

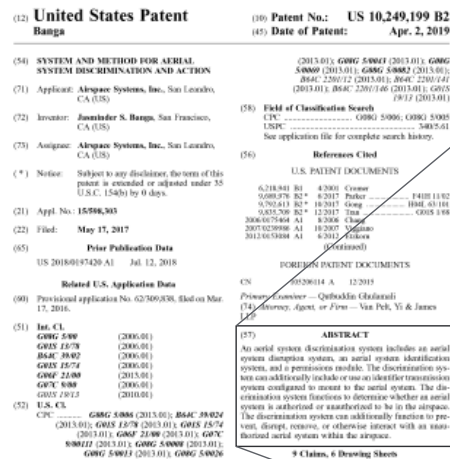
Patent Owner's Demonstratives for Oral Hearing

Case No. IPR2025-00530
U.S. Patent No. 10,249,199

List of Exhibits Cited

EX1001	EX2002
EX1024	EX2005
EX1025	EX2009
EX1026	

U.S. Patent No. 10,249,199



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.

 PRINCE LOBEL

Proposed Substitute Claim 10 (Revised Motion to Amend)

[[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.

Written Description & Definiteness – limitation 10.d

- “a second identifier received from a computing system that is remote relative to the discrimination system”
 - Identifiers can be dynamic, generated by remote computing system
 - Identifiers are received by identification receiver 102 – no requirement that they be “directly” received
 - Claim matches description: identifier originating from remote computing system is received by identification receiver
 - Disclosed example of receiving ID relayed through drone is sufficient disclosure of species for genus claim

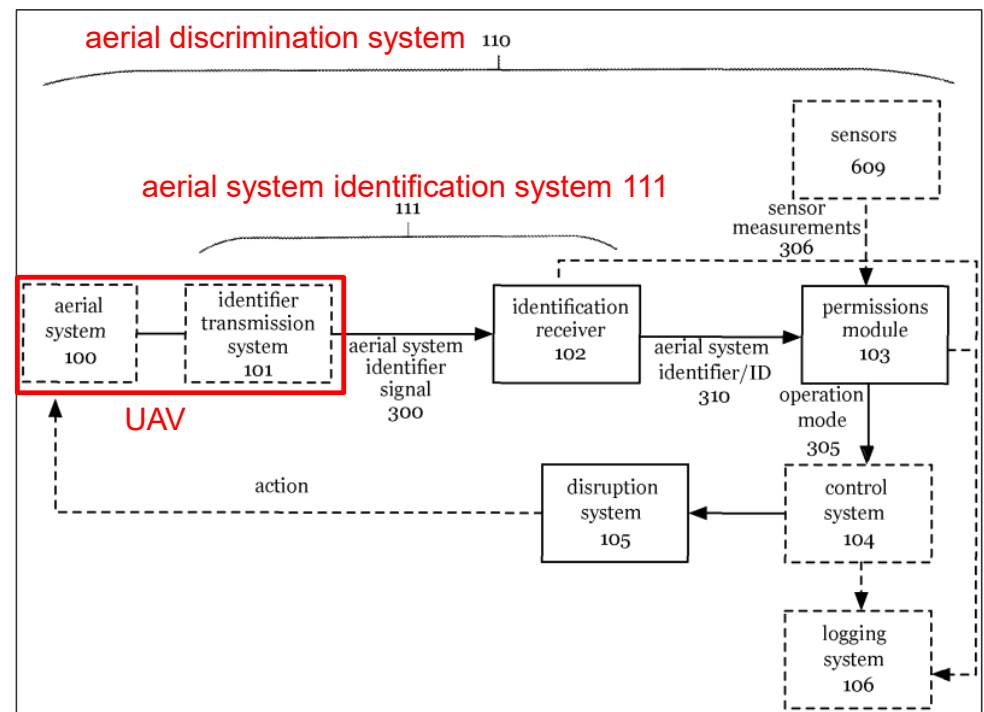
The discrimination system 110 can additionally include an identifier transmission system 101 that functions to mount to an aerial system 100 and **transmit an aerial system identifier signal 300 to the identification receiver 102**. ... The aerial system identifier 310 is preferably **dynamic**, but can alternatively be static. **Dynamic aerial system identifiers can be generated, re-assigned**, calculated (e.g., based on a static identifier and a changing equation; based on changing identifier and a static equation; based on static identifier, a static equation, and a changing factor, such

