

Petitioners Axon Enterprise, Inc. and
Dedrone Holdings, Inc.
Hearing Presentation for IPR2025-00530
U.S. Patent No. 10,249,199

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History**
- II. Dispute Overview**
- III. Substitute Claims 10-18 Lack Written Description**
- IV. Substitute Claims 10-18 are Indefinite**
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C**
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C**
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13**
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14**

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History**
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

(10) **Patent No.:** **US 10,249,199 B2**
(45) **Date of Patent:** **Apr. 2, 2019**

(21) Appl. No.: 15/598,303

(22) Filed: **May 17, 2017**

(65) **Prior Publication Data**

US 2018/0197420 A1 Jul. 12, 2018

Related U.S. Application Data

(60) Provisional application No. 62/309,838, filed on Mar. 17, 2016.

Patent Owner cites the '303 application and '838 Provisional to support the substitute claims

AXON EXHIBIT 1030

US010249199B2

(12) **United States Patent**
Banga

(10) Patent No.: US 10,249,199 B2
(45) Date of Patent: Apr. 2, 2019

(54) **SYSTEM AND METHOD FOR AERIAL SYSTEM DISCRIMINATION AND ACTION**

(2013.01); G08G 5/0043 (2013.01); G08G 5/0069 (2013.01); G08G 5/0082 (2013.01); B64C 2201/12 (2013.01); B64C 2201/141 (2013.01); B64C 2201/146 (2013.01); G01S 19/13 (2013.01)

(71) Applicant: **Airspace Systems, Inc.**, San Leandro, CA (US)

(72) Inventor: **Jasminder S. Banga**, San Francisco, CA (US)

(58) **Field of Classification Search**
CPC G08G 5/006; G08G 5/005
USPC 340/5.61
See application file for complete search history.

(73) Assignee: **Airspace Systems, Inc.**, San Leandro, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 15/598,303

(22) Filed: **May 17, 2017**

(65) **Prior Publication Data**
US 2018/0197420 A1 Jul. 12, 2018

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,218,941 B1	4/2001	Cromer	
9,689,976 B2 *	6/2017	Parker	F41H 11/02
9,792,613 B2 *	10/2017	Gong	H04L 63/101
9,835,709 B2 *	12/2017	Tran	G01S 1/68
2006/0175464 A1	8/2006	Chang	
2007/0239986 A1	10/2007	Viggiano	
2012/0153084 A1	6/2012	Eitzkoen	

(Continued)

FOREIGN PATENT DOCUMENTS

CN 105206114 A 12/2015

Primary Examiner — Qutbuddin Ghulamali
(74) Attorney, Agent, or Firm — Van Pelt, Yi & James LLP

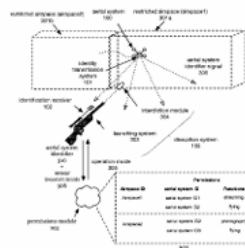
(51)	Int. CL	
	<i>G08G 5/00</i>	(2006.01)
	<i>G01S 13/78</i>	(2006.01)
	<i>B64C 39/02</i>	(2006.01)
	<i>G01S 15/74</i>	(2006.01)
	<i>G06F 21/00</i>	(2013.01)
	<i>G07C 9/00</i>	(2006.01)
	<i>G01S 19/13</i>	(2010.01)

(57) ABSTRACT

An aerial system discrimination system includes an aerial system disruption system, an aerial system identification system, and a permissions module. The discrimination system can additionally include or use an identifier transmission system configured to mount to the aerial system. The discrimination system functions to determine whether an aerial system is authorized or unauthorized to be in the airspace. The discrimination system can additionally function to prevent, disrupt, remove, or otherwise interact with an unauthorized aerial system within the airspace.

(52) U.S. CL
CPC *G08G 5/006* (2013.01); *B64C 39/024*
(2013.01); *G01S 13/78* (2013.01); *G01S 15/74*
(2013.01); *G06F 21/00* (2013.01); *G07C*
9/00111 (2013.01); *G08G 5/008* (2013.01);
G08G 5/0013 (2013.01); *G08G 5/0026*

9 Claims, 6 Drawing Sheets



AXON EXHIBIT 1001, Page 1

'199 Patent: Overview of Original Independent Claim 1

A discrimination system comprising :

an identifier transmission system coupled to an aerial system , wherein the identifier transmission system is configured to broadcast an aerial system identifier signal unique to the aerial system;

an identification receiver;

a permission module, wherein the identification receiver is configured to receive the aerial system identifier signal and to provide the aerial system identifier signal to the permission module, wherein the permission module is configured to determine that the aerial system associated with the aerial system identifier signal is not permitted to be in an airspace; and

a disruption system configured to disrupt an operation of the aerial system , wherein the disruption system is preemptively enabled based the received aerial system identifier signal.

Procedural History: '199 Patent

- The Petition (Paper 1) challenged claims 1-9 of the '199 Patent over the following grounds:

Ground	Claims	Basis (35 U.S.C. §)	Prior Art
1	1-3, 5-9	103	<i>Whitmarsh</i>
2	4	103	<i>Whitmarsh, Falk</i>
3	1-3, 5-9	103	<i>Whitmarsh, Goodrich</i>
4	4	103	<i>Whitmarsh, Goodrich, Falk</i>
5	1, 3, 5-9	103	<i>Viggiano, Goodrich</i>
6	4	103	<i>Viggiano, Goodrich, Falk</i>

- Patent Owner waived filed a Preliminary Response (POPR) (Paper 9)

Procedural History: '199 Patent

- The Board instituted trial (Paper 10)
 - The Board interpreted “permission module” under 35 U.S.C. § 112(f).
 - Function: “determining that the aerial system associated with the aerial system identifier signal is not permitted to be in an airspace,”
 - Structure: “storage on-board the disruption system, storage on-board the identification receiver, a remote computing system connected to the disruption system or any other suitable computing system programmed to compare an aerial system parameter, such as an identifier, with the permissions for the airspace.”
 - The Board agreed that Ground 1 (Whitmarsh) demonstrated a reasonable likelihood of success that claim 1 is unpatentable, and further instituted Grounds 2-6.

Procedural History: '199 Patent

- Patent Owner filed a Non-Contingent Motion to Amend (Paper 15) presenting Substitute Claims 10-18
 - Patent Owner did not file a Patent Owner's Response
- Petitioners filed an Opposition to Motion to Amend (Paper 20)
- The Board issued Preliminary Guidance (Paper 22) finding that Petitioner showed a reasonable likelihood that the proposed substitute claims 10-18 were obvious

Procedural History: '199 Patent

- Patent Owner filed a Non-Contingent Revised Motion to Amend (Paper 25) presenting a revised Substitute Claims 10-18
- Petitioners filed an Opposition to Revised Motion to Amend (Paper 32)
- Patent Owner filed a Reply to the Opposition (Paper 34)
- Petitioners filed a Sur-Reply to the Reply (Paper 36)

'199 Patent: Overview of Substitute Independent Claim 10

[[1]]10[.pre] A discrimination system comprising:

[10.a] an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an identification system comprising an identification receiver;

[10.c] a permission module,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

'199 Patent: Overview of Substitute Dependent Claims 11-18

[[2]]11. The system of claim 10, wherein the identifier transmission system and the identification receiver communicate using a radio chipset that is compatible with a communication protocol selected from the following: WiFi, LTE, or Bluetooth.

[[3]]12. The system of claim 10, wherein the identification receiver is a mobile device.

[[4]]13. The system of claim 10, wherein the identifier transmission system is configured to be reassigned from a first aerial system to a second aerial system.

[[5]]14. The system of claim 10, wherein when the disruption system is enabled the aerial system is caused to be removed from the airspace.

[[6]]15. The system of claim 10, wherein the disruption system comprises of a projectile launcher and an interdiction module.

[[7]]16. The system of claim 10, wherein the disruption system comprises of an interceptor drone coupled with an interdiction module.

[[8]]17. The system of claim 10, further comprising a control system for controlling the disruption system.

[[9]]18. The system of claim [[8]]10, further comprising a logging system that is configured to record activity of at least one of the identification receiver, the permission module, or the control system.

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview**
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Dispute Overview

- PO Disputes:
 - Whether *a second identifier* received from a computing system that is remote relative to the discrimination system **lacks written description support**
 - Whether *to provide the authenticated first identifier of the aerial system identifier signal to the permission module* **lacks written description support**
 - Whether *a second identifier* received from a computing system that is remote relative to the discrimination system is **indefinite**
 - Whether *preemptively enabled* is **indefinite**
 - Whether Grounds 7B-10B and 7C-10C **teach** a second identifier functioning as a second factor identifier
 - Whether Grounds 11-14 **teach** a second identifier received from a computing system that is remote relative to the discrimination system

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description**
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Substitute Claim 10 requires *a second identifier* received from *a computing system that is remote relative to the discrimination system* (element [10.d])

[[1]]10[.pre] A **discrimination system** comprising:

[10.a] an **identifier transmission system coupled to an unmanned aerial system**, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an **identification system** comprising an **identification receiver**;

[10.c] a **permission module**,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) **a second identifier from a computing system that is remote relative to the discrimination system**, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

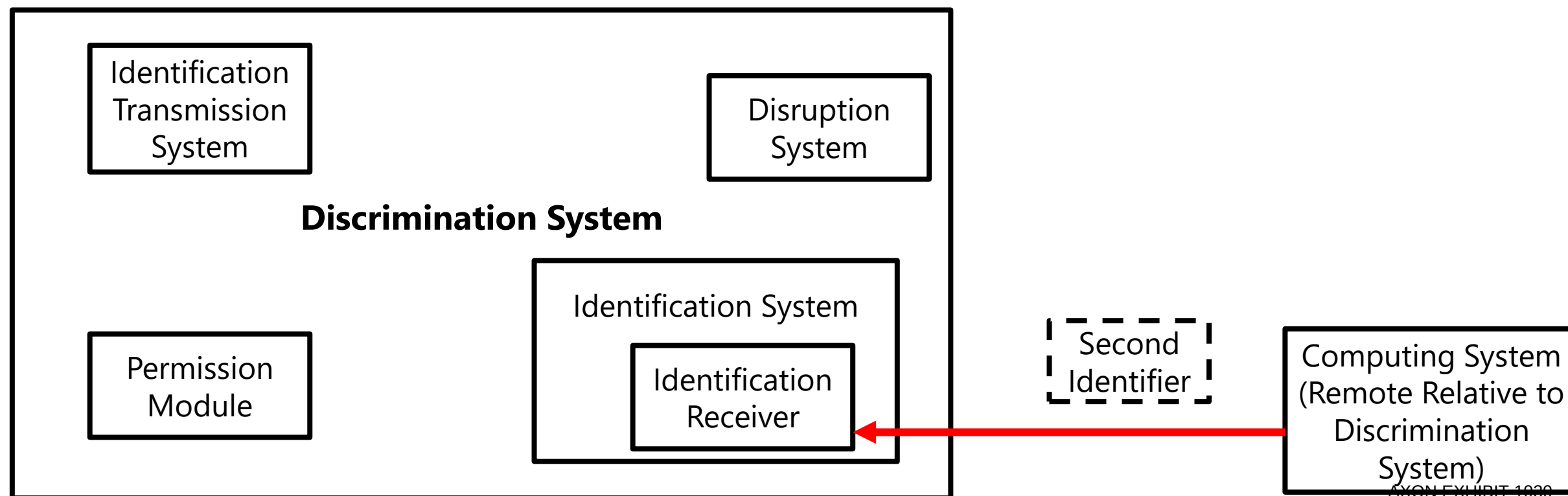
[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a **disruption system** configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

No Written-Description Support Exists for Element [10.d]

- The specification does not provide written description support for ***a second identifier received from a computing system that is remote relative to the discrimination system***



AXON EXHIBIT 1030

PO Attempts to Manufacture Written Description Support

- In its Reply, PO **combines four disparate specification passages** to argue that when read **“in context with each other”** they demonstrate “that one or two identifiers may be used, and either may be remote or local to the UAV.”
 - Citing EX2002 at 2:18-22, 4:15-22, 14:16-5:2, 39:6-9.
- PO's attempt to combine and vary these disclosures reveals it is **relying on obviousness to supply written description.**

Only One Source of Transmission of a *Second Identifier*

- The specification provides **only one source** for the transmission of the *second identifier*:
 - the **identifier transmission system** of aerial system 100 (UAV), **which is part of the discrimination system, not remote to it.**

15 tampering and/or reproduction. Fourth, in some variations, the aerial system 100 can
16 include a first and second identifier, transmitted by a first and second identifier
17 transmission system, respectively, wherein the second identifier can function as a
18 backup identifier (e.g., in case the primary identifier transmission system is inoperable),
19 a second factor identifier for the aerial system 100 (e.g., as a secondary authenticator for
20 the aerial system to prevent tampering and/or identifier reproduction), an identifier for

PO Argues Transmissions from a UAV are Not *Remote Relative to the Discrimination System*

- PO has taken the position that **transmissions from the UAV are not *remote relative to the discrimination system***; such disclosure thus **cannot be relied upon** to supply written description support.

