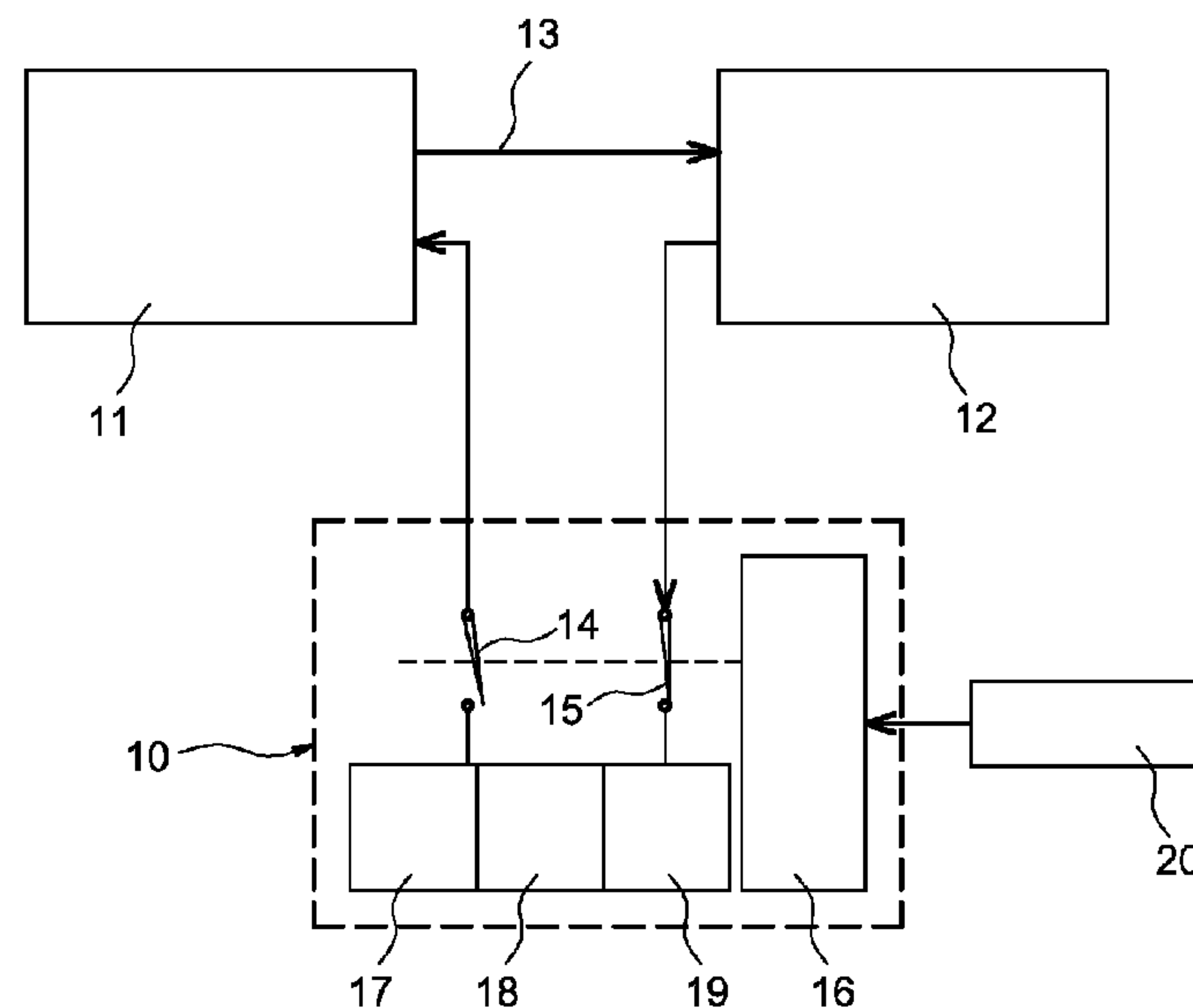




(86) **Date de dépôt PCT/PCT Filing Date:** 2008/06/03
(87) **Date publication PCT/PCT Publication Date:** 2008/12/11
(45) **Date de délivrance/Issue Date:** 2016/04/12
(85) **Entrée phase nationale/National Entry:** 2009/12/01
(86) **N° demande PCT/PCT Application No.:** EP 2008/056844
(87) **N° publication PCT/PCT Publication No.:** 2008/148756
(30) **Priorité/Priority:** 2007/06/06 (FR07 55514)

