

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AXON ENTERPRISE, INC. AND DEDRONE HOLDINGS, INC.
Petitioners

v.

AIRSPACE SYSTEMS, INC.
Patent Owner

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

PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-9 OF
U.S. PATENT NO. 10,249,199

TABLE OF CONTENTS

I.	MANDATORY NOTICES	1
II.	STANDING AND FEES	2
III.	OVERVIEW OF THE '199 PATENT	2
	A. Subject Matter of the '199 Patent.....	2
	B. Prosecution History and Priority Date of the '199 Patent.....	5
IV.	SUMMARY OF PRIOR ART	6
	A. Whitmarsh (EX1005)	6
	B. Viggiano (EX1007)	8
	C. Goodrich (EX1008).....	8
	D. Falk (EX1011).....	9
	E. Summary of Grounds	10
V.	LEVEL OF ORDINARY SKILL.....	10
VI.	CLAIM CONSTRUCTION.....	11
VII.	INSTITUTION IS PROPER	13
	A. The Fintiv Factors Favor Institution under §314(a).....	13
	B. Institution is Proper under §325(d)	15
VIII.	THE CHALLENGED CLAIM IS UNPATENTABLE.....	15
	A. Ground 1: Whitmarsh Renders Obvious Claims 1-3 and 5-9	15
	1. Claim 1	15
	2. Claim 2	27
	3. Claim 3	28
	4. Claim 5	29
	5. Claim 6	29
	6. Claim 7	31
	7. Claim 8	32
	8. Claim 9	33
	B. Ground 2: The Combination of Whitmarsh and Falk Renders Obvious Claim 4	35
	1. Motivation to Combine	35

Petition for *Inter Partes* Review of U.S. Patent No. 10,249,199

2.	Claim 4.....	37
C.	Ground 3: The Combination of Whitmarsh and Goodrich Renders Obvious Claims 1-3 and 5-9.....	40
1.	Motivation to Combine.....	40
2.	Claim 1	44
3.	Claim 2	47
4.	Claim 3	48
5.	Claim 5	48
6.	Claim 6.....	49
7.	Claim 7.....	50
8.	Claim 8.....	50
9.	Claim 9.....	51
D.	Ground 4: The Combination of Whitmarsh, Goodrich, and Falk Renders Obvious Claim 4	51
1.	Motivation to Combine.....	51
2.	Claim 4.....	51
E.	Ground 5: The Combination of Viggiano and Goodrich Renders Obvious Claims 1, 3, and 5-9.....	51
1.	Motivation to Combine.....	51
2.	Claim 1	55
3.	Claim 3	65
4.	Claim 5	65
5.	Claim 6.....	66
6.	Claim 7	66
7.	Claim 8.....	66
8.	Claim 9.....	67
F.	Ground 6: The Combination of Viggiano, Goodrich, and Falk Renders Obvious Claim 4	69
1.	Motivation to Combine.....	69
2.	Claim 4.....	71
IX.	OBJECTIVE INDICIA DO NOT SUPPORT PATENTABILITY	73

X.	CONCLUSION	73
-----------	-------------------------	-----------

LIST OF EXHIBITS

Ex. No. ¹	Description
1001	U.S. Patent No. 10,249,199 to Banga, “System and Method for Aerial System Discrimination and Action” (the “199 Patent”)
1002	File History for U.S. Patent No. 10,249,199
1003	Declaration of Dr. Girish Chowdhary
1004	Complaint for Patent Infringement, <i>Airspace Systems, Inc. v. Dedrone Holdings, Inc.</i> , Case No. 1-24-cv-01625 (E.D. VA), September 16, 2024
1005	U.S. Patent Application Publication No. 2019/0003807 to Whitmarsh <i>et al.</i> , “UAV Defense System,” (“ <i>Whitmarsh</i> ”) filed December 8, 2016 and published January 3, 2019
1006	U.S. Provisional Application No. 62/267,393 to Whitmarsh <i>et al.</i> , “UAV Defense System,” (“ <i>Whitmarsh Provisional</i> ”), filed December 15, 2015
1007	U.S. Patent Application Publication No. 2007/0239986 to Viggiano <i>et al.</i> , “Secure ADS-B Authentication System and Method,” (“ <i>Viggiano</i> ”) filed April 7, 2006 and published October 11, 2007
1008	U.S. Patent Application Publication No. 2016/0023760 to Goodrich, “Systems and Methods Countering an Unmanned Aerial Vehicle,” (“ <i>Goodrich</i> ”) filed July 16, 2015 and published January 28, 2016
1009	U.S. Patent No. 10,733,894 to Beard <i>et al.</i> , “Direct-broadcast Remote Identification (RID) Device for Unmanned Aircraft Systems (UAS),” filed February 26, 2018 and issued August 4, 2020
1010	U.S. Provisional Application No. 62/209/221 to Beard, “Automatic Dependent Surveillance Broadcast Transmission within Whitespace,” filed August 24, 2015

¹ Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to Exhibit 1002 are made with reference to the Bates-stamped pagination; citations to other exhibits are made to the page number of the document itself.