In the Whitmarsh-Viggiano combination, the alleged aerial system identifier and the alleged second factor are both received from the UAV, and not from “a computing system that is remote relative to the discrimination system.” Moreover, the authenticity of Whitmarsh’s MAC address cannot be verified using Viggiano’s

Aerial System Identifier 310 is Not the Claimed *Second Identifier*

- PO points to “aerial system identifier 310 [that] is preferably dynamic” and can be “generated remotely (e.g., at a remote computing system).”
 - But identifier 310, whether dynamic or static, is **never disclosed as being a *second identifier*** and at best relates to the *first identifier* instead.

1 The aerial system 100 is preferably associated with an aerial system identifier or ID 310
2 which may be transmitted via an aerial system identifier signal 300, but can
3 alternatively be unidentified. The aerial system identifier signal 300 can be that

Aerial System Identifier 310 is Not the Claimed *Second Identifier*

- The dynamic identifier is further only disclosed as transmitted in identifier signal 300, which is **part of the discrimination system, not remote from it.**

5 3.2. Identifier Transmission System.

6 The discrimination system 110 can additionally include an identifier transmission

7 system 101 that functions to mount to an aerial system 100 and transmit an aerial

8 system identifier signal 300 to the identification receiver 102. The identifier

The Specification Does Not Describe a Remote Computing System that is *Remote Relative to the Discrimination System*

- The disclosed “remote computing system” is simply “remote” **from aerial system 100 (i.e., the aircraft).**

23 or at any other suitable time. The dynamic aerial system identifier can be generated on-
24 board the aerial system 100, generated remotely (e.g., at a remote computing system,
1 etc.; updated in-flight or when connected to a predetermined communication
2 connection type, etc.), or generated by any other suitable system. The aerial system

- An identifier or system that might be **remote from an aircraft does not support *remote relative to the discrimination system***

Boilerplate Language in the Specification Cannot Provide Support

6 Although omitted for conciseness, the preferred embodiments include every
7 combination and permutation of the various system components and the various
8 method processes, wherein the method processes can be performed in any suitable
9 order, sequentially or concurrently.

- “[B]oilerplate language at the end of the [] Application's specification is not sufficient to show adequate disclosure of the actual combinations and attachments used in the [] Claims.”
 - *D Three Enters., LLC v. SunModo Corp.*, 890 F.3d 1042, 1051 (Fed. Cir. 2018).

PO's Indirect Transmission Theory is Unsupported

- PO's asserts a POSITA would understand SC 10 encompasses identifiers routed "indirectly (e.g., through the UAV)"
- A dynamic identifier may be:
 - "**generated remotely**" from an aircraft at a "remote computing system,"
 - "**updated in flight**," or
 - "connected to a **predetermined communication connection type**"
- **But none of this supports indirect communication in which a second identifier is transmitted**
 - (1) from a computing system remote relative to the discrimination system to a UAV, and then
 - (2) from the UAV to a receiver.

PO's Indirect Transmission Theory is Unsupported

- By conceding that the identifier must pass “through the UAV,” PO has itself established a lack of support.
- PO argued that an identifier “received from the UAV” is not received from a “computing system that is remote relative to the discrimination system”:

In the Whitmarsh-Viggiano combination, the alleged aerial system identifier and the alleged second factor are both received from the UAV, and not from “a computing system that is remote relative to the discrimination system.” Moreover, the authenticity of Whitmarsh’s MAC address cannot be verified using Viggiano’s

- Thus, a transmission passing “through the UAV” under PO’s own logic cannot provide written description support as PO said it is not within the scope of SC 10.

PO Cannot Show Possession of an Architecture Where Transmission Originates *Remote Relative to the Discrimination System*

- A component cannot be remote relative to the system it is a part of.
- The specification **exclusively ties** the transmission of the second identifier to the **identifier transmission system that is claimed as part of the discrimination system**,
- **PO therefore cannot show written description support for element [10.d].**

Substitute Claim 10 requires *to provide the authenticated first identifier...to the permission module* (element [10.e2])

[[1]]10[.pre] A discrimination system comprising:

[10.a] an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an identification system comprising an identification receiver;

[10.c] a permission module,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

No Written-Description Support Exists for Element [10.e2]

- The specification does not provide written description support for **providing an *authenticated first identifier..to the permission module***
- PO attempts to manufacture written description support by **stitching together several portions** of the specification and **impermissibly relying on obviousness**.

Raw or Processed Signals Does Not Disclose that Any *Authenticated First Identifier* is Provided to a *Permission Module*

- The specification describes “processing” a signal in the context of interpretation (e.g., decrypting a broadcast); **it never equates a “processed” signal with an “authenticated” first identifier verified using a second identifier.**

20 to the antenna 607. The chipset 608 can be connected to the permissions module 103,
21 wherein the chipset 608 sends the raw or processed signal to the permissions module
22 103 for permissions determination. However, the chipset 608 can include the

PO Impermissibly Uses Obviousness for Written Description

- “[I]nterpreting” a signal does not support authenticating a signal.

14 received aerial system identifier signal 300. The chipset 608 preferably interprets the
15 signal 300 into the aerial system identifier 310 (e.g., decrypts the signal, etc.), but can
16 alternatively interpret the signal 300 into a set of data indicative of the identifier 310, or
17 otherwise interpret the signal 300. The chipset 608 can function as a receiver only,

- PO impermissibly uses obviousness to conclude interpreting a signal is the same as “determining” a signal, solely to bridge to an entirely different section.

17 Determining an aerial system identifier 310 can optionally include verifying the
18 authenticity of the aerial system identifier 310. This functions to identify aerial systems

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite**
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Substitute Claim 10 requires *a second identifier* received from *a computing system that is remote relative to the discrimination system* (element [10.d])

[[1]]10[.pre] A **discrimination system** comprising:

[10.a] an **identifier transmission system coupled to an unmanned aerial system**, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an **identification system** comprising an **identification receiver**;

[10.c] a **permission module**,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) **a second identifier from a computing system that is remote relative to the discrimination system**, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a **disruption system** configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

Only One Source of Transmission of a *Second Identifier*

- The specification provides **only one source** for the transmission of the *second identifier*:
 - the identifier transmission system of aerial system 100 (UAV), **which is part of the discrimination system, not remote to it.**

15 tampering and/or reproduction. Fourth, in some variations, the aerial system 100 can
16 include a first and second identifier, transmitted by a first and second identifier
17 transmission system, respectively, wherein the second identifier can function as a
18 backup identifier (e.g., in case the primary identifier transmission system is inoperable),
19 a second factor identifier for the aerial system 100 (e.g., as a secondary authenticator for
20 the aerial system to prevent tampering and/or identifier reproduction), an identifier for

- The scope of SC 10 is thus unclear due to this deficiency in the specification: **a system cannot be remote from itself**

Element [10.d] creates a logical inconsistency

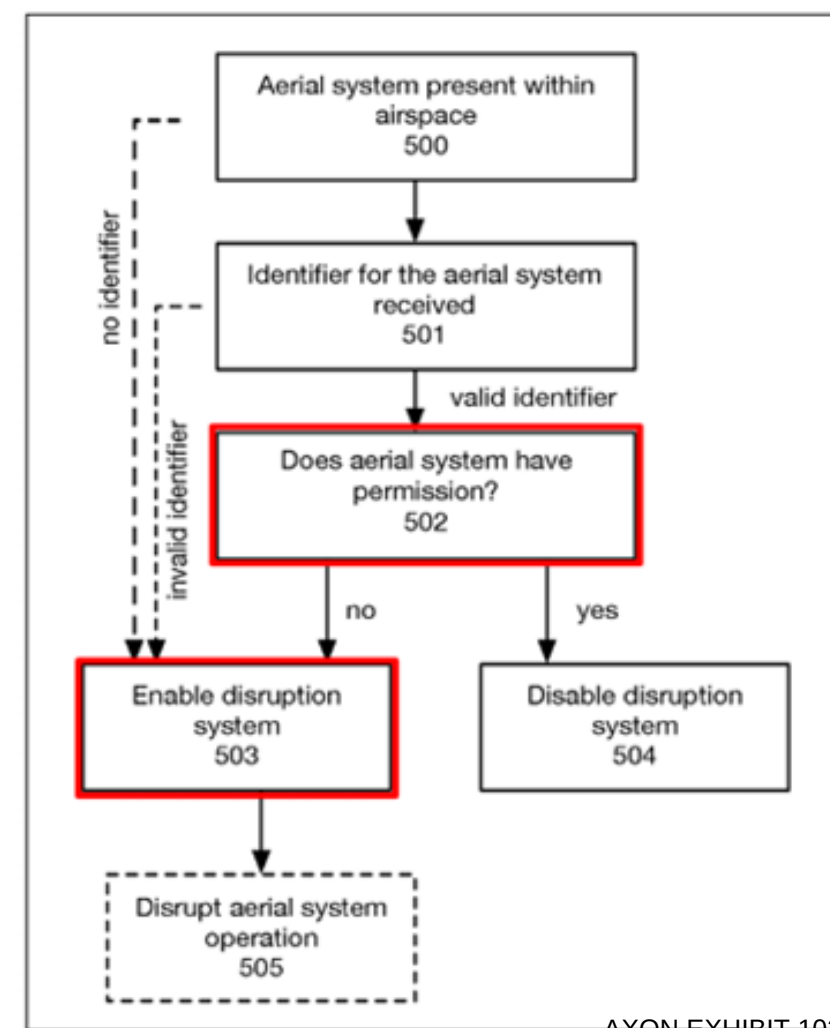
- PO's own conflicting arguments further demonstrate that the scope of element [10.d] is not reasonably certain.
- PO argues the claim **encompasses identifiers routed "through the UAV."**
 - But **PO took the opposite position in its RMTA**
- The scope of SC 10 is thus unclear due to PO's conflicting positions.