as a timestamp or a GPS coordinate, etc.), or otherwise determined at a predetermined frequency, in **response to the occurrence of a trigger event** (e.g., upon user reassignment of the identifier transmission system 101 to a different aerial system), or at any other suitable time. The dynamic aerial system identifier can be generated on-board the aerial system 100, **generated remotely (e.g., at a remote computing system, etc.;** updated in-flight or when connected to a predetermined communication connection type, etc.), or generated by any other suitable system.

Written Description & Definiteness – limitation 10.d (cont.)

- “a second identifier received from a computing system that is remote relative to the discrimination system”
 - Discrimination system includes a drone and ground-based system to ID and disrupt drones
 - “remote computing system” is not described or depicted as part of aerial discrimination system 110
 - No *in haec verba* requirement for written description

As shown in FIG. 1, the **aerial discrimination system 110** includes an aerial system **disruption system 105**, an aerial system **identification system 111**, and a **permissions module 103**. The discrimination system 110 can additionally include or use an **identifier transmission system 101** configured to mount to, or be embedded in, an **aerial system 100**.



Written Description & Definiteness – limitation 10.d (cont.)

- “a second identifier received from a computing system that is remote relative to the discrimination system”
 - In addition to first identifier, there can be a second identifier acting as a second factor identifier

Fourth, in **some variations**, the aerial system 100 can include a first and **second identifier**, transmitted by a first and second identifier transmission system, respectively, wherein **the second identifier** can function as a **backup identifier** (e.g., in case the primary identifier transmission system is inoperable), a **second factor identifier for the aerial system 100** (e.g., as a secondary authenticator for the aerial system to prevent tampering and/or identifier reproduction), an identifier for a **secondary identification system** (e.g., a user device-compatible identifier), or be used in any other suitable manner.

Ex. 2002, 4:15-22 (cited by Paper 34 at 1, Paper 25 at 7)

Written Description – limitation 10.e2

- “provide the authenticated first identifier of the aerial system identifier signal to the permission module”
 - The first identifier is authenticated before it is provided to the permissions module

The chipset 608 of the identification receiver 102 functions to interpret the received aerial system identifier signal 300. The **chipset 608 preferably interprets the signal 300 into the aerial system identifier 310** (e.g., decrypts the signal, etc.), but can alternatively interpret the signal 300 into a set of data indicative of the identifier 310, or otherwise interpret the signal 300.

Ex. 2002, 9:13-17 (cited by Paper 34 at 3, Paper 25 at 9)

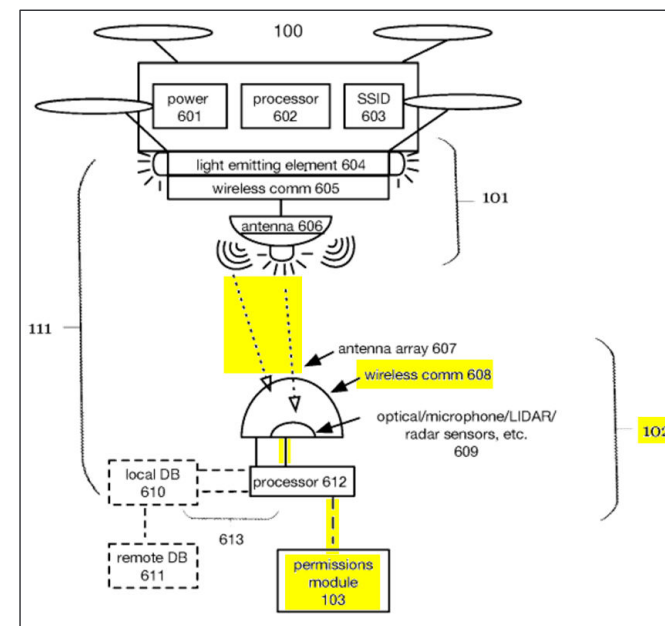
4.3 Authenticating an Aerial System

Determining an aerial system identifier 310 can optionally include verifying the authenticity of the aerial system identifier 310.

