕규
경기 용인시 처인구 해실로 19-14, (해곡동)
이성현
대전 유성구 노은동로 233, 203동 701호 (지족동, 열매마을2단지)
(74) 대리인
제일특허법인

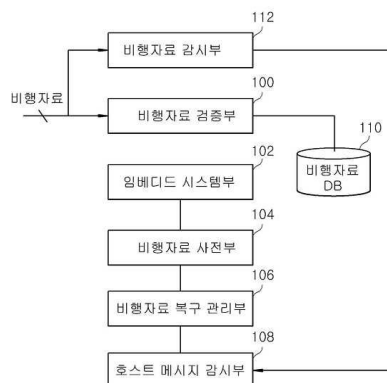
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 비행자료 보호 장치 및 비행자료 보호 방법

(57) 요약

본 발명은 내부 혹은 외부의 바이러스의 피해 및 비행자료 변조 및 수정 등의 해킹 발생에서 비행자료 시스템의 가용성, 신뢰성 및 무결성을 강화시켜 비행자료시스템 운영 시 관제 서비스를 마비시키는 다양한 사이버테러에 대응하여 실시간으로 비행자료를 자동으로 보호하는 시스템 및 그 방법에 대한 것이다. 비행자료 실시간 보호 시스템은 임베디드 시스템을 제공하며, EWF(Enhanced Write Filter)를 이용하고 OS(Operating System)를 보호하여 시스템을 안전하게 운용할 수 있는 장점을 갖는다.

대표도 - 도1



(72) 발명자

최병철

대전 유성구 배울2로 19, 909동 601호 (관평동, 대
덕테크노밸리9단지아파트)

김용균

서울 용산구 후암로30길 12, 402호 (후암동, 예인
아트빌)

한중옥

대전 유성구 전민로26번길 16, (전민동)

박효달

인천 남구 인하로 100, (용현동, 인하대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호 07항공-항행-03

부처명 한국항공우주연구원

연구사업명 항공선진화사업

연구과제명 비행자료 처리시스템 개발

기 여 율 1/1

주관기관 한국전자통신연구원

연구기간 2007.12.27 ~ 2014.08.22

특허청구의 범위

청구항 1

외부 데이터 공격으로부터 보호하기 위해 원본 비행자료를 필드별로 구분 및 검증하는 비행자료 검증부와,
상기 비행자료 검증부를 통해 검증되는 상기 원본 비행자료를 필드별로 저장하는 비행자료 데이터베이스와,
상기 비행자료 검증부로 입력되는 상기 원본 비행자료의 입출력 메시지를 가로채어 모니터링하는 비행자료 감시부와,
상기 비행자료 감시부로부터 제공되는 감시 결과 메시지에 대응하여 복구를 위한 비행자료를 생성하는 호스트 메시지 감시부와,
상기 호스트 메시지 감시부의 상기 복구를 위한 비행자료에 따라 상기 원본 비행자료를 복구하는 비행자료 복구관리부를 포함하는
비행자료 보호 장치.

청구항 2

제 1 항에 있어서,
상기 비행자료 검증부는,
상기 원본 비행자료에 대해 보안이 필요한 자료와 보안이 필요하지 않은 자료로 각각 구분하는 것을 특징으로 하는
비행자료 보호 장치.

청구항 3

제 2 항에 있어서,
상기 비행자료 검증부는,
상기 보안이 필요한 자료에 대해 세부 필드별 검증을 수행하는 것을 특징으로 하는
비행자료 보호 장치.

청구항 4

제 4 항에 있어서,
상기 비행자료 검증부는,
주요도(Priority) 검증 또는 항공기(Aircraft) ID 검증 또는 항적난기류(Wake Turbulence) 검증 또는 출발공항(Departure Aerodrome) 검증 또는 비행경로(Flight Route) 검증 또는 도착공항(Destination Aerodrome) 검증 중 적어도 하나에 대한 상기 세부 필드별 검증을 수행하는
비행자료 보호 장치.

청구항 5

제 1 항에 있어서,

상기 비행자료 감시부는,
필터 드라이버를 이용하여 상기 원본 비행자료에 대한 모니터링을 수행하는 것을 특징으로 하는
비행자료 보호 장치.

청구항 6

제 5 항에 있어서,
상기 필터 드라이버는,
파일 시스템 드라이버 또는 디스크 드라이버로 전달되는 입력 요청 정보 또는 출력 요청 정보를 가로채는 것을
특징으로 하는
비행자료 보호 장치.

청구항 7

제 1 항에 있어서,
상기 비행자료 검증부는,
임베디드 시스템을 이용하여 원본 비행자료를 필드별로 구분 및 검증하는 것을 특징으로 하는
비행자료 보호 장치.