Substitute Claim 10 requires *wherein the disruption system is preemptively enabled*
(element [10.g])

[10.g] a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

The Specification Does Not Differentiate Between *Preemptively Enabled* and “Enabled”

- **PO alleges** that the specification “clearly delineates a **non-preemptive enablement** of a disruption system (e.g., **based on a UAV being deemed not permitted**, and after the exercise of one or more less aggressive option), and a preemptive enablement”
- **PO also alleges** “in the context of Figure 5, a POSITA would understand **from the dotted lines** that the general flow can be short-circuited such that the disruption system is **preemptively enabled**, i.e., the check for the condition 502 can be omitted, if condition 501 is met.”



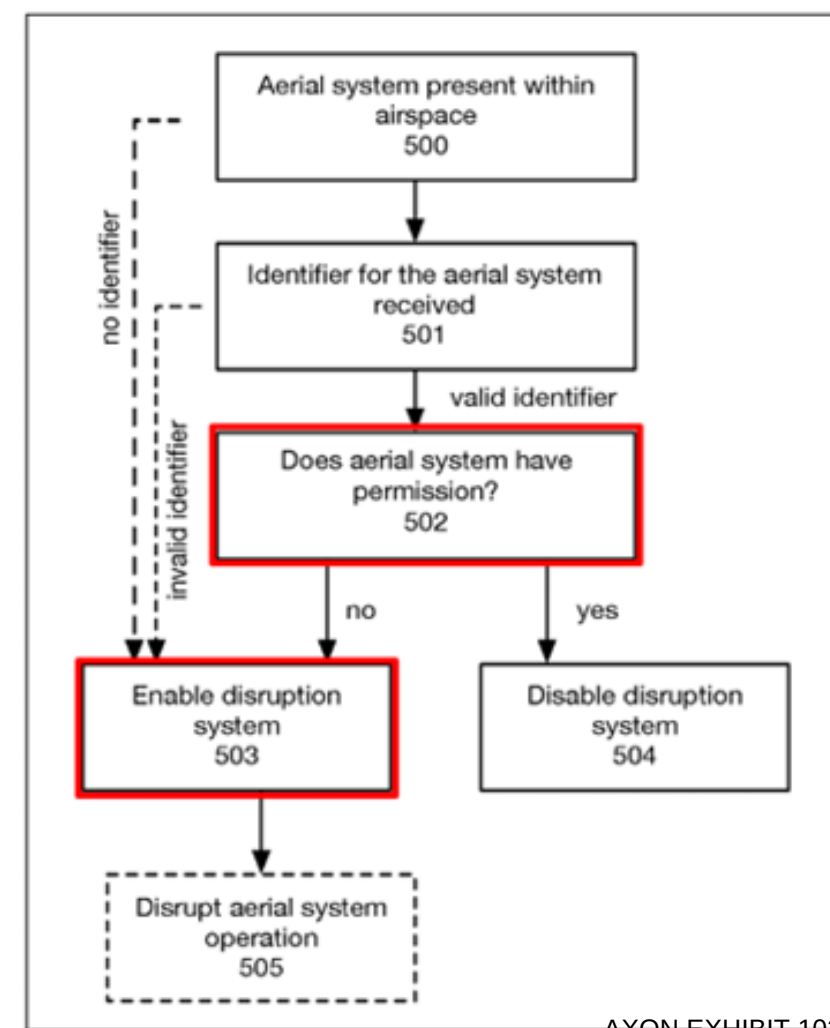
AXON EXHIBIT 1030

The Specification Does Not Differentiate Between *Preemptively Enabled* and “Enabled”

- EX2002 at 36:21-24:

21 to engage on short notice. As depicted in FIGURE 5, the disruption system 105 may thus
22 be preemptively enabled if certain conditions are met (e.g. aerial system detected w/o an
23 identifier 500, identifier is received but is invalid 501, identifier is valid but is not
24 permissioned 502, etc.). Such a configuration would minimize any delays associated

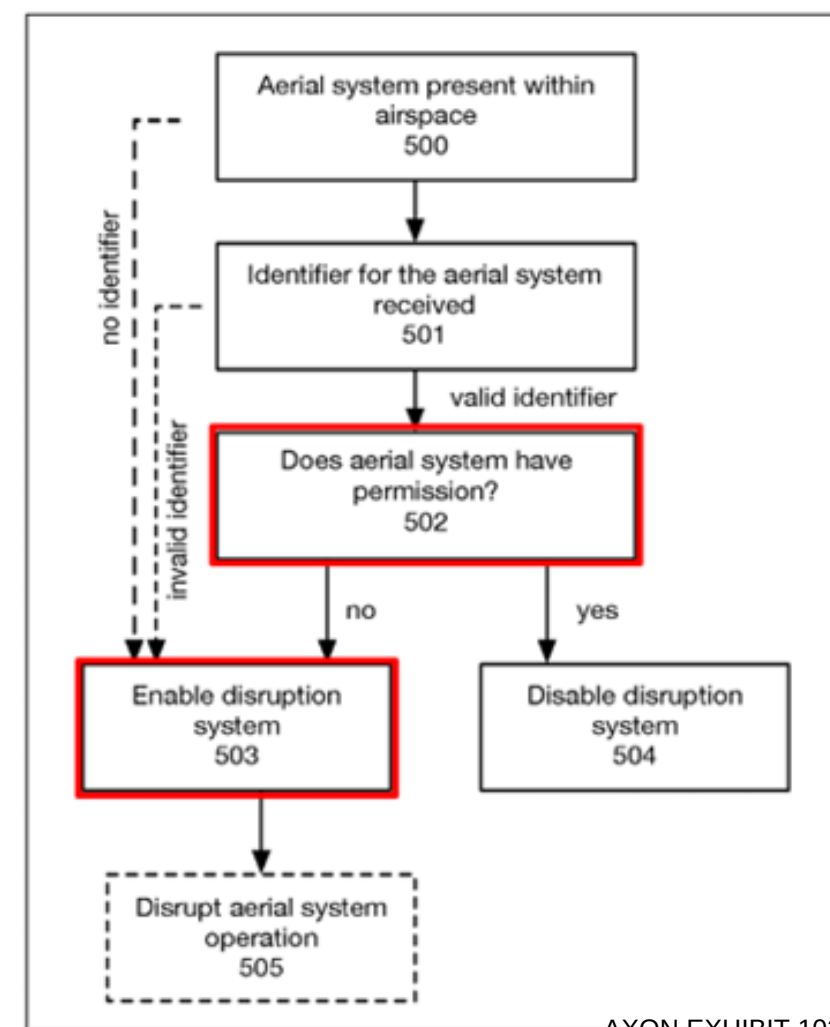
- The specification thus **specifically identifies** determining no permission in **step 502 as a condition for preemptive enablement**.
 - The lack of differentiation between *preemptively enabled* and “enabled” **sows uncertainty into SC 10 and suggests the claim could have different meanings**.
 - Interval Licensing v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014).



AXON EXHIBIT 1030

The Specification Does Not Differentiate Between *Preemptively Enabled* and “Enabled”

- **Condition 502 (“identifier is valid but is not permissioned”)**
 - Figure 5 shows that the disruption system is **directly “enable[d]” at step 503** and does not show anything that could be “preemptively enabled.”
 - **PO fails to address** how condition 502, is not shown by Figure 5 or otherwise explained as “forestal[ling]” or “preclude[ing]” any “less aggressive option”



AXON EXHIBIT 1030

The Contradiction in Meaning Demonstrates Uncertainty and Indefiniteness

- The **contradiction demonstrates indefiniteness** given “preemptively enabled” and “enabled” are different terms with different meanings, as **PO’s expert agrees**.

9	Q	Does "preemptively enabled" have a
10		different meaning than just "enabled"?
11	A	I think -- I think basically the Revised
12		Motion to Amend and my Declaration just clarifies
13		this. Yes, it -- in fact, just to rephrase this,
14		these are two different things but they are
15		related, if you look, for example, at the time
16		scale of activity.
17	Q	They're related but they have two
18		different meanings?
19	A	But they are different.

PO's Incorrect "Plain And Ordinary Meaning" Argument Demonstrates Indefiniteness

- PO additionally argues that "the plain and ordinary meaning of 'preemptive' and the disclosures of the specification, **clearly delineates:**
 - **a non-preemptive enablement of a disruption system (e.g., based on a UAV being deemed not permitted,** and after the exercise of one or more less aggressive option [sic]), and
 - **a preemptive enablement** of the disruption system (e.g., without exercising the less aggressive options)."
- **But a "UAV being deemed not permitted" is explicitly disclosed by the specification as being a condition for preemptive enablement: it is condition 502 ("identifier is valid but is not permissioned 502").**
 - And there is no "less aggressive option" associated with condition 502.

Substitute Claims 10-18 are Indefinite

- Because SC 10 is indefinite, SCs 11-18 are also indefinite.
- SC 18 is also indefinite as no antecedent basis exists for *the control system*.
 - PO does not address this argument and it is unrebutted.

[[9]]18. The system of claim [[8]]10, further comprising a logging system that is configured to record activity of at least one of the identification receiver, the permission module, or **the control system.**

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C**
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C

Ground	SC	Basis	Prior Art
7B/7C	10-12, 14-18	103	Whitmarsh, Jarrell, Gong637 (7B)/ Whitmarsh, Jarrell, Gong637, Pasko (7C)
9B/9C	10-12, 14-18	103	Whitmarsh, Goodrich, Jarrell, Gong637 (9B)/ Whitmarsh, Goodrich, Jarrell, Gong637, Pasko (9B)

Substitute Claim 10

[[1]]10[.pre] A discrimination system comprising:

[10.a] an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an identification system comprising an identification receiver;

[10.c] a permission module,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

Substitute Dependent Claims 11-12 and 14-18

[[2]]11. The system of claim 10, wherein the identifier transmission system and the identification receiver communicate using a radio chipset that is compatible with a communication protocol selected from the following: WiFi, LTE, or Bluetooth.

[[3]]12. The system of claim 10, wherein the identification receiver is a mobile device.

[[5]]14. The system of claim 10, wherein when the disruption system is enabled the aerial system is caused to be removed from the airspace.

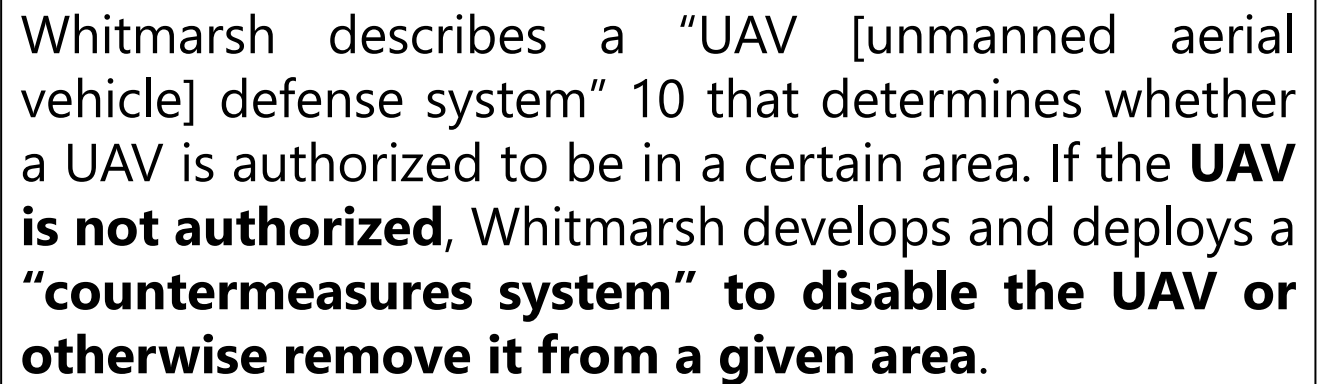
[[6]]15. The system of claim 10, wherein the disruption system comprises of a projectile launcher and an interdiction module.