© 2020 Prince Lobel Tye LLP

Ex. 2002, 30:17-18 (cited by Paper 34 at 3, Paper 25 at 9)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE



Ex. 2002, Fig. 6 (cited by Paper 25 at 9)

Written Description – limitation 10.e2

- “provide the authenticated first identifier of the aerial system identifier signal to the permission module”
 - Authenticating identifiers occurs prior to permissions

4.3 Authenticating an Aerial System

Determining an aerial system identifier 310 can optionally **include verifying the authenticity of the aerial system identifier 310**.

Ex. 2002, 30:17-18 (cited by Paper 34 at 3, Paper 25 at 9)

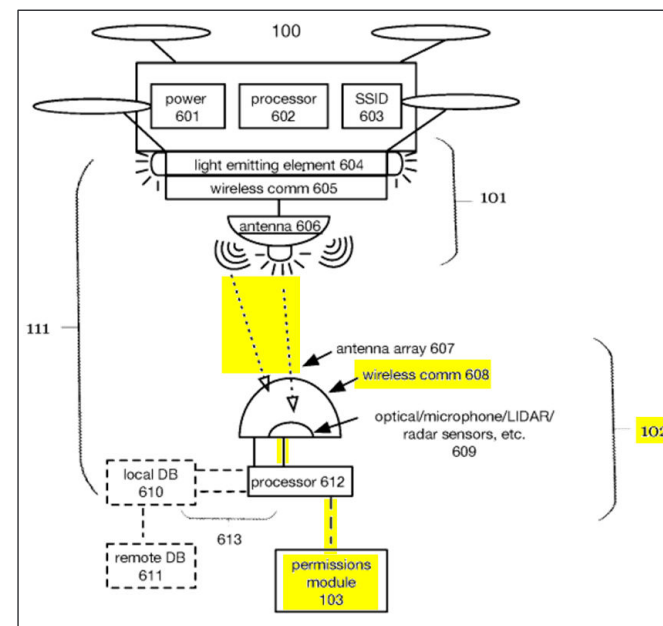
4.4 Permissioning an Aerial System

Determining a set of permissions associated with the restricted airspace functions to identify metrics by which to **determine whether the aerial system 100 is permitted** within the airspace. Determining the set of permissions associated with the restricted airspace preferably includes ... determining the permissions associated with the airspace identifier

© 2020 Prince Lobel Iye LLP

Ex. 2002, 32:19-33:1 (cited by Paper 25 at 10)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE



Ex. 2002, Fig. 6 (cited by Paper 25 at 9)