Petition for *Inter Partes* Review of U.S. Patent No. 10,249,199

1011	U.S. Patent No. 9,805,238 to Falk <i>et al.</i> , “System for Identifying and Controlling Unmanned Aerial Vehicles,” (“ <i>Falk</i> ”) filed July 11, 2016 and issued October 31, 2017
1012	U.S. Provisional Application No. 62/301,858 to <i>Falk</i> , “System for Identifying and Controlling Unmanned Aerial Vehicles (“ <i>Falk Provisional</i> ”), filed March 1, 2016
1013	Claim Listing of Challenged Claims
1014	Kayton, Myron and Fried, Walter, <i>Avionics Navigation Systems</i> , John Wiley and Sons, 1997.
1015	International Publication No. WO2016/154949 A1 to Gong <i>et al.</i> , “Authentication Systems and Methods for Generating Flight Regulations,” filed March 31, 2015 and published October 6, 2016
1016	International Publication No. WO2015/043123 A1 to Wang <i>et al.</i> , “Data Communication Systems and Methods,” filed January 14, 2014 and published April 2, 2015
1017	Burnside, Joseph E., “ADS-B Out: 978 UAT Or 1090ES?,” AviationSafety Magazine, published March 15, 2016.
1018	Nichols, Randall et al., <i>Counter Unmanned Aircraft Systems Technology and Operations</i> , New Prairie Press, 2020
1019	Austin, Reg, <i>Unmanned Aircraft Systems, UAVS Design, Development and Deployment</i> , Wiley, John Wiley and Sons, 2010

I. MANDATORY NOTICES

Real Party in Interest: Axon Enterprise, Inc. and Dedrone Holdings, Inc. (collectively, “Axon” or “Petitioners”) are the real parties in interest.

Related Matters: The ’199 Patent is involved in a pending lawsuit between Petitioners and Airspace Systems, Inc. (“Patent Owner,” or “PO”) entitled *Airspace Systems, Inc. v. Dedrone Holdings, Inc.*, Case No. 1-24-cv-01625 (E.D. VA) (“Airspace Litigation”). The ’199 Patent was first asserted in the Airspace Litigation on September 16, 2024. EX1004.

Lead Counsel and Back-Up Counsel: Petitioners designate lead and back-up counsel as noted below. A Power of Attorney is filed concurrently herewith under 37 C.F.R. §42.10(b).

Lead Counsel	Backup Counsel
Chad C. Walters, Reg. No. 48,022 Baker Botts L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6511 chad.walters@bakerbotts.com	Harrison Rich, Reg. No. 65,132 Baker Botts L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6561 harrison.rich@bakerbotts.com Joseph Andrew Grado, Reg. No. 80,316 Baker Botts L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6522 andrew.grado@bakerbotts.com Ellyar Barazesh, Reg. No. 74,096 Baker Botts L.L.P. 401 S. 1 st St., Suite 1300

	Austin, TX 78704-1296 Phone: (512) 322-2507 ellyar.barazesh@bakerbotts.com
--	--

Service Information: Correspondence to lead and back-up counsel can be provided at the postal and electronic addresses above. Petitioners also consent to service by electronic mail at DLAxonDedroneIPRs@bakerbotts.com, chad.walters@bakerbotts.com, harrison.rich@bakerbotts.com, andrew.grado@bakerbotts.com, and ellyar.barazesh@bakerbotts.com.

II. STANDING AND FEES

Standing: Petitioners certify under 37 C.F.R. §42.104(a) that the '199 Patent is eligible for *inter partes* review and that Petitioners are not barred or estopped from requesting *inter partes* review on the grounds set forth herein.

Fees: The Office is authorized to charge the fee set forth in 37 C.F.R. §42.15(a) to Deposit Account No. 02-0384 as well as any additional fees that might be due in connection with this Petition.