청구항 8

비행자료 검증부를 통해 원본 비행자료를 필드별로 구분하는 과정과,
필드별로 구분되는 원본 비행자료를 주요도 검증 또는 항공기 ID 검증 또는 항적난기류 검증 또는 출발공항 검
증 또는 비행경로 검증 또는 도착공항 검증 중 적어도 하나를 수행하는 과정과,
검증이 완료되는 원본 비행자료를 필드별로 저장하는 과정을 포함하는
비행자료 보호 방법.

청구항 9

제 8 항에 있어서,
상기 구분하는 과정은,
상기 원본 비행자료에 대해 보안이 필요한 자료와 보안이 필요하지 않은 자료로 각각 구분하는 과정을 포함하는
비행자료 보호 방법.

청구항 10

제 8 항에 있어서,
상기 수행하는 과정은,
임베디드 시스템을 이용하여 원본 비행자료를 필드별로 검증하는 과정을 포함하는

비행자료 보호 방법.

청구항 11

비행자료 검증부로 입력되는 원본 비행자료의 입출력 메시지를 비행자료 감시부가 가로채어 모니터링하는 과정과,

상기 모니터링 결과에 대응하여 복구를 위한 비행자료를 호스트 메시지 감시부를 통해 생성하는 과정과,

상기 복구를 위한 비행자료에 따라 비행자료 복구 관리부를 통해 비행자료를 복구하는 과정을 포함하는 비행자료 보호 방법.

명세서

기술분야

- [0001] 본 발명은 비행자료 보호 기술에 관한 것으로, 특히 내부 혹은 외부로 비행자료의 전송과 같은 관제 서비스를 제공하는데 있어 가용성, 신뢰성 및 무결성을 높여 비행자료 처리 시스템 운영을 방해하는 다양한 사이버 테러에 대응하여 비행자료의 위조 및 변조를 감시하고 자동으로 재해복구를 제공하는 비행자료 보호 장치 및 방법에 관한 것이다.

배경기술

- [0002] 비행관제에 있어 핵심이 되는 비행자료 처리 시스템은 다양한 국가와 다양한 비행자료를 처리해야 하기 때문에 그 데이터 량이 방대하며, 특정 다수에 의해 사용되는데 비해 내/외부의 공격은 다양화, 지능화되어 응용계층, 특히 비행자료처리 시스템 전체에 대해 위협이 증대되고 있는 실정이다.
- [0003] 특히, 기존 시스템인 방화벽, SSL(Secure Socket Layer), IDS(Intrusion Detection System)/IPS(Intrusion Prevention System), VPN(Virtual Private Network), 보안 OS(Operating System) 등을 이용하여 네트워크 계층에서의 방어를 한다 하더라도 내부 공격자로부터 자료 위/변조에 대해 자유롭지 못하며, 이와 같은 네트워크 계층의 보안이라 할지라도 어플리케이션 계층에서의 위협은 산재되어 있는 실정이다.
- [0004] 이러한 위협은 비행자료처리 시스템 전체 마비에 따른 관제 서비스 중단, 비행사고와 같은 인명 피해, 국가 공신력 및 신뢰성 실추, 피해복구에 따른 경제적 손실등과 같이 많은 피해가 발생할 수 있다.
- [0005] 종래에는, 시스템 취약의 다양성과 해킹 등 다양한 사이버테러 및 내부 공격자들로 인해 비행자료 처리 시스템을 보호할 수 없을 뿐만 아니라, 현재의 비행 망이 폐쇄 망이라 할지라도 각 국가가 모두 동일한 보안수준을 갖추고 있지 못하며, 동일한 보안 수준이라 할지라도 내부 위협자들 및 외부 해킹으로부터 자유로울 수 없다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국등록특허 10-0748246호, 침입탐지 로그수집 엔진과 트래픽 통계수집 엔진을 이용한 다단계 통합보안 관리 시스템 및 방법, 2007.08.03 등록

발명의 내용

해결하려는 과제

- [0007] 이에 본 발명의 실시예에서는, 네트워크상에 설치되어있는 비행자료 처리 시스템이 다양한 해킹 및 사이버테러

에 대하여 실시간으로 감시하여 비행자료 처리 시스템의 변조 및 수정이 발생할 경우 자동으로 재해 복구하여 관제 서비스를 중단 없이 제공할 수 있는 비행자료 보호 기술을 제공하고자 한다.