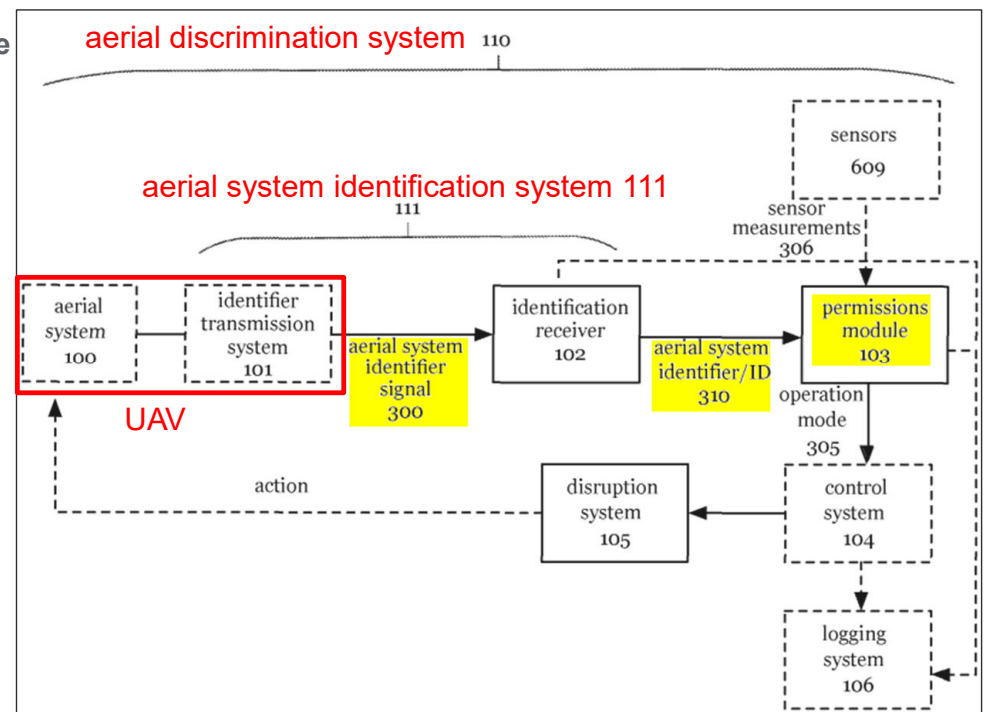
PRINCE LOBEL

Written Description – limitation 10.e2 (cont.)

- “provide the authenticated first identifier of the aerial system identifier signal to the permission module”
 - After it is processed (including being authenticated), the first identifier is provided to the permissions module

chipset 608 can be connected to the permissions module 103, wherein the chipset 608 sends the raw or **processed signal to the permissions module 103** for permissions determination

Ex. 2002, 9:20-22
(cited by Paper 34 at 3, Paper 25 at 9)



Definiteness – limitation 10.g

- “... wherein the disruption system is preemptively enabled based on the received aerial system identifier signal”
 - “preemptively enabled” has a well-understood ordinary meaning

58. The commonly understood meaning of the word “preemptively” is “to seize upon to the exclusion of others.” EX2025. Preemption also means “to prevent from happening or taking place,” i.e., to “forestall” or to “preclude.” *Id.* The ’199 patent discloses a preemption process that is consistent with this well understood meaning of preemptive.

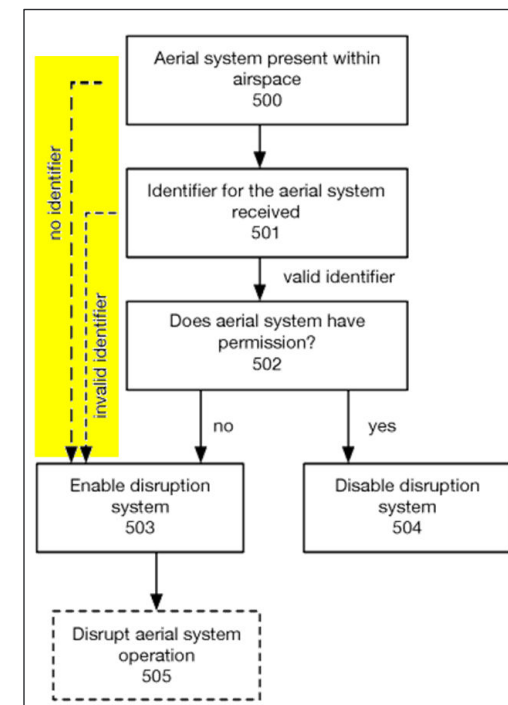
Ex. 2005 ¶ 58
(cited by Paper 34 at 4)

Definiteness – limitation 10.g (cont.)

- “... wherein the disruption system is preemptively enabled based on the received aerial system identifier signal”
 - The specification provides clear guidance as to “preemptively enabled”

In another example, certain scenarios may require the disruption system 105 to be ready to **engage on short notice**. As depicted in FIG. 5, the **disruption system 105** may thus be **preemptively enabled** if certain conditions are met (e.g. aerial system detected w/o an identifier 500, identifier is received but is invalid 501, identifier is valid but is not permissioned 502, etc.). Such a configuration would minimize any delays associated with powering on the disruption system 105 and thus allow the system to respond to fast moving aerial systems 100.