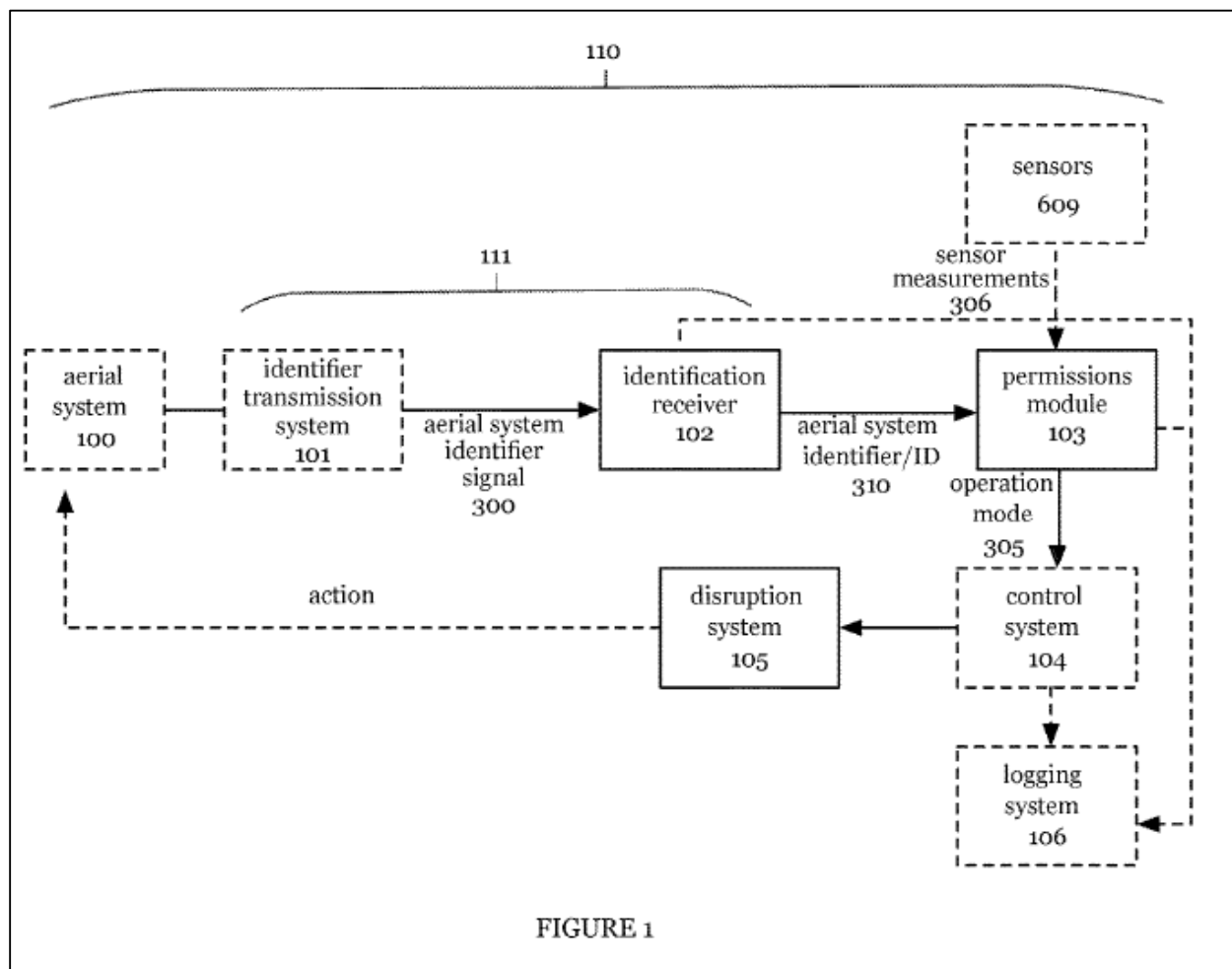
III. OVERVIEW OF THE '199 PATENT

A. *Subject Matter of the '199 Patent*

The '199 Patent generally relates to an “aerial system discrimination system” that “functions to determine whether an aerial system is authorized or unauthorized to be in the airspace.” EX1001, Abstract. The discrimination system comprises several components, including an “aerial system disruption system 105, an aerial

system identification system 111, and a permissions module 103.” *Id.*, 1:60-63.