과제의 해결 수단

- [0008] 본 발명의 실시예에 따른 비행자료 보호 장치는, 외부 데이터 공격으로부터 보호하기 위해 원본 비행자료를 필드별로 구분 및 검증하는 비행자료 검증부와, 상기 비행자료 검증부를 통해 검증되는 상기 원본 비행자료를 필드별로 저장하는 비행자료 데이터베이스와, 상기 비행자료 검증부로 입력되는 상기 원본 비행자료의 입출력 메시지를 가로채어 모니터링하는 비행자료 감시부와, 상기 비행자료 감시부로부터 제공되는 감시 결과 메시지에 대응하여 복구를 위한 비행자료를 생성하는 호스트 메시지 감시부와, 상기 호스트 메시지 감시부의 상기 복구를 위한 비행자료에 따라 상기 원본 비행자료를 복구하는 비행자료 복구 관리부를 포함할 수 있다.
- [0009] 여기서, 상기 비행자료 검증부는, 상기 원본 비행자료에 대해 보안이 필요한 자료와 보안이 필요하지 않은 자료로 각각 구분하는 것을 특징으로 할 수 있다.
- [0010] 또한, 상기 비행자료 검증부는, 상기 보안이 필요한 자료에 대해 세부 필드별 검증을 수행하는 것을 특징으로 할 수 있다.
- [0011] 또한, 상기 비행자료 검증부는, 주요도(Priority) 검증 또는 항공기(Aircraft) ID 검증 또는 항적난기류(Wake Turbulence) 검증 또는 출발공항(Departure Aerodrome) 검증 또는 비행경로(Flight Route) 검증 또는 도착공항(Destination Aerodrome) 검증 중 적어도 하나에 대한 상기 세부 필드별 검증을 수행할 수 있다.
- [0012] 또한, 상기 비행자료 감시부는, 필터 드라이버를 이용하여 상기 원본 비행자료에 대한 모니터링을 수행하는 것을 특징으로 할 수 있다.
- [0013] 또한, 상기 필터 드라이버는, 파일 시스템 드라이버 또는 디스크 드라이버로 전달되는 입력 요청 정보 또는 출력 요청 정보를 가로채는 것을 특징으로 할 수 있다.
- [0014] 또한, 상기 비행자료 검증부는, 임베디드 시스템을 이용하여 원본 비행자료를 필드별로 구분 및 검증하는 것을 특징으로 할 수 있다.
- [0015] 본 발명의 실시예에 따르면, 비행자료 검증부를 통해 원본 비행자료를 필드별로 구분하는 과정과, 필드별로 구분되는 원본 비행자료를 주요도 검증 또는 항공기 ID 검증 또는 항적난기류 검증 또는 출발공항 검증 또는 비행경로 검증 또는 도착공항 검증 중 적어도 하나를 수행하는 과정과, 검증이 완료되는 원본 비행자료를 필드별로 저장하는 과정을 포함하는 비행자료 보호 방법을 제공할 수 있다.
- [0016] 여기서, 상기 구분하는 과정은, 상기 원본 비행자료에 대해 보안이 필요한 자료와 보안이 필요하지 않은 자료로 각각 구분하는 과정을 포함할 수 있다.
- [0017] 또한, 상기 수행하는 과정은, 임베디드 시스템을 이용하여 원본 비행자료를 필드별로 검증하는 과정을 포함할 수 있다.
- [0018] 본 발명의 실시예에 따르면, 비행자료 검증부로 입력되는 원본 비행자료의 입출력 메시지를 비행자료 감시부가 가로채어 모니터링하는 과정과, 상기 모니터링 결과에 대응하여 복구를 위한 비행자료를 호스트 메시지 감시부를 통해 생성하는 과정과, 상기 복구를 위한 비행자료에 따라 비행자료 복구 관리부를 통해 비행자료를 복구하는 과정을 포함하는 비행자료 보호 방법을 제공할 수 있다.

발명의 효과

- [0019] 본 발명에 의하면, 비행자료 처리 시스템에서 발생하는 사이버테러 또는 악성변화에 대해 비행자료 처리 시스템의 가용성을 최대화시키고, 비행자료 처리 시스템의 정지시간 동안 안정적으로 관제 서비스를 제공할 수 있다. 본 발명은 다양한 공격들(예를 들어, 사이버테러, 내부자 공격, 파일 위/변조 등)에 대해 비행자료에 대한 처리 및 복구가 가능하며, 이벤트 로그를 이용하여 추후 이에 대한 분석을 통해 동일한 공격형태를 예방할 수 있다. 또한, 본 발명은 비행자료 변조로부터 복구가 수동이나 갑작스런 초기상태로의 복구가 아닌 자동으로 실시간 복구되어 복구 비용 측면뿐만 아니라 국가 신뢰도 및 인명피해를 사전에 예방할 수 있다.