[[7]]16. The system of claim 10, wherein the disruption system comprises of an interceptor drone coupled with an interdiction module.

[[8]]17. The system of claim 10, further comprising a control system for controlling the disruption system.

[[9]]18. The system of claim [[8]]10, further comprising a logging system that is configured to record activity of at least one of the identification receiver, the permission module, or the control system.

(19) **United States**
(12) **Patent Application Publication** (10) Pub. No.: US 2019/0003807 A1
Whitmarsh et al. (43) Pub. Date: Jan. 3, 2019



(12) **United States Patent**
Jarrell

(10) Patent No.: US 9,087,451 B1
(45) Date of Patent: Jul. 21, 2015

AXON EXHIBIT 1025, Page 1
Axon Enterprises, Inc. and Dedrone Holdings, Inc. v. Airspace Systems, Inc., IPR2025-00530

Jarrell is directed to techniques to “**authenticate or validate the registration or license identifier of [] [a] UAV.**” A UAV transmits its identifier to a “communications station 101,” which communicates with a “**control center 148 remote from the communications station 101, to authenticate or validate**” the identifier of the UAV. The control center 148 “provide[s] a list, and the communications station 101 may compare the UAV registration or license identifier to the list and make a determination regarding the UAV’s compliance.”

Overview of Gong637

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization

International Bureau

(43) International Publication Date
13 October 2016 (13.10.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/161637 A1

(51) International Patent Classification:
H04W 40/02 (2009.01)

(21) International Application Number:
PCT/CN2015/076335

(22) International Filing Date:
10 April 2015 (10.04.2015)

(25) Filing Language:
English

(26) Publication Language:
English

(71) Applicant: SZ DJI TECHNOLOGY CO., LTD.
[CN/CN], 6F, HKUST SZ IER Bldg., No.9 Yuexing 1st Rd., Hi-Tech Park(South), Nanshan District, Shenzhen, Guangdong 518057 (CN).

(72) Inventors: GONG, Ming; 6F, HKUST SZ IER Bldg., No.9 Yuexing 1st Rd., Hi-Tech Park(South), Nanshan District, Shenzhen, Guangdong 518057 (CN); PAN, Wei; 6F, HKUST SZ IER Bldg., No.9 Yuexing 1st Rd., Hi-Tech Park(South), Nanshan District, Shenzhen, Guangdong 518057 (CN).

(74) Agents: SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD. et al.; 9F, Hongqin Building, No. 83 Longguan East Rd., Longhua New Dist., Shenzhen, Guangdong 518109 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GR, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published

with international search report (Art. 21(3))

(54) Title: METHOD, APPARATUS AND SYSTEM OF PROVIDING COMMUNICATION COVERAGE TO AN UNMANNED AERIAL VEHICLE

(Fig. 1)

100

101

102

103

(57) Abstract: The systems and methods are provided to provide communication coverage to an unmanned aerial vehicle. A proposed flight path of a UAV may be collected, and a communication signal distribution, such as a cellular signal distribution, along the proposed flight of the UAV may be determined. At positions having low or no communication signal, relays may be provided to improve a quality of the communication signal. The relay may be a ground device or an aerial vehicle. A stable and continuous communication between the UAV and user terminals during the entire flight path of UAV may be provided, and a coverage of cellular signal may be expanded.

AXON EXHIBIT 1022, Page 1

Axon Enterprises, Inc. and Dredone Holdings, Inc. v. Airspace Systems, Inc., IPR2025-00530

Gong637 discloses UAV aircraft authentication in which a UAV “may be authenticated through the entire flight path.” Gong explains that **UAV identification can be “authenticated by checking and confirming the identification with an authentication center** on the communication network.” Failed authentication results in the UAV being “forced to land.”

(19) **United States**
(12) **Patent Application Publication**
Pasko et al.

(10) Pub. No.: US 2016/0125740 A1
(43) Pub. Date: May 5, 2016

(12) **Patent Application Publication**
Pasko et al.

(10) Pub. No.: US 2016/0125740 A1
(43) Pub. Date: May 5, 2016

(52) U.S. CL
CPC G08G 5/0034 (2013.01); H04B 1/06
(2013.01); G08G 5/0039 (2013.01); B64C
39/024 (2013.01)

(2013.01); G08G 5/0039 (2013.01); B64C 39/024 (2013.01)

(57) **ABSTRACT**

A device receives a request for a flight path for a UAV from a first location to a second location, credentials for the UAV,

and component information for the UAV. The device determines, based on the credentials, whether the UAV is authenticated for utilizing the device and a network, and determines

whether the UAV is capable of flight based on the component information and maintenance information. The design rules

calculates the flight path based on capability information for the

UAV and/or other information, and determines whether the UAV is capable of traversing the flight path based on the

repeatedly information about the current information. The device generates flight path instructions for the flight path, and provides the flight path instructions to the UAV to permit the UAV to travel from the first location to the second location via the flight path.

A device receives a request for a flight path for a UAV from a first location to a second location, credentials for the UAV, and component information for the UAV. The device determines, based on the credentials, whether the UAV is authenticated for utilizing the device and a network, and determines whether the UAV is capable of flight based on the component information and maintenance information. The device calculates, the flight path based on capability information for the UAV and/or other information, and determines whether the UAV is capable of traversing the flight path based on the capability information and/or the other information. The device generates flight path instructions for the flight path and provides the flight path instructions to the UAV to permit the UAV to travel from the first location to the second location via the flight path.



AXON EXHIBIT 1030

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.:** US 2016/0023760 A1
Goodrich (43) **Pub. Date:** Jan. 28, 2016

(52) **U.S. CL**
CPC *B64C 39/024* (2013.01); *B64C 11/00*
(2013.01); *G05D 1/12* (2013.01); *B64C*
2201/02 (2013.01); *B64C 2201/12* (2013.01);
B64C 2201/141 (2013.01)

(72) Inventor: **Wayne Goodrich**, White Salmon, WA
(US)

(21) Appl. No. : 14/801,479

(22) Filed: Jul. 16, 2015

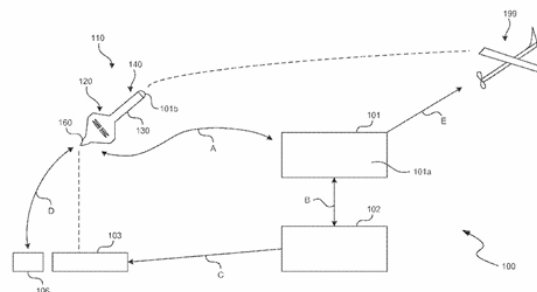
Related U.S. Application Data

(60) Provisional application No. 62/030,024, filed on Jul. 28, 2014

Publication Classification

(51) Int. Cl.
B64C 39/02 (2006.01)
G05D 1/12 (2006.01)
B64C 11/00 (2006.01)

(57) ABSTRACT
Systems and methods for countering an unmanned air vehicle are disclosed. Representative methods include directing an interceptor UAV toward a target UAV, and directing the interceptor UAV back to ground along a controlled flight path, for example, in response to an instruction not to engage with the target UAV, and/or in response to an unsuccessful engagement. Another representative method includes disabling the target UAV by deploying a disabling element (e.g., a net) from the interceptor UAV to contact the target UAV. Representative systems include a target acquisition system, a launch control system, and an engagement system carried by the interceptor UAV. In particular embodiments, the interceptor UAV can have a generally cylindrical fuselage, one or more fins carried by the fuselage, control surfaces, a payload carried by the fuselage, and a disabling system that is configured to disable the target UAV.



AXON EXHIBIT 1008, Page 1

AXON EXHIBIT 1030

Elements [10.d] and [10.e1]

- The **Grounds 7B and 9B (Jarrell)** Combinations Render [10.d] and [10.e1] Obvious

The Grounds 7B and 9B (Jarrell) Combinations Render [10.d] Obvious

wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;

- As combined with Jarrell, Whitmarsh's parts forming the identification receiver would have received:
 - (1) the wireless communications that include information or signatures unique to the UAV, such as the MAC address of the UAV, from the UAV (*wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system*) and
 - (2) a list of valid MAC address identifiers **that includes a valid MAC address identifier** relevant to the UAV, received from a remote control center (*and (ii) **a second identifier** from a computing system that is remote relative to the discrimination system*).

The Grounds 7B and 9B (Jarrell) Combinations Render [10.d] Obvious

- The **valid MAC address identifier** (*the second identifier*) **of the list** is *functioning as a second factor identifier* for the UAV.
 - It is a **second identifier to the UAV's transmitted MAC address** that authenticates the transmitted MAC address and determines whether the UAV is compliant.
 - EX1025 (Jarrell), 13:23-37, 13:44-59:

In some examples, a communications station 101 can determine whether a UAV 150 has a valid or current registration or license. For example, the communications station 101 can request a registration or license identifier from the UAV 150, and can receive a message from the UAV 150 that includes a registration or license identifier of the UAV 150. In various implementations, the communications station 101 may compare the received registration or license identifier from the UAV 150 with a list of valid (or in some examples, invalid) registration or license identifiers, for example. In some examples, the communications station 101 may store a list of registration or license identifiers in a memory of the communications station 101, and may compare received registration or license identifiers with identifiers on the stored list. In some examples, the communications station 101 may

In some examples, the communications station 101, upon receiving the registration or license identifier from the UAV 150, may communicate with a control center 148 remote from the communications station 101, to authenticate or validate the registration or license identifier of the UAV 150, or to determine that the registration or license identifier is invalid. For example, the communications station 101 may transmit a message for receipt by the control center 148 that includes the received registration or license identifier from the UAV. The communications station 101 may then receive from the control center 148 a message that includes an indication (e.g., valid or invalid) regarding the registration or license identifier from the UAV 150. In some examples, the control center 148 may provide a list, and the communications station 101 may compare the UAV registration or license identifier to the list and make a determination regarding the UAV's compliance.

PO Mischaracterizes the Combinations, Alleging That Jarrell's List Itself Forms the Claimed *Second Identifier*

- Jarrell teaches a valid MAC address identifier relevant to the UAV, which is located on a list, forms the claimed *second identifier*.
- PO's argument does not address Petitioners' position.

PO Argues for an Improper Construction of *Second Identifier Functioning as a Second Factor Identifier*

- PO asserts the *first identifier* and *second identifier functioning as a second factor identifier* must each be a different one of “**something you know**” (“**SYK**”), “**something you have**” (“**SYH**”) or “**something you are**” (“**SYA**”)
- **PO’s construction is wrong and improperly relies exclusively on extrinsic evidence to vary claim meaning**
 - The Reply solely cites to PO’s expert declaration, which itself cites to several extrinsic sources for alleged support.
 - *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1332 (Fed. Cir. 2003)
 - *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369 (Fed. Cir. 2003)

Nothing in the Intrinsic Record Supports PO's Incorrect Construction

- **Only one reference to a “factor”** exists in the specification (EX2002, 4:15-20) and no discussion of SYK, SYH, or SYA.