Ex. 2002, 36:20-37:2
(cited by Paper 34 at 5)



Ex. 2002,
Fig. 5
(cited by
Paper 34 at 5)

Definiteness – limitation 10.g

- “... wherein the disruption system is preemptively enabled based on the received aerial system identifier signal”
 - “preemptively enabled” has a well-understood ordinary meaning

94. The '199 patent discloses a preemption process that is consistent with the commonly understood meaning of that term. The '199 patent's system seizes upon the aggressive option of taking a disruptive action to the exclusion of other less aggressive options, such as communicating with the aerial system, allowing it to leave airspace, etc. *See supra* § VII.B. Thus, the less aggressive options are forestalled or precluded. This may prevent an unauthorized aerial vehicle from continuing its operation in a restricted airspace, which the aerial vehicle could have accomplished if one of the less aggressive options were chosen instead of preemptively enabling the disruption system.

95. As FIG. 5 depicts, and the discussion of “preemptively enabled” in the specification states, in certain more time-sensitive situations, a disruption system may be enabled without exercising the less aggressive options described above. For example, as soon as it is determined that a received identifier is not authenticated, the disruption system may be enabled, without ever allowing the UAV to leave the airspace voluntarily after communication occurs between the UAV's pilot and the disruption system. *See* EX2002, 37:8-18; EX1001, 18:31-47. Moreover, if a UAV does not provide an identifier, and none is detected by the identification system, the disruption system may also be enabled without even contacting the pilot of the UAV. *See* EX2002, 37:8-18; EX1001, 19:31-47. It is the omission of such less aggressive options “if certain conditions are met” that causes the disruption system to be *preemptively enabled*. Thus, the specification both clearly describes and depicts clearly the “preemptively enabled” feature of the disruption system.

Non-Obviousness – Jarrell Grounds (MTC1) fail to Disclose 10.d or 10.e1

- Jarrell does not disclose or suggest a “second identifier”
- The opposition identifies Jarrell’s “list” as the second identifier

aerial system) as well as (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*). EX1025, 10:53-59, 11:49-55, 12:12-17, 12:47-65,

Paper 32 at 13

- A list does not *identify* a particular UAV

Non-Obviousness – Jarrell Grounds (MTC1) fail to Disclose 10.d or 10.e1

- Jarrell does not disclose or suggest a “the second identifier functioning as a second factor identifier for the unmanned aerial system”
- “multi factor” authentication and use of “second factor” has well-known meaning in art:

4.3. Tokens

The classic paradigm for authentication systems identifies **three factors as the cornerstone of authentication:**

- **Something you know** (for example, a password)
- **Something you have** (for example, an ID badge or a cryptographic key)
- **Something you are** (for example, a fingerprint or other biometric data)

Multi-factor authentication refers to the **use of more than one of the factors** listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that **use two factors** are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors. (As discussed in Section 4.1, other types of information, such as location data or device identity, may be used by an RP or Verifier to reject or challenge a claimed identity, but they are not considered authentication factors.)

Ex. 2009 at 20
(quoted by Ex. 2005 ¶ 46,
cited by Paper 34 at 7)

- Petitioner and its expert essentially ignore the “acting as a second factor” limitation, identify no other interpretation

Non-Obviousness – Jarrell Grounds (MTC1) fail to Disclose 10.d or 10.e1

- Jarrell does not disclose or suggest a “the second identifier functioning as a second factor identifier for the unmanned aerial system”

- Jarrell’s two instances of the same MAC address do not constitute a “first” and “second” factor:

107. Second, as I explained above, in the context of authentication, if one identifier is one factor, e.g., something you have,” the “second” factor must be something other than “something you have.” The second factor must either be “something you know” or “something you are.” *See supra* § VI. In the proposed combination, the first identifier is a MAC address, i.e., “something you have.” A matching identifier in Jarrell’s list of MAC identifier is not a different factor. In fact, it is not even a different instance of the “what you have” factor; it is the same identifier. Therefore, Jarrell does not teach a “second identifier functioning as a second factor identifier.”