도면의 간단한 설명

[0020]

도 1은 본 발명의 실시예에 따른 비행자료 보호 장치를 포함하는 비행자료 보호 시스템에 대한 블록도,

도 2는 본 발명의 실시예에 따른 비행자료 보호 과정을 예시적으로 설명하는 흐름도,

도 3은 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 정보 사건을 획득하여 실시간 자동 재해 복구를 구현하는 과정을 예시한 흐름도,

도 4는 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 정보 사건을 생성하여 비행자료의 원본을 보관하는 과정을 예시한 흐름도,

도 5는 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 감시부(112)의 처리 과정을 예시한 흐름도,

도 6은 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 복구 과정을 예시한 흐름도.

발명을 실시하기 위한 구체적인 내용

[0021]

본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 도면부호는 동일 구성 요소를 지칭한다.

[0022]

본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0023]

첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조품을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0024]

또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또한, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0025]

실시예의 설명에 앞서, 본 발명은 해커의 침입 혹은 사이버 테러로 인해 비행자료 처리 시스템에서 서비스 또는 비행자료가 삭제되거나 변조 또는 수정되면 실시간으로 자동 재해복구 시스템에게 비행자료 처리 시스템의 변화를 통보하고 복구가 자동으로 진행되도록 한다는 것으로, 이러한 기술 사상으로부터 본 발명의 목적으로 하는

바를 용이하게 달성할 수 있을 것이다.

- [0026] 이하, 첨부된 도면을 참조하여 본 발명의 실시예에 대해 상세히 설명하기로 한다.
- [0027] 도 1은 본 발명의 실시예에 따른 비행자료 보호 장치에 대한 블록도로서, 비행자료 검증부(100), 임베디드(embedded) 시스템부(102), 비행자료 사전부(dictionary module)(104), 비행자료 복구 관리부(recovery management module)(106), 호스트 메시지 감시부(108), 비행자료 DB(Database)(110), 비행자료 감시부(112) 등을 포함할 수 있다.
- [0028] 비행자료 검증부(100)는 악의적인 공격으로부터 비행자료를 보호하기 위해 원본 비행자료를 필드별로 구분하고 검증하는 역할을 할 수 있다. 예컨대, 비행자료 검증부(100)는 입력되는 비행자료에 대해 보안이 필요한 자료와 보안이 필요하지 않은 자료로 구분하고, 보안이 필요한 자료를 세부 필드별로 구분한 후 검증을 수행할 수 있다. 비행자료 검증부(100)를 통해 검증이 완료되는 비행자료는 필드별로 구분되어 비행자료 DB(110)에 저장될 수 있다.
- [0029] 임베디드 시스템부(102)는 비행자료 검증부(100)를 통해 비행자료가 필드별로 구분 및 결합될 수 있도록 적절한 임베디드 시스템을 저장하고 있다.
- [0030] 비행자료 사전부(104)는 원본 비행자료를 저장하고, 저장된 원본 비행자료를 복제할 수 있다.
- [0031] 비행자료 복구 관리부(106)는 원본 비행자료를 각 상황에 맞도록 복구하고, 이벤트 로그를 저장하는 역할을 할 수 있다.
- [0032] 호스트 메시지 감시부(108)는 후술하는 비행자료 감시부(112)를 통해 제공되는 감시 결과 메시지에 대응하여 복구를 위한 비행자료를 비행자료 복구 관리부(106)로 제공할 수 있다. 이러한 호스트 메시지 감시부(108)는 각 상황에 따라 복구를 위한 비행자료 전송 및 비행자료 감시부(112)와의 연결 매개체가 될 수 있다.
- [0033] 비행자료 DB(110)에는 비행자료 검증부(100)를 통해 필드별로 구분되어 제공되는 비행자료가 저장될 수 있다.
- [0034] 비행자료 감시부(112)는 필터 드라이버(filter driver)를 이용하여 입력되는 원본 비행자료에 대한 모니터링을 수행할 수 있다. 예컨대, 비행자료 감시부(112)는 파일 시스템 드라이버 또는 디스크 드라이버 등으로 전달되는 입/출력 요청 정보를 가로채어 기존의 드라이버가 제공하는 기능을 보완하거나 새로운 기능을 추가할 수 있다. 이러한 비행자료 감시부(112)는 데몬 형태로 상주하여 비행자료의 이상 여부를 감시할 수 있다.
- [0035] 이와 같은 비행자료 보호 장치는, 외부 네트워크를 통해 감시 결과 메시지가 전송되며, 각 상황에 따라 복구를 위한 비행자료 전송 및 시스템의 데몬과 호스트의 에이전트의 연결 매개체가 된다.
- [0036] 비행자료 보호 장치의 구성들 중 임베디드 시스템부(102), 비행자료 DB(110), OS 저장소 모듈(도시 생략됨), 비행자료 사전부(104)는 EWF(Enhanced Write Filter)로 쓰기 방지를 하여 시스템을 보호하며, 이를 통해 시스템의 가용성, 신뢰성 및 무결성을 높일 수 있다.
- [0037] 이하, 상술한 구성과 함께, 본 발명의 실시예에 따른 비행자료 보호 방법을 첨부한 도 2 내지 도 6의 흐름도를 참조하여 상세히 설명하기로 한다.
- [0038] 먼저, 도 2는 본 발명의 실시예에 따른 비행자료 보호 과정을 예시적으로 설명하는 흐름도이다.
- [0039] 본 과정은 비행자료 검증부(100)로 비행자료가 입력됨으로써 진행될 수 있다. 모든 비행전문은 그 이력에 따라 구분 작업을 거쳐야 한다. 이때, 구분 작업은 검증된 자료에 대해서 이루어지며, 구분된 각 데이터는 분석 및 사고 발생시 사용하게 된다.
- [0040] 도 2에 도시한 바와 같이, 비행자료를 입력 받아(S100), 비행자료를 큰 항목별로 분리하며(S102), 보안이 필요한 자료와 필요하지 않은 자료를 분리하고(S104), 보안이 필요하지 않은 자료는 외부로 처리할 수 있다(S106).
- [0041] 보안이 필요한 자료는 다시 세부 필드로 분리 작업을 진행할 수 있다(S108).
- [0042] 이후, 분리된 세부 필드에 대해 검증 과정을 진행할 수 있다(S110). 검증 과정은, 예컨대 주요도(Priority) 검증, 항공기(Aircraft) ID 검증, 항적난기류(Wake Turbulence) 검증, 출발공항(Departure Aerodrome) 검증, 비행경로(Flight Route) 검증, 도착공항(Destination Aerodrome) 검증 등을 포함할 수 있다.