15 tampering and/or reproduction. Fourth, in some variations, the aerial system 100 can
16 include a first and second identifier, transmitted by a first and second identifier
17 transmission system, respectively, wherein the second identifier can function as a
18 backup identifier (e.g., in case the primary identifier transmission system is inoperable),
19 a second factor identifier for the aerial system 100 (e.g., as a secondary authenticator for
20 the aerial system to prevent tampering and/or identifier reproduction), an identifier for

- PO's argument is also **incompatible with the language of SC 10**, because both the *first identifier* and the *second identifier functioning as a second factor identifier* are **identifiers**.
 - **PO does not resolve how two identifiers must be a different one of SYK, SYH, or SYA.**

Grounds 7B and 9B (Jarrell) align with the '199 Patent Specification

- Jarrell's use of the valid MAC address identifier relevant to the UAV (*the second identifier functioning as a second factor identifier*) on a list **"prevent[s] tampering" just like the '199 Patent**.
 - If a UAV had a tampered MAC address, this tampered address **would not be authenticated as it would not match the UAV's proper, valid MAC address** (*second identifier*) on Jarrell's list.

The Grounds 7B and 9B (Jarrell) Combinations Render [10.e1] Obvious

wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

- A POSITA would have understood or at least found obvious that Whitmarsh's computer system/processor/component (*the identification system*) would have been configured to **determine the MAC address of the UAV from the wireless communications** (*is configured to determine the first identifier from the aerial system identifier signal*).
 - Whitmarsh performs authentication based on the received MAC address, so thus would have **deciphered this address from wireless communications**.

The Grounds 7B and 9B (Jarrell) Combinations Render [10.e1] Obvious

- Whitmarsh's computer system/processor/component (*the identification system*) "compare[s]" the MAC address of the UAV (*first identifier*) to the list of valid MAC address identifiers to perform authentication and thus check an authenticity of the MAC address of the UAV (*verify an authenticity of the first identifier*)
 - A **match** between the MAC address of the UAV (*first identifier*) and the valid MAC address identifier relevant to the UAV (*the second identifier*) located on the list "**authenticate[s] the MAC address of the UAV** (*verify an authenticity of the first identifier using the second identifier*).

PO Does Not Address Jarrell's Teachings or the Combinations

- PO **fails to address Jarrell's explicit "authenticat[ion]"** teachings.

In some examples, the communications station 101, upon receiving the registration or license identifier from the UAV 150, may communicate with a control center 148 remote from the communications station 101, to authenticate or validate the registration or license identifier of the UAV 150, or to determine that the registration or license identifier is invalid.

- PO further fails to confront how the transmitted MAC address and valid MAC address are "different" (to the extent this is even required) because one is transmitted by the UAV and unauthenticated at that time, and the other is located on the list and known by the system as being valid.

The Grounds 7B and 9B (Jarrell) Combinations Render [10.e1] Obvious

wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

- Successful authentication would have resulted in Whitmarsh's UAV MAC address having been authenticated, and thus **provided an authenticated UAV MAC address** (*and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified*).
 - PO does not dispute.

Elements [10.d] and [10.e1]

- The **Grounds 7C and 9C (Jarrell-Pasko)** Combinations Render [10.d] and [10.e1] Obvious

The Grounds 7C and 9C (Jarrell-Pasko) Combinations Render [10.d] Obvious

wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;

- The analysis for Grounds 7C/9C is the same as for 7B/9B, except:
 - the (ii) a ***second identifier*** from a computing system that is remote relative to the discrimination system is formed by **Pasko's account information (e.g., government registration number)** that is received from Jarrell's remote control center
 - The account information is used by Whitmarsh's computer system/processor/component to authenticate the received UAV MAC (*first identifier*)

The Grounds 7C and 9C (Jarrell-Pasko) Combinations Render [10.d] Obvious

- EX1026 (Pasko), ¶0035-0038

location (e.g., the location in the particular region). The origination location and the destination location may be provided in the particular region. In some implementations, the credentials of UAV 220 may include an identification number, a model number, a serial number, an identifier of a UICC (or another type of smart card), a government registration number, etc. associated with UAV 220. In some implementations, the credentials of UAV 220 may include information identifying components of UAV 220 (e.g., serial numbers, model numbers, part numbers, etc. of the components).

[0038] In some implementations, UAV platform 230 may determine whether UAV 220 is registered with an appropriate authority (e.g., a government agency) based on the credentials of UAV 220. For example, if the credentials of UAV 220 include a government registration number of UAV 220, UAV platform 230 may compare the government registration number to the UAV account information in data storage 235 to determine whether UAV 220 is registered with a government agency to legally fly in airspace regulated by the government agency. In some implementations, UAV 220 may include a common protocol with other UAVs 220. The common proto-

[0037] As further shown in FIG. 4A, process 400 may include determining whether the UAV is authenticated for network(s) and is registered with an appropriate authority based on the UAV credentials (block 410). For example, UAV platform 230 may determine whether UAV 220 is authenticated for using UAV platform 230 and/or one or more of networks 240-260 based on the credentials of UAV 220. In some implementations, UAV platform 230 may compare the credentials of UAV 220 with UAV account information stored in data storage 235 (e.g., information associated with authenticated and registered UAVs 220, such as identification numbers of UAVs 220, public and/or private keys of UAVs 220, account status information, etc.) in order to determine whether UAV 220 is authenticated for using UAV platform 230 and/or one or more of networks 240-260. For example, if the credentials of UAV 220 include a serial number of UAV 220, UAV platform 230 may compare the serial number to the UAV account information in data storage 235 to determine whether UAV 220 is registered with UAV platform 230, whether an account of UAV 220 is in good standing (e.g., paid for), etc. In some implementations, UAV platform 230 may determine whether UAV 220 is authenticated for using UAV platform 230 and/or one or more of networks 240-260 based on a UICC associated with UAV 220.

The Grounds 7C and 9C (Jarrell-Pasko) Combinations Render [10.d] Obvious

- An **authenticity** of the UAV's MAC address is verified as the MAC address is associated with a **properly government registered UAV** and good standing account through the authentication comparisons.
- Moreover, an **authenticity** of the UAV's MAC address is further verified as the **MAC address is associated with a UAV that is properly registered with a government authority**.
- The received account information (*the second identifier*) is *functioning as a second factor identifier* for the UAV because it is a **second identifier (including UAV identification number, UAV public/private keys, UAV account status, and government registration number)** to the UAV's transmitted MAC address that **authenticates the MAC address**
 - The account information is also a **different piece of information** (e.g., a government registration number) from the UAV MAC address that is used in an additional comparison (e.g., using government registration numbers)

PO's Arguments Against Grounds 7C and 9C (Jarrell-Pasko) are Erroneous

- PO makes the same **incorrect** claim construction argument discussed previously.
- PO further argues against the **Pasko reference individually**, which is **improper**.
- PO argues the combinations are not "rooted" in Pasko
 - The combinations **are rooted** in Pasko's **authentication teachings** that involve **comparisons using multiple pieces of information, and further verifies an authenticity** of the UAV's MAC address

The Grounds 7C and 9C (Jarrell-Pasko) Combinations Render [10.e1] Obvious

wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

- The analysis for Grounds 7C/9C is the same as for 7B/9B, except:
 - the *second identifier* is formed by Pasko's account information (e.g., government registration number) received from Jarrell's remote control center, and
 - Whitmarsh's computer system/processor/component (*identification system*) authenticates the received UAV MAC address using the account information (*verify an authenticity of the first identifier using the second identifier*)
 - **An authenticity of the UAV's MAC address is verified as it is associated with a properly government registered UAV and good standing account through the authentication comparisons, and**
 - **The combinations further verify an authenticity of the UAV's MAC address as the MAC address is associated with a UAV that is properly registered with a government authority.**

PO Does Not Properly Consider the Combinations

- PO argues that “verifying that a UAV’s identifier is registered to fly does not verify whether the identifier a UAV provides is authenticated”
 - PO ignores the combinations:
 - A UAV’s MAC address is determined as associated with a properly government-registered UAV and good standing account through authentication comparisons, which **further verifies an authenticity of the UAV’s MAC address as the MAC address is associated with a UAV that is properly registered with a government authority.**

The Grounds 7C and 9C (Jarrell-Pasko) Combinations Render [10.e1] Obvious

wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

- Successful authentication would have resulted in Whitmarsh's UAV MAC address having been authenticated, and thus **provided an authenticated UAV MAC address** (*and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified*).
 - PO does not dispute.

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C**
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C

Ground	SC	Basis	Prior Art
8B/8C	13	103	Whitmarsh, Falk, Jarrell, Gong637 (8B)/ Whitmarsh, Falk, Jarrell, Gong637, Pasko (8C)
10B/10C	13	103	Whitmarsh, Goodrich, Falk, Jarrell, Gong637 (10B)/ Whitmarsh, Goodrich, Falk, Jarrell, Gong637, Pasko (10C)

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13**
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14

Obviousness of Substitute Claims 10-12 and 14-18: Grounds 11 and 13

Ground	SC	Basis	Prior Art
11	10-12, 14-18	103	Whitmarsh, Viggiano, and Gong637
13	10-12, 14-18	103	Whitmarsh, Goodrich, Viggiano, and Gong637

(19) **United States**
(12) **Patent Application Publication**
Viggiano et al.

(10) Pub. No.: US 2007/0239986 A1
(43) Pub. Date: Oct. 11, 2007

(57) ABSTRACT

A secure system for authenticating the identity of ADS-B systems, including: an authenticator, including a unique id generator and a transmitter transmitting the unique id to one

A secure system for authenticating the identity of ADS-B systems, including: an authenticator, including a unique id, a generator and a transmitter transmitting the unique id to one or more ADS-B transmitters; one or more ADS-B transmitters, including a receiver receiving the unique id, one or more secure processing stages merging the unique id with the received unique id to generate a secure key; a receiver receiving and generating a secure code identification and a transmitter transmitting a response containing the secure code and the ADS-B transmitter's data to the authenticator; the authenticator including means for independently determining each ADS-B transmitter's secret key, a receiver receiving each ADS-B transmitter's secret key, a secure processing stage merging the unique id with the received unique id to generate a secure key, a secure processing stage merging the unique id, ADS-B transmitter's identification and data and generating a secure code, and comparison processing comparing the authenticator-generated secure code and the ADS-B transmitter-generated secure code, providing an authentication signal based on the comparison.

(21) Appl. No.: 11/491,917

(22) Filed: **Apr. 7, 2006**

Publication Classification

(51) Int. Cl.

(52) U.S. Cl. 713/168



Viggiano discloses a "system for authenticating the identity of ADS-B systems," and is directed to **aircraft authentication techniques in which multiple forms of aircraft identification are used to authenticate the aircraft's identity.**

Substitute Claim 10

[[1]]10[.pre] A discrimination system comprising:

[10.a] an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system;

[10.b] an identification system comprising an identification receiver;

[10.c] a permission module,

[10.d] wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;[[and]

[10.e1] wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

[10.e2] to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

[10.f] wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

[10.g] a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

The Grounds 11 and 13 Combinations Render [10.d] Obvious

wherein the identification receiver is configured to receive: (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system, and (ii) a second identifier from a computing system that is remote relative to the discrimination system, the second identifier functioning as a second factor identifier for the unmanned aerial system;

- Whitmarsh's parts forming an identification receiver would have received:
 - (1) UAV aircraft identification information that is the wireless communication signal including the MAC address of a UAV, from a first communication unit of the UAV (*wherein the identification receiver is configured to receive (i) the aerial system identifier signal comprising the first identifier from the unmanned aerial system*), and
 - (2) **a message AC formed from identification information of the UAV and a secret key of the UAV, from a second communication unit of the UAV** (*and (ii) a second identifier from a computing system that is remote relative to the discrimination system*).
- The message AC (*the second identifier*) is *functioning as a second factor identifier* for the unmanned aerial system as it is formed from identification information and a unique secret key of the UAV, is a second piece of identification information that is received (the first piece of identification information is the MAC address of the UAV), and is used to authenticate the UAV aircraft's identity.