(51) **Cl.Int./Int.Cl.** *H04L 9/32* (2006.01),
B64D 47/00 (2006.01), *G06F 21/31* (2013.01),
G06F 21/85 (2013.01)
(72) **Inventeur/Inventor:**
GENISSEL, JEAN-PAUL, FR
(73) **Propriétaire/Owner:**
AIRBUS OPERATIONS, FR
(74) **Agent:** GOUDREAU GAGE DUBUC

(54) **Titre : SYSTEME DE CONTROLE D'ACCES EMBARQUE SERVANT A LA COMMUNICATION ENTRE LE DOMAINE OUVERT ET
LE DOMAINE DE L'AVIONIQUE**
(54) **Title: ONBOARD ACCESS CONTROL SYSTEM FOR COMMUNICATION FROM THE OPEN DOMAIN TO THE AVIONICS
DOMAIN**



(57) **Abrégé/Abstract:**

An onboard access control system to an information system onboard an aircraft, for communication from the open domain to the avionics domain, the open end avionics domains being connected to each other through a single-directional link from the avionics domain to the open domain. The system includes: a security device including: access switches controlling access to the avionics and open domains, a controller, a module for acquisition putting data into buffer memory and transmission to the avionics domain, a data control module, an acquisition module from the open domain and putting into buffer memory, and an operator's authentication mechanism.

ABSTRACT

An onboard access control system to an information system onboard an aircraft, for communication from the open domain to the avionics domain, the open end avionics domains being connected to each other through a single-directional link from the avionics domain to the open domain. The system includes: a security device including: access switches controlling access to the avionics and open domains, a controller, a module for acquisition putting data into buffer memory and transmission to the avionics domain, a data control module, an acquisition module from the open domain and putting into buffer memory, and an operator's authentication mechanism.

**ONBOARD ACCESS CONTROL SYSTEM FOR COMMUNICATION FROM THE
OPEN DOMAIN TO THE AVIONICS DOMAIN**

TECHNICAL FIELD

5

The invention relates to an onboard access control system for communication from the open domain to the avionics domain. This system may be placed onboard an aircraft, for example a plane.

10

STATE OF PRIOR ART

An onboard information system is a system composed of two "domains": the avionics domain (AW), that
15 satisfies clearly defined certification rules, and the open domain (OW), based on general public computer components. At the present time, this communication is only authorised in the direction from the avionics domain to the open domain, subsequent to data processing
20 security directives. Nevertheless, there is a need to communicate in both directions and this need has become imperative in the interest of the system.

The Avionics Domain

25

The avionics domain is dedicated to avionics computers that process all avionics functions including critical functions such as flight controls.

The avionics domain must be protected against data
30 processing attacks in order to guarantee its integrity and thus guarantee operating reliability. Avionics equipment is developed in agreement with aerial

navigability rules and regulations dictated by official services, thus guaranteeing flight safety. The secure domain must be protected against uncontrolled intrusion attempts that could originate from the open domain.

5

The avionics domain is dedicated to processing a number of items including: everything necessary for immediate operations contributing to operational use of the aircraft and good flight control; everything
10 necessary for flight preparation for good operational use; acquisitions of some "sensitive" data originating from the ground.

The Open Domain

15 The "open" domain includes an application server supplying a host capacity for maintenance applications, operational applications and passenger cabin applications that have no impact on flight safety. An onboard Ethernet local network in the aircraft enables information
20 exchanges between the different components of the open domain. The open domain may also communicate with an information system belonging to the airline company based on the ground, through a high speed satellite communication.

25

This domain is considered to be "open" because it is open to every operator. It is considered as being uncontrolled, because it uses general public components and data processing standards: Ethernet local networks,
30 COTS (Components Off The Shelf) software and hardware.

The computer security elements used must guarantee that any viruses and/or attacks of any type cannot be propagated.

5 The "open" domain provides:

 low cost solutions, for example market solutions, to reduce the complexity related to security, safety and availability;

 maximum flexibility for the operator who wishes
10 to install his own applications ("Third party applications") with a minimum involvement or even no involvement by the aircraft manufacturer, thus limiting implementation costs and times;

 ease of installation of applications for which
15 the airline is responsible, satisfying operational rules (FAR 121, FAR 145...);

 a capacity to accommodate non-major functions/applications for immediate operations.

20 Another purpose of the invention is to take account of needs and general and specific objectives of an onboard information system particularly related to data security, safety, performances, installation, configuration and aircraft certification, by providing an
25 onboard access control system enabling secure communication from the open domain to the avionics domain, so as to enable two-directional communications between the avionics domain and the open domain.