- [0043] 모든 검증이 완료되면 세부 필드로 분리하여 저장할 수 있다(S112).
- [0044] 도 3은 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 정보 사건을 획득하여 실시간 자동 재해 복구를 구현하는 과정을 예시한 흐름도이다.
- [0045] 도 3에 도시한 바와 같이, 비행자료 보호 방법은, 비행자료 사건을 호스트로부터 정보를 얻어서 진행하며(S200), 호스트의 비행자료 감시부(108)를 통해 비행자료를 감시하고(S202), 시스템 이벤트 발생시 파일을 후킹(Hooking)하여 파일의 삭제, 위조, 변조(S204) 또는 시스템에 새로운 비행자료가 생성되면 호스트 메시지 감시부(108)에 비행자료를 전달(S206)(S208)하여 복구모듈을 작동시키고(S210), 각 상황에 맞도록 처리 후, 이벤트 로그를 저장하고(S212) 처리상황을 복구관리자에게 알려줄 수 있다(S214). 이때, 처리상황은 전자메일(email), SMS 등을 통해 관리자에게 통보될 수 있다.
- [0046] 도 4는 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 정보 사건을 생성하여 비행자료의 원본을 보관하는 과정을 예시한 흐름도이다.
- [0047] 도 4에 도시한 바와 같이, 비행자료 정보 사건을 생성하는 본 과정은 비행자료의 원본을 보관하는 것이다.
- [0048] 최초 항공고정통신망(Aeronautical Fixed Telecommunication Network, AFTN)을 통해 들어온 비행자료(S300), 혹은 입력된 비행자료에 대해 데이터를 저장(S302)한다.
- [0049] 이때, 저장할 수 있는 권한은 전적으로 관리자에게 있으며, 저장된 비행자료는 비행자료 보호 장치의 비행자료 DB(110)에 복제 혹은 복사될 수 있다(S304)(S306).
- [0050] 도 5는 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 감시부(112)의 처리 과정을 예시한 흐름도이다.
- [0051] 도 5에 도시한 바와 같이, 비행자료 감시부(112)는 입출력 요청 패킷(I/O request packet)을 감시한다.
- [0052] 비행자료 감시부(112)는 기본적으로 필터 드라이버를 이용하며, 필터 드라이버는 파일 시스템 드라이버나 디스크 드라이버와 같은 드라이버에 전달되는 I/O 요청을 가로채어(S400), 기존의 드라이버가 제공하는 기능을 보완하거나 새로운 기능을 추가할 수 있는 형태이다.
- [0053] 비행자료의 요청이나 처리된 비행자료의 요청이 있는 경우, 요청에 대하여 처리된 비행자료를 전송하는 경우 각각 가로채어 정당한 요청과 정당한 처리결과인지 모니터링할 수 있다(S402).
- [0054] 파일 후킹을 진행하여 파일 변조 및 삭제 여부를 확인하고(S404), 이상 발생시 호스트 메시지 감시부(108)에 시스템 메시지(즉, 감시 결과 메시지)를 전송(S406)함으로써, 호스트 메시지 감시부(108)는 각 상황에 맞도록 프로세스를 실행할 수 있다.
- [0055] 이때, 실행되는 프로세스는 다음과 같은 절차를 따른다.
- [0056] 비행자료 보호 장치에서 데몬 형태로 있으면서 호스트 및 비행자료 처리 장치의 에이전트가 보내는 메시지를 분석(S414)하여 각 상황에 맞는 프로세스를 실행할 수 있다.
- [0057] 마지막으로 비행자료 사건부(104)에서 기존 변조가 있는 비행자료와 비교 검색할 수 있다(S408). 이때, 이상이 발생한 경우 각 상황에 맞춰 복구형태를 결정하며, 실시간 비행자료 복구시스템이 복구될 수 있다(S412).
- [0058] 도 6은 본 발명의 실시예에 따른 비행자료 보호 방법으로서, 비행자료 복구 과정을 예시한 흐름도이다.
- [0059] 도 6은 비행자료 복구 관리부(106)에서 처리되는 과정으로, 비행자료에 대해 이상이 발생한 경우 비행자료 사건과 비교하여 처리를 진행할 수 있다(S500).
- [0060] 비행자료의 삭제가 발생한 경우(S502), 비행자료 유(110)에서 원본복제 파일을 검색하여 장애가 발생된 시점으로 비행자료를 전송하여 복구하며, 불법적인 비행자료 추가가 발생한 경우 비행자료에 대한 삭제를 진행할 수 있다(S504).