The Grounds 11 and 13 Combinations Render [10.d] Obvious

- EX1007 (Viggiano), ¶¶0013-0014, Fig. 1

ticator and the corresponding responses 38. The Authenticator's system generates a unique identifier and transmits an authentication challenge 12, which includes the unique identifier to the ADS-B transmitter 20. The ADS-B transmitter 20 inputs the unique identifier, the ADS-B transmitter's ID 22 and specific data 24 into the authentication processing to generate its authentication challenge response. The ADS-B transmitter's specific data 24 may include such data as position, velocity, and intent as might be provided by a flight management system. In one embodiment of the present invention, the authentication processing of the ADS-B transmitter system comprises a secret-key 36, a secure hash generator 40 and a Message Authentication Code (MAC) generator 35, which transform the input data into a MAC 38. The MAC 38, the ADS-B transmitter's ID 22 and the ADS-B transmitter's specific data 24 are then transmitted to the Authenticator 10 in an authentication response 18.

[0014] In one preferred embodiment of the present invention, the MAC 38 is transmitted as part of a 1090 MHz ADS-B message using unused and/or reserved bits in the ADS-B 1090 MHz broadcast message format. In another preferred embodiment, the MAC 38 is transmitted in response to an authentication challenge 12 as part of the ADS-B UAT broadcast position message, using unused and/or reserved bits in the ADS-B UAT message format. The ADS-B UAT broadcast position message is broadcast approximately every second by ADS-B UAT equipped aircraft and vehicles. Authenticator 10 may receive an ADS-B transmitter's ID 22 and specific data 24 after transmitting the authentication challenge 12.

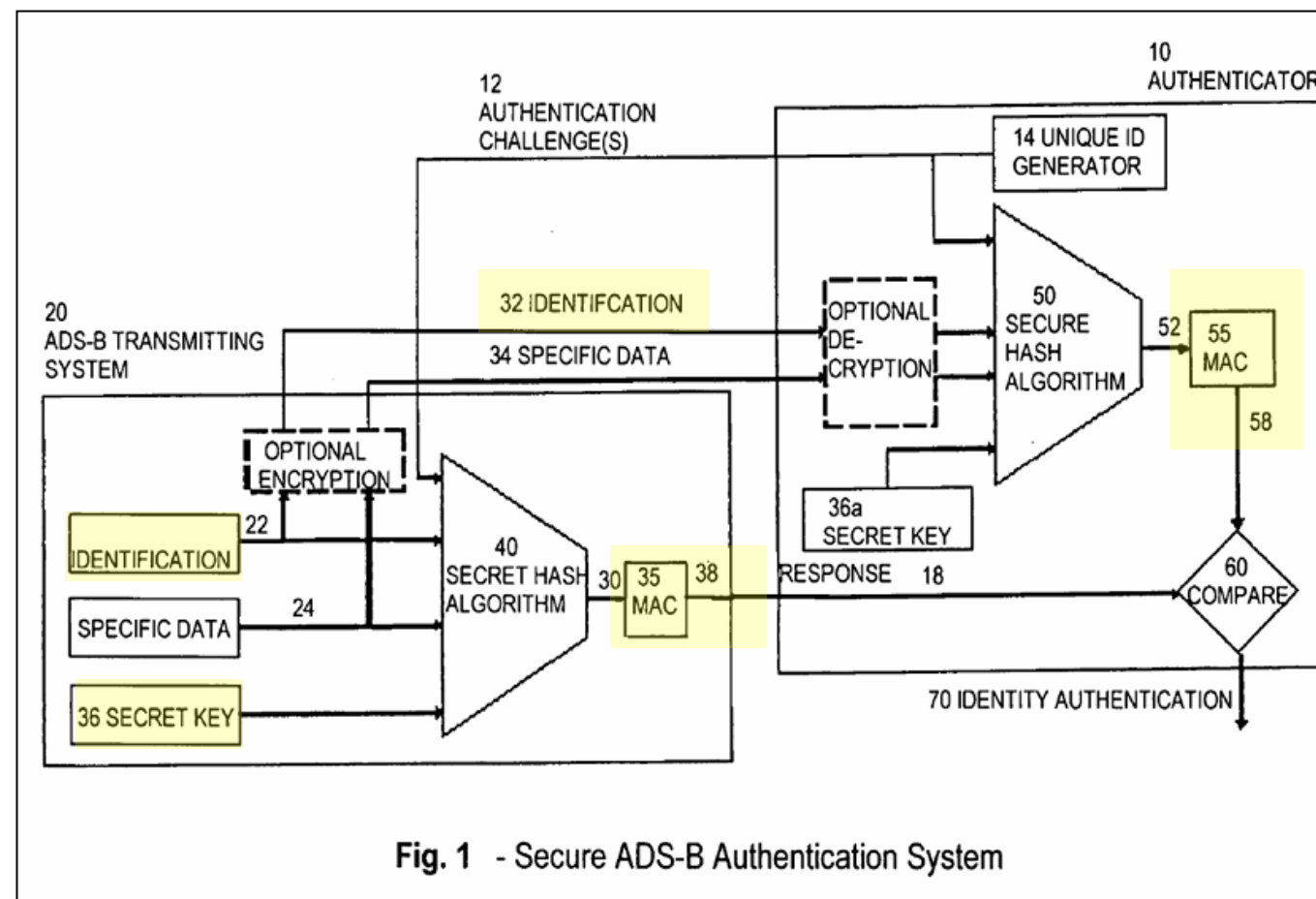


Fig. 1 - Secure ADS-B Authentication System

PO alleges the “message AC” (*second identifier*) would be transmitted by an identifier transmission system that is a “component of the claimed ‘discrimination system.’”

- PO ignores the combinations
 - The communication system transmitting message AC is **not part of the identifier transmission system** (that is part of the discrimination system) and is **a separate computing device of the UAV**.
 - The **message AC** (*second identifier*) is thus transmitted from a computing device that is ***remote relative to the discrimination system***.
- PO further advances the same incorrect claim construction argument addressed previously.

Outline of Arguments: IPR2025-00530 ('199 Patent)

- I. Overview of the '199 Patent and Procedural History
- II. Dispute Overview
- III. Substitute Claims 10-18 Lack Written Description
- IV. Substitute Claims 10-18 are Indefinite
- V. Obviousness of Substitute Claims 10-12 and 14-18: Grounds 7B/7C and 9B/9C
- VI. Obviousness of Substitute Claim 13: Grounds 8B/8C and 10B/10C
- VII. Obviousness of Substitute Claim 10-12 and 14-18: Grounds 11 and 13
- VIII. Obviousness of Substitute Claim 13: Grounds 12 and 14**

Obviousness of Substitute Claim 13: Grounds 12 and 14

Ground	SC	Basis	Prior Art
12	13	103	Whitmarsh, Falk, Viggiano, and Gong637
14	13	103	Whitmarsh, Goodrich, Falk, Viggiano, and Gong637

Substitute Claim 13

- Grounds 12 and 14 render obvious substitute claim 13 for the same reasons discussed above for Grounds 8B/8C and 10B/10C.

Backup Slides

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine Whitmarsh, Jarrell, and Gong637 (7B)/ Whitmarsh, Goodrich, Jarrell, and Gong637(9B)

- UAV systems were known to present “unauthorized or intrusive surveillance opportunities that could arise as unmanned aerial vehicles become more prevalent.”
- Another known problem in UAV systems was “spoofing” or fraudulent UAV identities. Bad actors using such techniques could gain access to unauthorized airspace.
- As Jarrell and Gong637 are highly relevant to addressing such known problems, a POSITA would have made the combinations.
- Whitmarsh, as well as Whitmarsh and Goodrich, teach using a UAV MAC address to identify a UAV, and Jarell and Gong637 provide enhancements by teaching identification techniques that help ensure such a UAV MAC address is authentic and not fraudulent.

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine Whitmarsh, Jarrell, and Gong637 (7B)/ Whitmarsh, Goodrich, Jarrell, and Gong637(9B)

- The combinations would have provided that:
 - a received UAV MAC address is authenticated, by Whitmarsh's computer system, processor, or similar component that identifies UAVs based on their received MAC addresses, by checking the address against a list received from a remote center, verifying an authenticity of the UAV MAC address
 - the UAV is forced to land if authentication fails
- After successful authentication, an authenticated UAV MAC address would have then been usable by the combinations' systems, which would have been a benefit by ensuring that the MAC address is valid.

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine Whitmarsh, Jarrell, Gong637, and Pasko (7C)/ Whitmarsh, Goodrich, Jarrell, Gong637, and Pasko (9C)

- Pasko's remotely stored account information (including identification information and government registration number) would have been present at Jarrell's remote control center, where Whitmarsh's system/processor/component
 - (1) receives credentials including the identifier UAV MAC address and government registration number from a UAV,
 - (2) receives the account information from Jarrell's remote control center, and
 - (3) authenticates a received UAV MAC using the account information, comparing the UAV MAC address and government registration number of the UAV credentials against identification information and a government registration number of the account information.
- The combinations would have provided the same benefits discussed previously and would have improved system security, providing an additional layer of authentication through verification of additional information (e.g., government registration number).

A discrimination system comprising:

-
- FIG. 1 is a block diagram of a system for detecting and countering unauthorized aircraft. The system includes a Sensor Network (12) connected to a Processing System (30). The Processing System contains a Local DB (32), User Input System (34), Display System (45), and a Countermeasures System (48). It is also connected to a Network (42), which links to a UAV Registry (36), AI Processor (38), 3rd Party Systems (40), and a Security Vehicle (44). A dashed circle (10) represents a detection zone with sensors (18) and a central unit (14).

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.a] Obvious

an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system

- Whitmarsh discloses a transmission system coupled to an unmanned aerial vehicle (UAV) (*an identifier transmission system...*).
- Whitmarsh discloses wireless communications transmitted by the UAVs transmission system comprise information or signatures unique to the UAV, such as a MAC address of the UAV, that is used to identify the transmitting UAV (*the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system*).

[0020] Briefly, and with reference now primarily to FIG. 3, commercially produced UAVs 14 are provided with one or more wireless communication system(s) 56 that periodically broadcast radio signals 54. The radio signals 54 allow the UAV 14 to communicate with a host control system 58 controlled by the operator (not shown) of the UAV 14. The information that is periodically broadcast by the wireless communication system(s) 56 of UAV 14 typically includes at least a beacon frame which contains certain information and data about the UAV 14, including its media access control address or MAC address. Of course, additional information may be broadcast as well.

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.b] Obvious

an identification system comprising an identification receiver

- A POSITA would have understood, or at least found obvious, that Whitmarsh's UAV defense system comprises a computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*identification system*)
- The system/processor/similar component would have further included the parts forming an identification receiver that receives wireless communications and identification information (e.g., the MAC addresses) contained therein that is transmitted by UAVs (*identification system comprising an identification receiver*)

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.c] Obvious

a permission module,

- Whitmarsh discloses, or at least renders obvious, "*a permission module*," as addressed in Limitation [10.f], discussed below.

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.e2] Obvious

to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

- The combinations teach that successful authentication would have resulted in Whitmarsh's authenticated UAV MAC address provided to the *permission module* (*to provide the authenticated first identifier of the aerial system identifier signal to the permission module*).
- A POSITA would have understood that for the "*permission module*" to use the UAV's identity (as indicated by the received MAC address) to determine to deploy a particular countermeasure, the "*identification receiver*" would have first provided the wireless communication comprising the MAC address ("*the authenticated first identifier of the aerial system identifier signal*") to the "*permission module*."