PRESENTATION OF THE INVENTION

The invention relates to an onboard system controlling access to an information system, onboard an aircraft, comprising an avionics domain satisfying
5 clearly defined certification rules, and an open domain based on general public components accessible to all operators, these two domains being connected to each other through a single-directional link from the avionics
10 domain to the open domain for security reasons, characterised in that it comprises:

operator authentication means,

a security device comprising:

15 a set of two access switches controlling access to each of these two domains, operating like an electronic lock,

a controller that controls opening of these two switches for durations that depend on the operator's profile,

20 a module for acquisition, putting data originating from the open domain into buffer memory and transmission to the avionics domain,

an acquisition module acquiring data from the open domain and putting it into buffer memory,

25 a data control module that defines filter criteria applicable to all exchanges between buffer memories,

to enable secure communication from the open domain to the avionics domain and thus allow two-directional
30 communications between these two domains.

In a first variant, the operator authentication means comprise means of reading electronic cards, biometric means or code reading means.

5 In a second variant, the operator authentication means comprise a secure link between the aircraft and the ground enabling an operator located on the ground to authenticate himself, this link then being connected to the controller.

10

Advantageously, the switches are hardware switches.

The control module may include protection mechanisms in the network, transport and application layers of the
15 OSI model. Advantageously, the control module includes encryption means. The control module may be configured by a data filtering table.

Advantageously, the protocols used in each of these
20 two avionics and open domains are different and participate in increasing the security of data exchanges between these two domains.

BRIEF DESCRIPTION OF THE DRAWINGS

25

FIG. 1 shows the onboard access control system according to the invention.

FIG. 2 is a flowchart illustrating an example of how
30 the onboard access control system according to the invention operates.

DETAILED PRESENTATION OF PARTICULAR EMBODIMENTS

As shown in FIG. 1, the onboard access control system according to the invention is connected between
5 the avionics domain 11 and the open domain 12. These two domains 11 and 12 are conventionally connected by a single-directional link 13 in the direction from the avionics domain 11 towards the open domain 12.

10 The system according to the invention comprises:
a security device 10 comprising:
hardware switches 14 and 15 providing access to each of these two domains,
a controller 16,
15 a module 17 for acquisition, buffer memorisation and transmission to the avionics domain 11,
a data control module ("firewall") 18, and
an acquisition module 19 for data from the open
20 domain 12 and for buffer memorisation, operator authentication means 20.

In a first variant, the operator authentication means consist of an authentication device that for
25 example includes means of reading electronic card, biometric means or code reading means.

In a second variant, the operator authentication means comprise a secure link between the aircraft and the
30 ground enabling an operator located on the ground to authenticate himself, this link then being connected to the controller 16.

The onboard access control system according to the invention is similar to an "electronic lock" comprising an access switch to each avionics domain and to the open domain. Data can pass from one domain to the other when the access switch to the other domain is closed, thus preventing any permanent physical link between the two domains and can give protected communications between these two domains.

10

Opening and closing of the two hardware switches 14 and 15 are controlled by the security device 10 after the operator has been authenticated. This security device 10 allows a secure link in the opposite direction of the link 13, from the open domain 12 to the avionics domain 11.

The volume of data transmitted is determined based on the capacity of the two acquisition, buffer memorisation and transmission modules 17 and 19.

Due to the security device 10, the link from the open domain to the avionics domain is always open, which prevents permanent access to the avionics domain, limiting or even prohibiting access of any malicious intruder.

This security device 10 has the following functions.

30 Controller 16

The controller 16 accepts authentication of the operator and defines rules used by the security device 10

that operates as a function of the operator's profile. The controller 16 configures the security device 10 as a function of operators to make the connection between the open domain and the avionics domain. In particular, the
5 controller 16 assigns a time window that depends on the operator's profile, during which communication is possible. To achieve this, it controls opening of access switches 14 and 15 for durations that depend on the operator's profile determined during authentication of
10 the operator.

Access Module 19

The access module 19 to the open domain 12 takes account of use of a first protocol and stores data
15 originating from the open domain 12 in buffer memory.

Access Module 17

The access module 17 to the avionics domain 11 allows for the use of a second protocol and stores data
20 originating from the open domain 12 in buffer memory (through control module 18) so that they can be transmitted to the avionics domain 11.