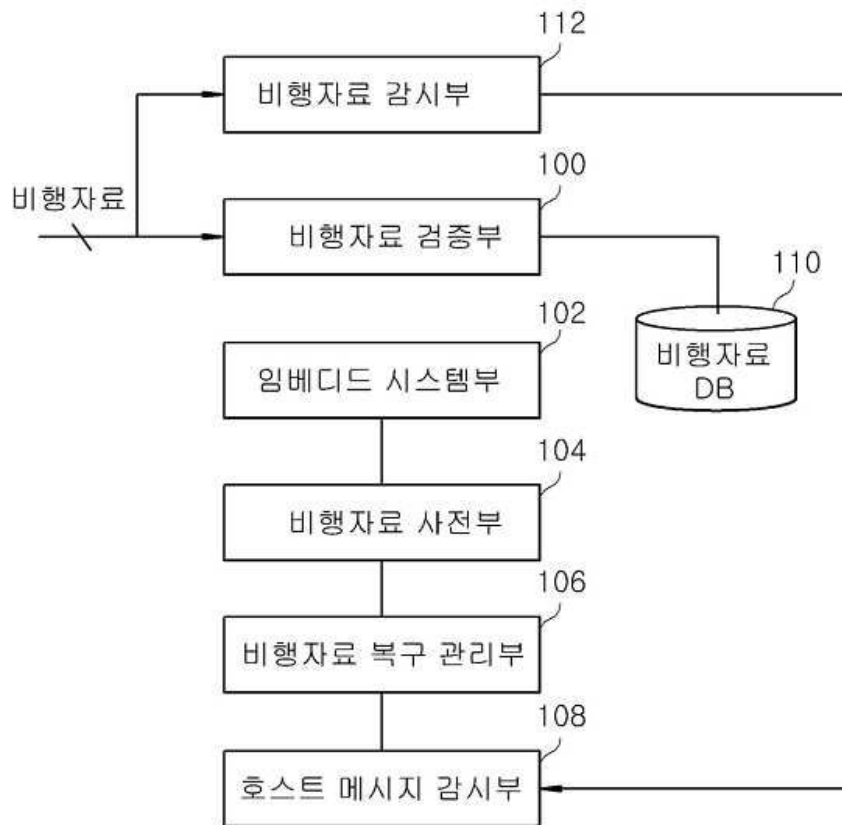
- [0061] 비행자료 수정 및 변조가 발생한 경우(S506), 이상 비행자료는 삭제하고 원본 복사 파일을 전송하여 시스템을 복구할 수 있다(S508).
- [0062] 비행자료 첨부 및 비행자료 수정의 경우(S510), 각 상황(예를 들어, 이상적인 행위, 비이상적인 행위)에 대처하고(S512), 각 비행자료를 검역소에 저장하여 차후의 문제를 동일 패턴에 대해 처리하도록 한다(S514).
- [0063] 이상 설명한 바와 같은 본 발명의 실시예에 의하면, 네트워크상에 설치되어있는 비행자료 처리 시스템이 다양한 해킹 및 사이버테러에 대하여 실시간으로 감시하여 비행자료 처리 시스템의 변조 및 수정이 발생할 경우 자동으로 재해 복구하여 관제 서비스를 중단 없이 제공할 수 있는 비행자료 보호 기술을 제공하고자 한다.