Ex. 2005 ¶ 107
(cited by Paper 34 at 7)

- Petitioner and its expert essentially ignore the “acting as a second factor” – present no contrary analysis

Non-Obviousness – Jarrell Grounds (MTC1) fail to Disclose 10.d or 10.e1

- Jarrell does not disclose or suggest “verify an authenticity of the first identifier using the second identifier” ... “the second identifier functioning as a second factor identifier”

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

Ex. 1025 at 13:28-32 (cited by Paper 32 at 7)

- Conventional single-factor authentication of the UAV
- Checking ID against list does nothing to authenticate the *identifier* itself, e.g. against “identifier reproduction” (cloned or stolen IDs)

Non-Obviousness – Pasko Grounds (MTC2) fail to Disclose 10.d or 10.e1

- Pasko does not disclose or suggest “verify an authenticity of the first identifier using the second identifier” ... “the second identifier functioning as a second factor identifier”
- Conventional single-factor authentication of the UAV
- Checking UAV’s credentials against list does nothing to authenticate the *credentials* themselves, e.g. against “identifier reproduction” (cloned or stolen credentials)
 - Just checking if UAV is permitted in airspace
- Petitioner identifies no motivation to modify Pasko to authenticate *identifiers* instead of authenticating the *UAV*

[0010] As further shown in FIG. 1A, user A may instruct user device A (or the UAV) to generate a request for a flight path (e.g., from location A to location B) for the UAV, and to provide the request to the UAV platform. The request may include credentials (e.g., a serial number, an identifier of a universal integrated circuit card (UICC), etc.) associated with the UAV. The UAV platform may utilize the UAV credentials to determine whether the UAV is authenticated for utilizing the UAV platform and/or one or more of the networks, and is registered with an appropriate authority (e.g., a government agency) for use. For example, the UAV platform may compare the UAV credentials with UAV account information (e.g., information associated with authenticated and registered UAVs) provided in the data storage to determine whether the UAV is authenticated. As shown in FIG. 1A, assume that the UAV is authenticated, and that the UAV platform provides a message indicating that the UAV is authenticated to one or more of the networks (e.g., to the wireless network). The UAV may connect with the wireless network, the satellite network, and/or the other networks based on the authentication of the UAV.

Non-Obviousness – Pasko Grounds (MTC2) fail to Disclose 10.d or 10.e1

- Pasko does not disclose or suggest a “the second identifier functioning as a second factor identifier for the unmanned aerial system”
- Pasko’s “account information,” “government registration number,” and “keys” are all same factor, not “second factor”

121. Additionally, *none* of UAV’s serial number, government registration number, and any of the keys that Pasko describes, is a “*second factor* identifier.” This is because, each of these identifiers (to the extent a key can be considered an identifier), belongs to the category “what you have.” None of these entities is “something you know” or “something you are.” As such, none of these entities can function as a “second factor identifier” with respect to any of the entities. *See supra* § VI.

Ex. 2005 ¶ 121
(cited by Paper 34 at 10)

- Petitioner and its expert essentially ignore the “acting as a second factor” limitation, identify no other interpretation

Non-Obviousness – Viggiano-Gong637 Grounds fail to Disclose 10.d or 10.e1

- The Viggiano-Gong 637 combinations do not disclose or suggest the “identification receiver is configured to receive... a second identifier from a computing system that is *remote relative to the discrimination system*”

89. The combinations would have thus 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, as well as (2) a message authentication code formed from identification information of the UAV and a secret key of the UAV, from a second communication unit of the UAV. Sections XIV.G.2.a ([10.a]),

Ex. 1024 at ¶ 89
(cited by Paper 32 at 21)

- Petitioner’s theory has both alleged “identifier[s]” originating from the UAV’s communication units
- That is not “remote relative to the discrimination system” because the claimed discrimination system includes “an identifier transmission system coupled to an unmanned aerial system”

Non-Obviousness – Viggiano-Gong637 Grounds fail to Disclose 10.d or 10.e1

- Neither Viggiano nor Gong 637 discloses or suggests a “the second identifier functioning as a second factor identifier for the unmanned aerial system”
- MAC address and message authentication code do not constitute a “first” and “second” factor:

127. Additionally, the message authentication code 38 is generated from Whitmarsh’s MAC ID. The message authentication code 38 and the MAC ID are both “something you have.” As such, neither of these can function as a “second factor identifier” with respect to the other. *See supra* § VI.

Ex. 2005 ¶ 127
(quoted by Paper 34 at 12)

- Petitioner and its expert essentially ignore the “acting as a second factor” limitation, identify no other interpretation