Control Module 18

25 The control module 18 provides protection between the open domain 12 and the avionics domain 11. In particular, it performs a firewall function. To achieve this, it can be configured by a loaded data filtering table in which filter criteria are defined and are
30 applicable to all exchanges between buffer memories. This control module 18 checks the data integrity.

The security level to be applied is determined as a function of the type of data to be transferred. Examples of risks to be taken into account are particularly attacks by intruders, commercial espionage, accidental
5 disclosure of company data (users, employees and company data) and service denial attacks.

The first and second protocols are chosen from among protocols well known to those skilled in the art. They
10 may be different and thus participate in securing data exchanges between the open domain 12 and the avionics domain 11.

Such a control module 18 conventionally includes
15 protection mechanisms for the following layers of the OSI ("Open System Interconnection") model:

network layer,
transport layer,
application layer.

20

It may use encryption to enable confidentiality, authentication and to improve integrity.

Access Switches 14 and 15

25 Controller 16 manages opening and closing of access switches 14 and 15. They operate like an electronic lock in which data can pass from one domain to the other only when the switch in the opposite domain is closed, which prevents any physical link between the two domains.

30

A process in which data are transmitted between the open domain 12 and the avionics domain 11 includes the following steps:

5 - Operator Authentication

The controller 16 acquires data transmitted by the operator authentication device 20 and allocates rights as a function of the user's profile, with the following steps:

10 close the open domain access switch 15,
 initialise the first protocol,
 store data in buffer memory.

 - Store data in Buffer Memory

15 store data in buffer memory, in module 19 from which all prior data have been removed, for all candidate data to be transmitted,
 open the open domain access switch 15.

20 - Checking/Filtering Data

transmit data stored in buffer memory to the control module 18,

filter data as a function of determined filter criteria.

25

 - Store Authorised Data in Buffer Memory

check that switches 14 and 15 controlling access to the avionics domain 11 and the open domain 12 are open and closed respectively,

30 transmit data to the buffer memorisation module 17, after all previous data have been deleted,
 erase memories in module 19,

close the avionics domain access switch 14 (the open domain access switch 15 being open),

initialise the second protocol to transfer data from the acquisition module 17 to the avionics domain.

5

FIG. 2 is a flowchart illustrating an example operation of the system according to the invention.

This flowchart includes the following steps:

10 a step 21 to initialise configuration of the system according to the invention; the access switch 15 to the open domain 12 being open and the access switch 14 to the avionics domain 11 being closed,

15 a step 22 to update the system according to the invention receiving an access control configuration 23 and an authentication or access control rules 24,

a test 25 to change the configuration of the system according to the invention with

20 a switch 15 open and switch 14 closed output 26 followed by a step 27 to initialise the second protocol (avionics domain end) and return to step 21,

a switch 15 closed and switch 14 open output 28 followed by

25 a step 29 to initialise the first protocol (open domain end),

a step 30 to store data in buffer memory and to acquire data from the open domain,

30 a step 31 to filter data (firewall function) receiving a data filter configuration 32,

a step 33 to memorise valid data, and
return before the change configuration step 25,
and

a step 34 to erase the buffer memory.

5

Data are transferred between the open domain and the
avionics domain 11 as follows:

output 28 from test 25 is used in the first step;

output 26 from the same test 25 is used in the
10 second step.

CLAIMS

1. An onboard access control system to an information system onboard an aircraft, including an
5 avionics domain satisfying clearly defined certification rules, and an open domain based on general public components accessible to all operators, the open domain operating according to a first communication protocol and the avionics domain operating according to a second
10 communication protocol that is different from the first communication protocol, the system comprising:

a single-directional link that allows communication from the avionics domain to the open domain; and

a secure link for communication from the open domain
15 to the avionics domain, the secure link including

an operator authentication section obtaining an operator's profile, and

a security device comprising

first and second hardware access switches
20 operating as an electronic lock preventing a permanent communication link from the open domain to the avionics domain, the first hardware access switch connected between the open domain and a first access module and the
25 second hardware access switch connected between a second access module and the avionics domain,

a controller that receives the operator's profile and controls opening of the first and second hardware access switches for durations
30 that depend on the operator's profile,

the first access module including a first buffer memory, the first access control module

being configured to receive data from the open domain through the first hardware access switch according to the first communication protocol and store the data originating from the open domain in the first buffer memory, the second access module including a second buffer memory, the second access module being configured to put the data from the first buffer memory into the second buffer memory for subsequent transmission through the second hardware access switch to the avionics domain according to the second communication protocol, a data control module situated between the first and second access modules and configured to define filter criteria applicable to all exchanges between the first and second buffer memories, and the controller is further configured to erase the first buffer memory before closing the second hardware access switch to allow the data from the second buffer memory to be transmitted through the second hardware access switch to the avionics domain according to the second communication protocol.