부호의 설명

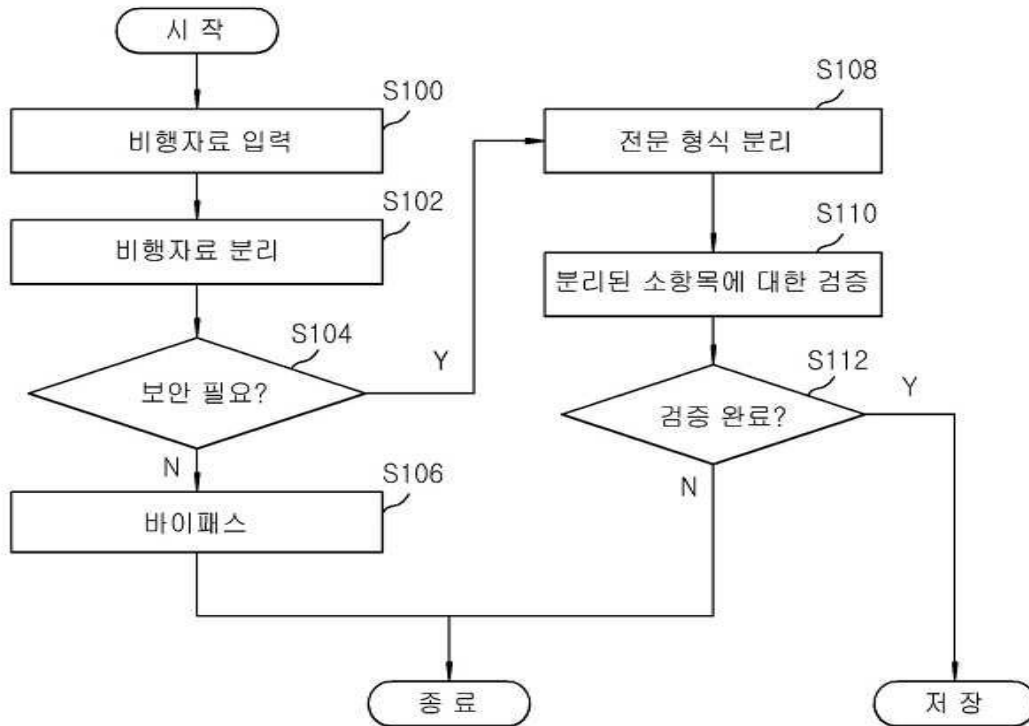
- [0064] 100: 비행자료 검증부
102: 임베디드 시스템부
104: 비행자료 사전부
106: 비행자료 복구 관리부
108: 호스트 메시지 감시부
110: 비행자료 DB
112: 비행자료 감시부