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.f] Obvious

wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

- The combinations teach the components forming the *permission module* would have determined that a UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace*).

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.f] Obvious

- Whitmarsh discloses, or at least renders obvious, the “permission module” regardless of if it is subject to §112(f)
 - **Function:**
 - “determin[ing] that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace.”
 - Whitmarsh discloses that after its UAV defense system receives a MAC address from a UAV within its area, the UAV defense system determines if a countermeasure against the detected UAV should be performed “based on the identity and/or position of the detected UAV 14.”
 - **Structure:**
 - “storage on-board the disruption system, storage on-board the identification receiver, a remote computing system connected to the disruption system or any other suitable computing system programmed to compare an aerial system parameter, such as an identifier, with the permissions for the airspace.”
 - Whitmarsh’s computer system or processor performs comparing MAC addresses of UAVs with information and data relating to prior detection and countermeasures activities (permissions) to allow the system to identify troublesome or suspect UAVs.

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.g] Obvious

a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

- The combinations teach a disruption of the detected UAV provided by a countermeasures system would have occurred when the components forming the permission module determine that the UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in an airspace*)

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.g] Obvious

- The combinations further teach that Whitmarsh's countermeasures system (*disruption system*) disrupts operation of the UAV by forcing it to land (*configured to disrupt an operation of the unmanned aerial system*), as taught by Gong637, when the authentication of the UAV's MAC address fails and authenticity of the UAV's MAC address is not verified ((ii) *when the authenticity of the first identifier is not verified*).

the entire flight path. In some instances, when the UAV flies at location where the UAV can directly communicate with the communication network, the identification of the UAV may be authenticated by checking and confirming the identification with an authentication center on the communication network. For instance, if the authentication fails, the UAV may be forced to land. Optionally, when the UAV flies at location where the UAV cannot directly communicate with the communication network, the

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.g] Obvious

- The combinations further teach *wherein the disruption system is preemptively enabled based on the received aerial system identifier signal*.

Whitmarsh (Grounds 7B and 9B)

- A POSITA would have understood that in first determining a countermeasure in response to receiving a wireless communication including the MAC address of an unauthorized UAV ("*the received aerial system identifier signal*") that is 5 miles from a protected asset, Whitmarsh's countermeasure system ("*disruption system*") is **"*preemptively enabled*" because it is enabled before the detected UAV is within range of a protected asset, thereby allowing the countermeasures system time to develop and deploy an appropriate countermeasure** before the detected UAV is proximate to, and at risk of damaging or otherwise interfering with, the protected asset.

PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render [10.g] Obvious

- The combinations further teach *wherein the disruption system is preemptively enabled based on the received aerial system identifier signal*.

Whitmarsh and Goodrich (Grounds 7C and 9C)

- In the combined Whitmarsh-Goodrich system, the process of launching an interceptor UAV (as described by Goodrich) upon receiving a UAV signature (e.g., MAC address) ("*the received aerial system identifier signal*") from a UAV (as described by Whitmarsh) constitutes "***preemptively enabl[ing]***" the interceptor UAV "***based [on] the received aerial system identifier signal,***" because the interceptor UAV is deployed (i.e., launched) before an "engagement decision" is made to actually disrupt the detected UAV.

Claim 11: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 11 Obvious

The system of claim 10, wherein the identifier transmission system and the identification receiver communicate using a radio chipset that is compatible with a communication protocol selected from the following: WiFi, LTE, or Bluetooth.

- Whitmarsh discloses a drone defense system that monitors wireless communications for signals transmitted by UAVs that include information that identifies the UAVs.
 - The signals may be transmitted according to the WiFi protocol.
- A POSITA would have understood, or at least found obvious, that Whitmarsh's "identifier transmission system" and "identification receiver" use a "radio chipset that is compatible with" the WiFi communication protocol.

Claim 12: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 12 Obvious

The system of claim 10, wherein the identification receiver is a mobile device.

- Whitmarsh discloses that its UAV defense system may be deployed in a variety of mobile environments, including “on an aircraft to protect such aircraft against UAVs,” and “[s]ea-based applications” such as on a “ship or vessel.”
- A POSITA would have understood that in such implementations, Whitmarsh’s “identification receiver” would be a “mobile device,” because it is located on a mobile vehicle such as an aircraft or a ship.

Claim 14: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 14 Obvious

The system of claim 10, wherein when the disruption system is enabled the aerial system is caused to be removed from the airspace.

- Whitmarsh discloses developing and deploying various countermeasures against a detected UAV, including an “intercept countermeasure” wherein the countermeasures system “may dispatch one or more security vehicles 44 and operate it so that it actually collides with the detected UAV 14.”
- A POSITA would have understood that when the intercept countermeasure is executed, the collision between the dispatched security vehicle(s) and the detected UAV would have resulted in damage such that it would have been “removed from the airspace” (e.g., due to falling to the ground).

Claim 15: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 15 Obvious

The system of claim 10, wherein the disruption system comprises of a projectile launcher and an interdiction module.

- Whitmarsh Provisional (EX1006), incorporated by reference in Whitmarsh, discloses an intercept countermeasure performed by the countermeasures system wherein “armed drone systems” are deployed to “intercept (e.g., shoot down) the unauthorized or hostile drone.”
- A POSITA would have understood, or at least found obvious, that Whitmarsh’s UAV defense system comprises armed drone systems that include a “projectile launcher” and projectiles (“interdiction module[s]”) used to “shoot down” the detected UAV.
 - This understanding is consistent with the ‘199 Patent, which identifies “a set of masses (e.g., bullets) that physically intercept the aerial system motive mechanism and/or electronics” as “a second variation” of “the interdiction module.”

Claim 16: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 16 Obvious

The system of claim 10, wherein the disruption system comprises of an interceptor drone coupled with an interdiction module.

- Whitmarsh's countermeasures system ("*the disruption system*") comprises an armed drone system that shoots down a detected UAV.
- A POSITA would have understood, or at least considered it obvious, that the armed drone system comprises ("is coupled with") a "projectile launcher" that shoots projectiles ("an interdiction module") at the detected UAV.

Claim 17: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 17 Obvious

The system of claim 10, further comprising a control system for controlling the disruption system.

- Whitmarsh's countermeasures system may develop a "commandeer countermeasure" wherein the detected UAV is caused "to follow instructions from the UAV defense system 10 rather than from the original operator of the detected UAV 14."
- A POSITA would have understood that to control a detected UAV in such a manner, the UAV defense system would implement a "control system" that provides instructions to the detected UAV through the countermeasure system.
- It would have been obvious to a POSITA to implement additional components, such as a "control system," to control the countermeasures system when implementing the commandeering countermeasure, as this measure involves providing instructions to the UAV, which a POSITA would have recognized is better handled by a distinct component.

Claim 18: PO Does Not Dispute that the Grounds 7B/7C and 9B/9C Combinations Render Claim 18 Obvious

The system of claim 10, further comprising a logging system that is configured to record activity of at least one of the identification receiver, the permission module, or the control system.

- Whitmarsh Provisional (EX1006) discloses recording “the signature of each non-recognized signature” received from a detected UAV.
- A POSITA would have understood that Whitmarsh discloses a “logging system” that records the reception of any non-recognized signatures (e.g., MAC address) by the “identification receiver.”
- Further, Whitmarsh discloses that “[l]ocal database 32 may also be used to store information and data relating to the operation of the UAV defense system 10 for subsequent analysis, troubleshooting, or system diagnostics.”
- A POSITA would have understood that this local database 32 operates as a “logging system” configured to record activity of the UAV defense system and its components. EX1003, ¶152. This is consistent with the ‘199 Patent. EX1001, 13:34-52.

Overview of Falk

Falk discloses a **"beacon"** that is **"attached to an unmanned aerial vehicle"** and "includes an attachment mechanism configured to **securely and removably attach the [beacon] to the unmanned aerial vehicle.**" The beacon includes "indicia" that "together form a unique identifier associating the owner or responsible party with the unmanned aerial vehicle." The beacon also includes a "remote communications module" that facilitates wireless communication "to and from a remote operator."

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine the Grounds 7B/7C and 9B/9C references with Falk

- A POSITA would have been motivated to implement Falk's "beacon" as the mechanism used by UAVs to transmit their identification information (e.g., MAC addresses)
 - Design incentives and market forces would have motivated a POSITA to implement Falk's beacon
 - A POSITA would have recognized the value of implementing Falk's beacon, which is capable of wireless communication according to various protocols, to improve a UAV's ability to wirelessly identify itself.
 - Incorporating Falk's beacon to transmit UAV identity information is applying a known technique (Falk's beacon for wireless communication of UAV identity information) to improve similar devices (Whitmarsh's UAVs transmitting identity information such as a MAC address) in the same way.

Substitute Dependent Claim 13

[[4]]13. The system of claim 10, wherein the identifier transmission system is configured to be reassigned from a first aerial system to a second aerial system.

Claim 13: PO Does Not Dispute that the Ground 8B/8C and 10B/10C Combinations Render Claim 13 Obvious

The system of claim 10, wherein the identifier transmission system is configured to be reassigned from a first aerial system to a second aerial system.

- Falk discloses a "beacon" that is "attached to an unmanned aerial vehicle" and "includes an attachment mechanism configured to securely and removably attach the [beacon] to the unmanned aerial vehicle."
- The beacon includes "indicia" that identifies an owner or responsible party of the UAV as well as the UAV itself.
- In the combination, Falk's beacon acts as the "identifier transmission system" that wirelessly transmits a MAC address of an associated UAV.
- Physical reassignment:
 - The beacon is configured to "securely and removably attach" to a UAV, meaning it can attach (and reattach) to multiple different UAVs..
- Electronic reassignment:
 - Changing the indicia of the beacon would be warranted when the beacon is removed from a first UAV and attached to a second UAV.

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine Whitmarsh, Viggiano, and Gong637 (Ground 11)/ Whitmarsh, Goodrich, Viggiano, and Gong637(Ground 13)

- The combinations would have provided that Whitmarsh's component for receiving wireless communications and the identification information **would have received**:
 - (1) **UAV aircraft identification information** that is the wireless communication signal including the MAC address of a UAV, from a **first communication unit of the UAV**, and
 - (2) **a message AC formed from identification information of the UAV and a secret key of the UAV**, from a **second communication unit of the UAV**
- Whitmarsh's computer system/processor/ component that identifies UAVs would have **verified an authenticity of the received UAV MAC address** by
 - (1) **forming a first message AC** using the received UAV MAC address and
 - (2) **comparing the first message AC to the received message AC**
 - a comparison match indicates the UAV's MAC address (identity) is verified
 - no match indicates authenticity is not verified— with Whitmarsh's countermeasures system disrupting operation of the UAV in such a case by forcing it to land

PO Does Not Dispute that a POSITA Would Have Been Motivated to Combine Whitmarsh, Viggiano, and Gong637 (Ground 11)/ Whitmarsh, Goodrich, Viggiano, and Gong637(Ground 13)

- A **known problem** in UAV systems was “**spoofing**” or **fraudulent UAV identities**. Bad actors using such techniques could gain access to unauthorized airspace.
- Whitmarsh, as well as Whitmarsh and Goodrich, teach using a UAV MAC address to identify a UAV,
 - Viggiano and Gong637 provide **enhancements by teaching identification authorization techniques** that would help ensure such a UAV MAC address is properly authenticated.
- Gong637 further teaches **basic and well-known communication techniques** of using separate communication units for different transmissions.
- The combinations represent application of known techniques (known aircraft identification authentication and communication techniques) to a known system (Whitmarsh/Whitmarsh and Goodrich systems) ready for improvement; the results would have been predictable with a reasonable expectation of success.