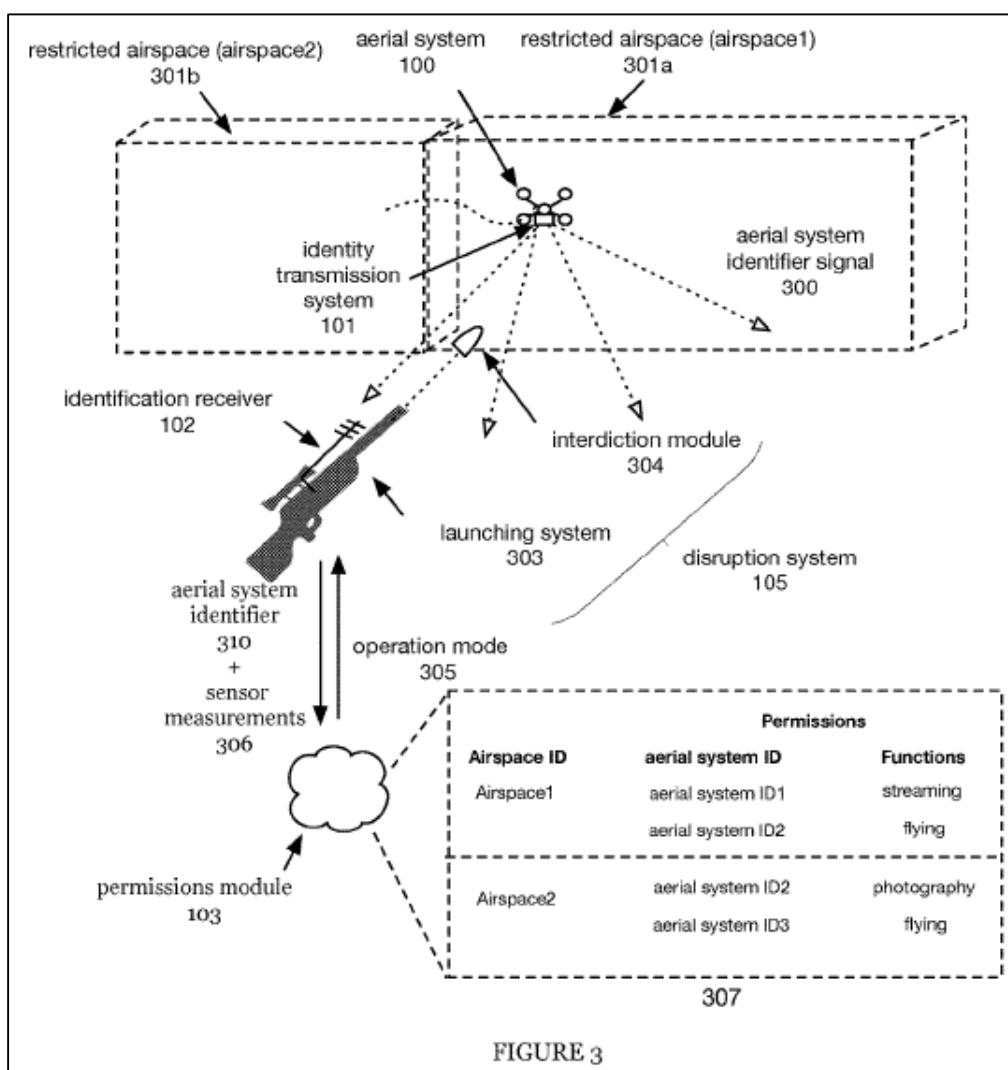
Figure 1 of the '199 Patent, copied below, depicts discrimination system 110:



EX1001, Fig. 1.

In operation, the identification system “receives an aerial system identifier 300 broadcast from a [sic] aerial system 100. The aerial system identifier 300 is checked against the permissions module 103, which determines whether the aerial system identifier 300 is associated with an authorized or unauthorized UAV.” *Id.*, 2:10-15. When the detected UAV is unauthorized, the disruption system can be

“automatically activated (e.g., unlocked),” which means that a “launcher 303 can launch the interdiction module 304 toward the UAV, wherein the interdiction module 304 can immobilize the motive mechanism of the aerial system 100 (e.g., by disabling the power system, entangling the motive mechanism, etc.).” *Id.*, 2:15-26. Figure 3 of the '199 Patent, copied below, depicts such implementation of the interdiction module:



Id., Fig. 3.