도면

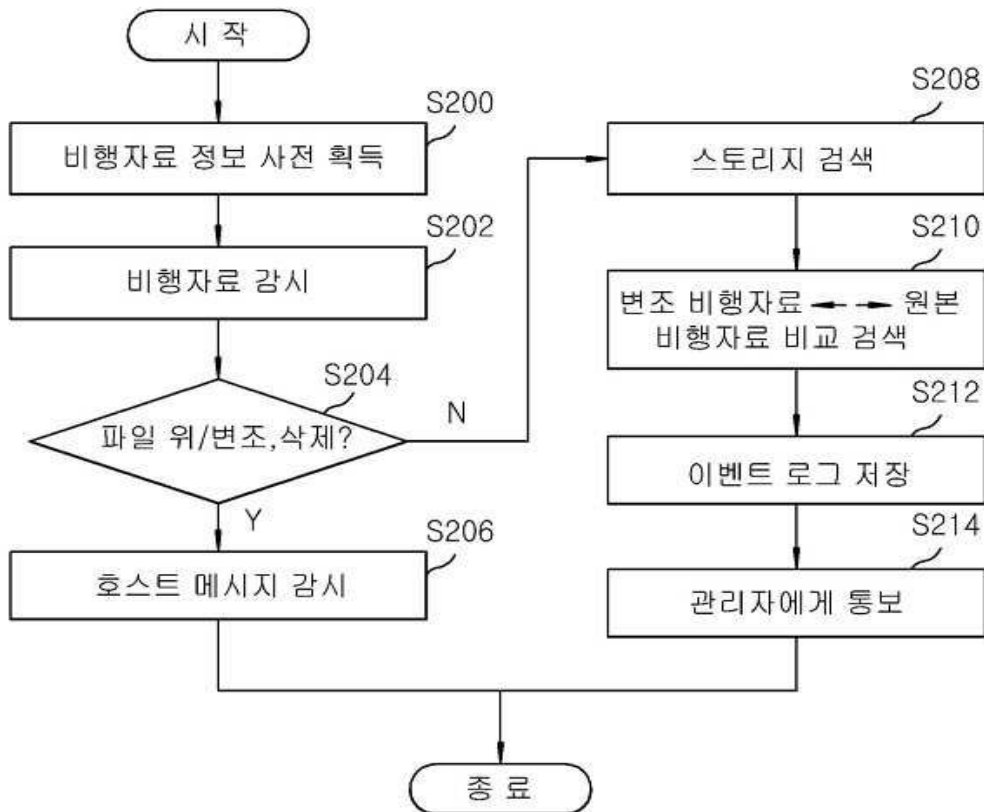
도면1



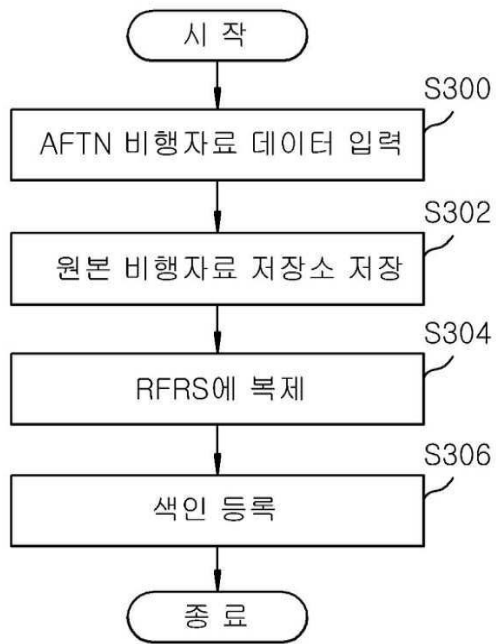
도면2



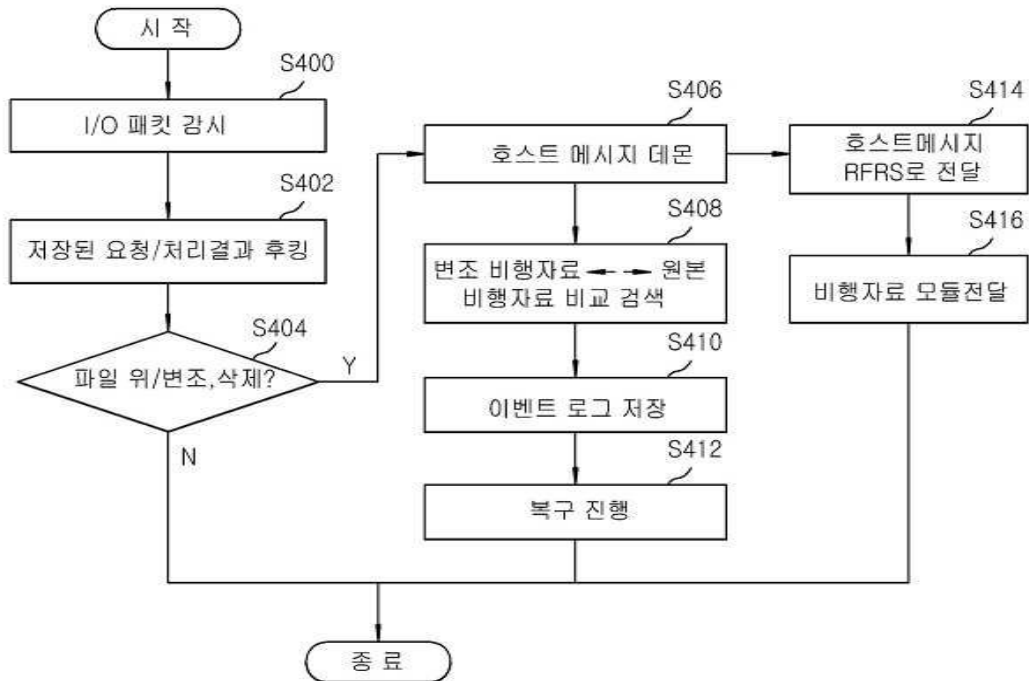
도면3



도면4



도면5



도면6