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.pre] Obvious

A discrimination system comprising:

- Whitmarsh describes a "UAV defense system" 10 that determines whether a UAV is authorized to be in a certain area.
- Whitmarsh's system "discriminates" between authorized/friendly and unauthorized/hostile drones to provide security to a protected area.

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.a] Obvious

an identifier transmission system coupled to an unmanned aerial system, wherein the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system

- Whitmarsh discloses a transmission system coupled to an unmanned aerial vehicle (UAV) (*an identifier transmission system coupled to an unmanned aerial system*).
- Whitmarsh discloses wireless communications transmitted by the UAVs transmission system comprise information or signatures unique to the UAV, such as a MAC address of the UAV, that is used to identify the transmitting UAV (*the identifier transmission system is configured to broadcast an aerial system identifier signal comprising a first identifier unique to the unmanned aerial system*).

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.b] Obvious

an identification system comprising an identification receiver

- A POSITA would have understood, or at least found obvious, that Whitmarsh's UAV defense system comprises a computer system, processor, or similar component that identifies UAVs based on their received MAC addresses (*identification system*)
- The system/processor/similar component would have further included the parts forming an identification receiver that receives wireless communications and identification information (e.g., the MAC addresses) contained therein that is transmitted by UAVs (*identification system comprising an identification receiver*)

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.c] Obvious

a permission module,

- Whitmarsh discloses, or at least renders obvious, "*a permission module*," as addressed in Limitation [10.f], discussed below.

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.e1] Obvious

wherein the identification system is configured to determine the first identifier from the aerial system identifier signal, and verify an authenticity of the first identifier using the second identifier, and to provide an authenticated first identifier of the aerial system identifier signal when the authenticity has been verified, and

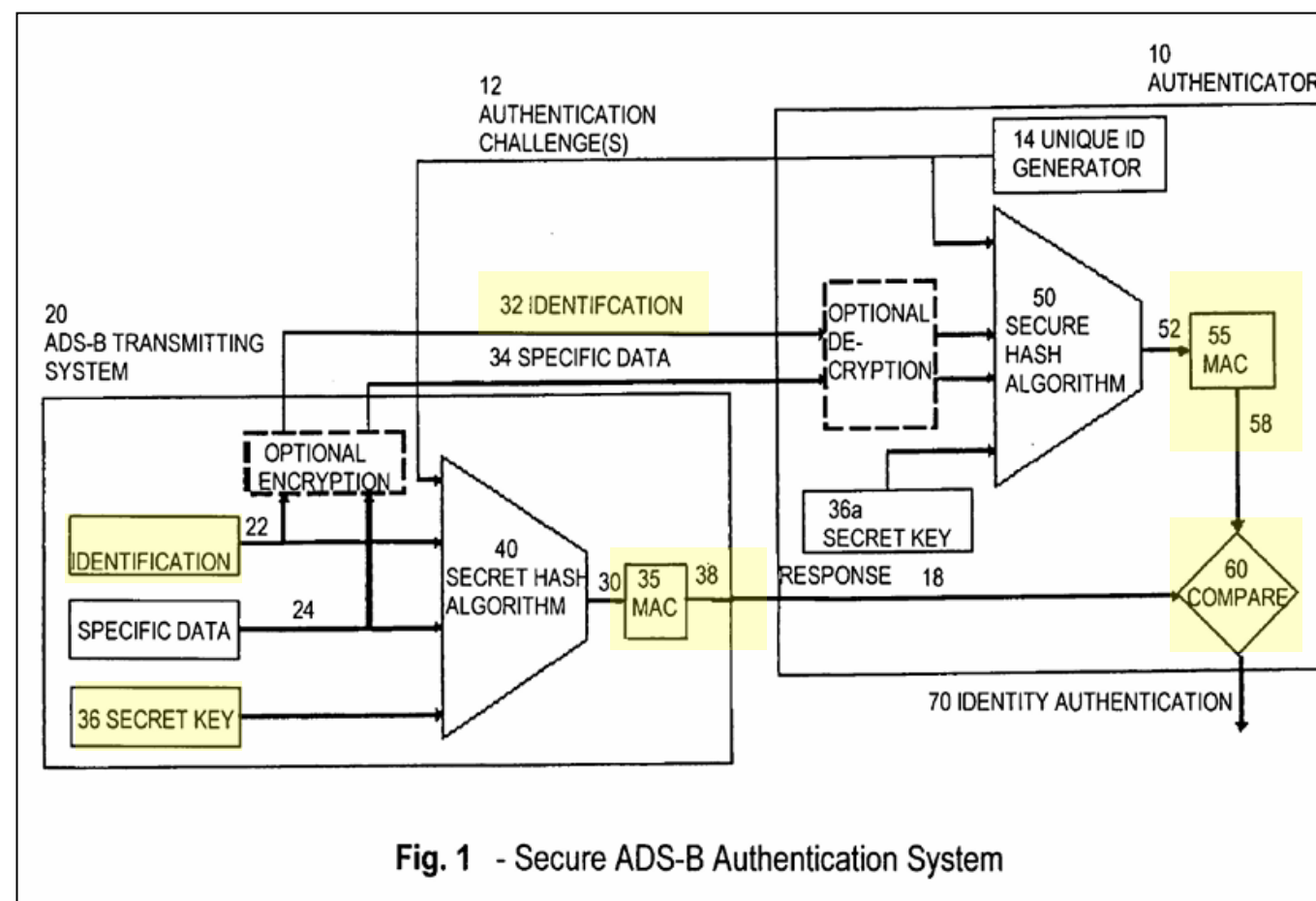
- The combinations teach Whitmarsh's computer system/processor/ component that identifies UAVs (*identification system*) would have verified an authenticity of the UAV's MAC address by
 - (1) forming a first message AC using the received UAV MAC address and
 - (2) comparing the first message AC to the received message AC, where a match indicates the UAV's MAC address (identity) is verified (*configured to...verify an authenticity of the first identifier using the second identifier*).
- A POSITA would have understood or at least found obvious that Whitmarsh's computer system/processor/ component (*the identification system*) would have deciphered the received MAC address from the wireless communications it was contained in (*is configured to determine the first identifier from the aerial system identifier signal*).
- Successful authentication would have resulted in Whitmarsh's UAV MAC address having been authenticated and thus provided by Whitmarsh's identification system an authenticated UAV MAC address (*to provide an authenticated aerial system identifier of the aerial system identifier signal when the authenticity has been determined and verified*).

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.e1] Obvious

- EX1007 (Viggiano), ¶¶0014-0015, Fig. 1

approximately every second by ADS-B UAT equipped aircraft and vehicles. Authenticator 10 may receive an ADS-B transmitter's ID 22 and specific data 24 after transmitting the authentication challenge 12.

[0015] When the Authenticator 10 receives the ADS-B transmitter's authentication response 18, in either encrypted or unencrypted form, the Authenticator 10 inputs the locally generated unique identifier, with the received ADS-B transmitter's ID 32, and specific data 34 and the secret-key 36a into a secure hash generator 50, to generate an Authenticator-generated secure hash value 52. The secure hash value 52 is input into the MAC generation processing 55 to generate an Authenticator-generated MAC 58. The Authenticator's system applies the received ADS-B transmitter-generated MAC 38 and the Authenticator-generated MAC 58 to comparator 60 to authenticate the ADS-B transmitter's 20 identity. If the MAC 38 received from the ADS-B transmitter 20 matches the Authenticator-generated MAC 58, an authentication signal 70 is produced indicating that the identity of the ADS-B transmitter is authenticated. In one embodiment of the present invention, if an ADS-B transmitter 20 fails two or more consecutive authentication response comparisons, the Authenticator 10 notifies a responsible higher command authority of the authentication failures, so that the responsible higher command authority can respond appro-



PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.e2] Obvious

to provide the authenticated first identifier of the aerial system identifier signal to the permission module, and

- The combinations would have provided the authenticated UAV MAC address to the components forming the permission module (*to provide the authenticated aerial system identifier of the aerial system identifier signal to the permission module*).

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.f] Obvious

wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace; and

- Successful authentication results in an authenticated UAV MAC address
- The components forming the permission module would determine a UAV associated with the authenticated UAV MAC address is not authorized to be in a particular area (*wherein the permission module is configured to determine that the unmanned aerial system associated with the authenticated first identifier of the aerial system identifier signal is not permitted to be in an airspace*).

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.g] Obvious

a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in the airspace, or (ii) when the authenticity of the first identifier is not verified, wherein the disruption system is preemptively enabled based on the received aerial system identifier signal.

- The combinations teach a countermeasures system disrupts detected UAV operation when the components forming the permission module determine the UAV associated with the authenticated UAV MAC address is not authorized for a particular area (*a disruption system configured to disrupt an operation of the unmanned aerial system (i) when it is determined by the permission module that the unmanned aerial system associated with the authenticated first identifier is not permitted to be in an airspace*).
- The countermeasures system (*disruption system*) disrupts the UAV's operation by forcing it to land (*configured to disrupt an operation of the unmanned aerial system*) when the authentication comparison involving the UAV MAC address fails and authenticity of the UAV's MAC address is not verified (*(ii) when the authenticity of the first identifier is not verified*).

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.g] Obvious

- The combinations further teach *wherein the disruption system is preemptively enabled based on the received aerial system identifier signal*.

Whitmarsh (Ground 11)

- A POSITA would have understood that in first determining a countermeasure in response to receiving a wireless communication including the MAC address of an unauthorized UAV ("*the received aerial system identifier signal*") that is 5 miles from a protected asset, Whitmarsh's countermeasure system ("*disruption system*") is **"*preemptively enabled*" because it is enabled before the detected UAV is within range of a protected asset, thereby allowing the countermeasures system time to develop and deploy an appropriate countermeasure** before the detected UAV is proximate to, and at risk of damaging or otherwise interfering with, the protected asset.

PO Does Not Dispute that the Grounds 11 and 13 Combinations Render [10.g] Obvious

Whitmarsh and Goodrich (Ground 13)

- In the combined Whitmarsh-Goodrich system, the process of launching an interceptor UAV (as described by Goodrich) upon receiving a UAV signature (e.g., MAC address) ("*the received aerial system identifier signal*") from a UAV (as described by Whitmarsh) constitutes "***preemptively enabl[ing]***" the interceptor UAV "***based [on] the received aerial system identifier signal,***" because the interceptor UAV is deployed (i.e., launched) before an "engagement decision" is made to actually disrupt the detected UAV.

Substitute Dependent Claims 11-12 and 14-18

[[2]]11. The system of claim 10, wherein the identifier transmission system and the identification receiver communicate using a radio chipset that is compatible with a communication protocol selected from the following: WiFi, LTE, or Bluetooth.

[[3]]12. The system of claim 10, wherein the identification receiver is a mobile device.

[[5]]14. The system of claim 10, wherein when the disruption system is enabled the aerial system is caused to be removed from the airspace.

[[6]]15. The system of claim 10, wherein the disruption system comprises of a projectile launcher and an interdiction module.

[[7]]16. The system of claim 10, wherein the disruption system comprises of an interceptor drone coupled with an interdiction module.

[[8]]17. The system of claim 10, further comprising a control system for controlling the disruption system.

[[9]]18. The system of claim [[8]]10, further comprising a logging system that is configured to record activity of at least one of the identification receiver, the permission module, or the control system.

Substitute Claims 11, 12, and 14-18

- Grounds 11 and 13 render obvious substitute claims 11, 12, and 14-18 for the same reasons discussed above for Grounds 7B/7C and 9B/9C