B. Prosecution History and Priority Date of the '199 Patent

The application leading to the '199 Patent was filed on May 17, 2017, as U.S. Application 15/598,303 (the "'303 Application"). EX1001, items (21), (22). The '199 Patent claims priority to provisional application No. 62/309,838 (the "'838 Provisional"), which was filed on March 17, 2016. *Id.*, item (60). Because the '303 Application was filed more than 12 months after the '838 Provisional's filing date, applicant filed a petition to restore priority to the '838 Provisional on March 23, 2018. EX1002, 157-158. This petition was granted on April 5, 2018. *Id.*, 146-149. For the purposes of this petition, Petitioners assume without conceding that the priority date of the '199 Patent is March 17, 2016.

The Patent Office issued a first Non-Final Office Action on September 17, 2019, rejecting Claims 1-11 as anticipated by various combinations of U.S. Patent No. 9,792,613 ("*Gong*"), U.S. Patent No. 9,835,709 ("*Tran*"), U.S. Patent No. 9,689,976 ("*Parker*"), and U.S. Patent Publication No. 2017/0059692 ("*Laufer*"). EX1002, 120-126. Further, Claims 1-11 were rejected as being indefinite based on Claim 1's recitation of the limitation "the identification receiver system," and Claims 1-11 were objected to for various informalities. EX1002, 119-120.

In response, applicant made various amendments, including adding the limitation "*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,” to independent Claim 1. EX1002, 106-109. Applicant acknowledged that *Gong* “separately discloses UAV identifiers and a countermeasure system,” but argued that “Gong does not appear to disclose that the countermeasure system is preemptively enabled based on the UAV identifiers.” *Id.*, 111-112. Applicant further amended Claim 1 to address the written description rejection and informalities objections. *Id.*, 111.

On January 2, 2019, the Patent Office issued a notice of allowance. *Id.*, 88-92.

IV. SUMMARY OF PRIOR ART

A. *Whitmarsh (EX1005)*

Whitmarsh is U.S. Patent Application Publication 2019/0003807A1 which was filed on December 8, 2016, as PCT App. No. PCT/US16/65606, and which published on January 3, 2019. EX1005. *Whitmarsh* claims priority to U.S. Provisional Application No. 62/267,393 (EX1006, “*Whitmarsh Provisional*”) filed on December 15, 2015. *Whitmarsh* properly claimed benefit to (EX1008, item (60)), was filed copending with (*id.*, item (22)), and shared a common inventor with (*id.*, item (72)) *Whitmarsh Provisional*. See AIA 35 U.S.C. §102(d); MPEP §2154.01(b). Also, the subject matter relied upon in *Whitmarsh* is described in *Whitmarsh Provisional*. See MPEP §2154.01(b).

Dynamic Drinkware does not apply. See *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1379-80 (Fed. Cir. 2015). The Board has determined that, “for prior-art determinations under AIA §102, ‘there is no need to evaluate whether any claim of [a reference] patent document is *actually entitled to priority* or benefit under 35 U.S.C. 119, 120.’” See, e.g., *Penumbra, Inc. v. RapidPulse, Inc.*, IPR2021-01466, Paper 34 (P.T.A.B. March 20, 2023) (precedential), at 32 (emphasis original; citing MPEP §2154.01(b); holding that the requirement in *Dynamic Drinkware* (that under pre-AIA 35 U.S.C. §102(e), a reference patent’s claims must have written description support in its provisional application in order to be entitled to the filing date of the provisional application) does not apply to AIA 35 U.S.C. §102(d)); see also *Apple Inc. v. Telefonaktiebolaget LM Ericsson*, IPR2022-00341, Paper 10 (P.T.A.B. Sept. 14, 2022), at 19.

Thus, for prior art purposes, *Whitmarsh* was effectively filed on December 15, 2015. Accordingly, *Whitmarsh* qualifies as prior art under AIA §102(a)(2). Like the ’199 Patent, *Whitmarsh* describes a “UAV [unmanned aerial vehicle] defense system” 10 that determines whether a UAV is authorized to be in a certain area. EX1005, [0002], [0013], [0028], [0033], [0050]; EX1006, [0001], [0009] (“The primary function of the RTSS [remote transmission security system] is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected.”), [0010], [0013]. If the UAV is not authorized, *Whitmarsh*

develops and deploys a “countermeasures system” to disable the UAV or otherwise remove it from a given area. EX1005, [0017]-[0018]; EX1006, [0011], [0018]. Thus, *Whitmarsh* is from the same field of art as the ’199 Patent and describes a defense system similar to the system described in the ’199 Patent. EX1003, ¶107.