25

2. A system according to claim 1, in which the operator authentication section comprises an electronic reader, a biometric sensor, or a code reader.

30

3. A system according to claim 1, in which the operation authentication section comprises a secure link between the aircraft and ground to allow an operator on

the ground to identify himself/herself to thereby obtain the operator's profile.

4. A system according to claim 1, in which the
5 data control module includes protection mechanisms in a network, and transport and application layers of an OSI model.

5. A system according to claim 1, in which the
10 data control module includes an encryption unit.

6. A system according to claim 1, in which the
data control module is configured by a data filtering
table.

15

7. A system according to claim 1, in which the
first and second communication protocols used in each of
the avionics and open domains are different and
participate in increasing security of data exchanges
20 between the avionics and open domains.

8. A system according to any one of claims 1 to 7,
in which the aircraft is a plane.

25 9. An aircraft using a system according to claim
1.

1 / 2

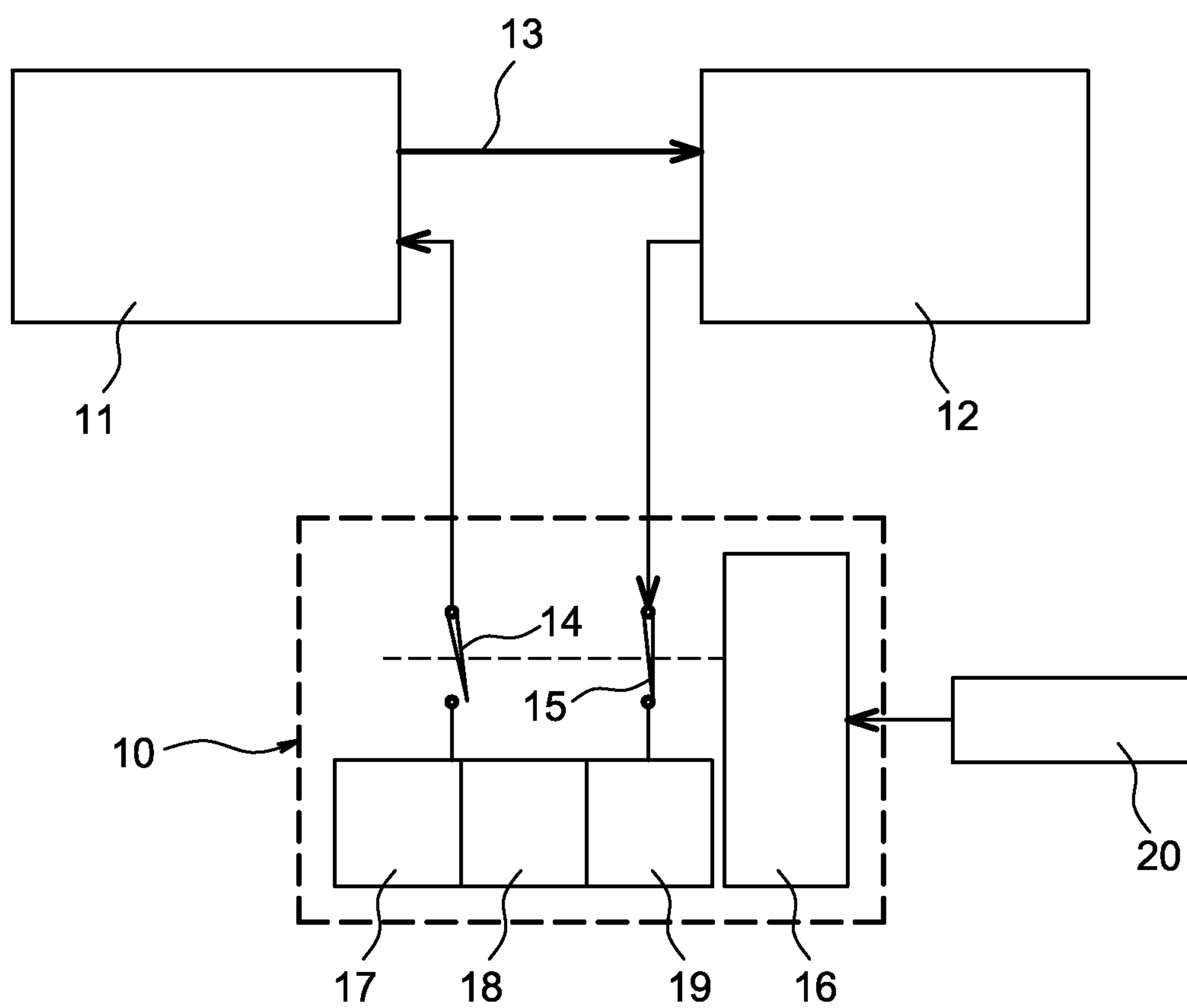


FIG. 1

2 / 2

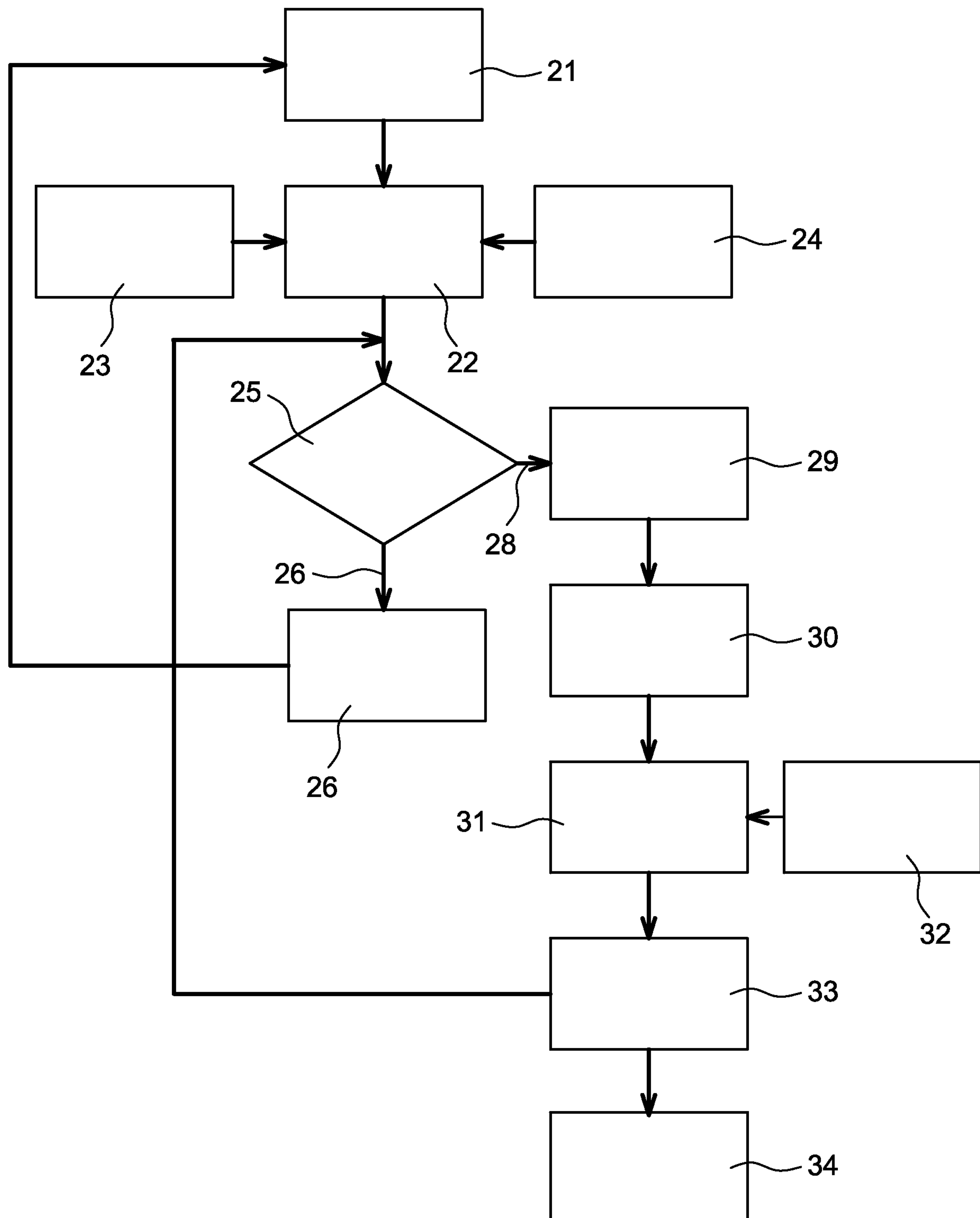


FIG. 2