B. *Viggiano (EX1007)*

Viggiano is U.S. Patent Application Publication 2007/0239986A1 which was filed on April 7, 2006, and which published on October 11, 2007. *Viggiano* is thus prior art to the ’199 Patent at least under 35 U.S.C. §§102(a)(1) and 102(a)(2).

Viggiano describes “authentication apparatus” that “employs an authentication challenge-response methodology and encryption techniques to authenticate the identity of an ADS-B [Automatic Dependent Surveillance-Broadcast] equipped aircraft.” EX1007, [0012]. Thus, *Viggiano* is from the same field of art as the ’199 Patent and describes an aircraft authentication system that is similar to the system described in the ’199 Patent. EX1003, ¶109.

C. *Goodrich (EX1008)*

Goodrich is U.S. Patent Application Publication 2016/0023760A1 which was filed on July 16, 2015, and which published on January 28, 2016. *Goodrich* is thus prior art to the ’199 Patent at least under 35 U.S.C. §§102(a)(1) and 102(a)(2).

Goodrich discloses a counter-UAV system that deploys “an interceptor UAV 110 configured to disable or destroy a target UAV 199.” EX1008, [0011], [0014].

When the interceptor UAV is in range of the target UAV, an “engagement decision” is made to direct the interceptor UAV to either “abort” its intercept track and return to its base or engage the target UAV by executing a “terminal maneuver” that disables the target UAV. *Id.*, [0027]-[0031]. Thus, *Goodrich* is from the same field of art as the ’199 Patent and describes an aircraft disruption system that is similar to the system described in the ’199 Patent. EX1003, ¶111.

D. *Falk* (EX1011)

Falk is U.S. Patent No. 9,805,238 which was filed on July 11, 2016, and which issued on October 31, 2017. EX1011. *Falk* claims priority to U.S. Provisional Application No. 62/301,858 (EX1012, “*Falk Provisional*”) filed on March 1, 2016. *Falk* properly claimed benefit to (EX1011, item (60)), was filed copending with (*id.*, item (22)), and shared a common inventor with (*id.*, item (72)) *Falk Provisional*. See AIA 35 U.S.C. §102(d); MPEP §2154.01(b). Also, the subject matter relied upon in *Falk* is described in *Falk Provisional*. See MPEP §2154.01(b).

Thus, for prior art purposes, *Falk* was effectively filed on March 1, 2016. Accordingly, *Falk* qualifies as prior art under AIA §102(a)(2).

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.” EX1011, 3:35-36; EX1012 [0009]. The beacon includes “indicia” that “together form a unique identifier associating the

owner or responsible party with the unmanned aerial vehicle.” EX1011, 3:42-47; EX1012, [0010]. The beacon also includes a “remote communications module” that facilitates wireless communication “to and from a remote operator.” EX1011, 3:56-64; EX1012, [0011]. Thus, *Falk* is from the same field of art as the ’199 Patent and describes an identifier transmission system similar to the system described in the ’199 Patent. EX1003, ¶113.

E. Summary of 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>

EX1003, ¶37; EX1013 (listing challenged claim elements).

V. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (POSITA) would have either (1) a Bachelor of Science in Mechanical Engineering, Electrical Engineering, Aerospace Engineering, Aviation Technologies, Avionics, or an equivalent field, as well as at least 2 years of academic or industry experience in the aerospace, avionics, telecommunications, or electronic device manufacturing industry, or (2) at least four years of industry experience in any of the above industries. EX1003, ¶62.

VI. CLAIM CONSTRUCTION

The challenged claims all recite a “*permission module*.” The Federal Circuit has in some circumstances interpreted the term “module” in computer-related uses to be a nonce term subject to 35 U.S.C. §112(f). *See, e.g., Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015) (“‘Module’ is a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.”). To the extent that this term² needs to be construed under §112(f), and without conceding that the claim limitations satisfy 35 U.S.C. §112, Petitioners identify below this term’s corresponding function and structure.³

Claim 1 recites “*a permission module*” and “*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*.” If §112(f) applies, the term’s function is “determining that the aerial system associated with the aerial system

² Although Claims 6 and 7 include the term “*interdiction module*,” Petitioners do not believe that this term is subject to §112(f), as this is not a computer-related term. A POSITA would instead understand, based on its use in the claim and specification, it to refer to specific structures. *See, e.g.,* EX1001, 11:40-12:52 (identifying a “net” as an example of the “*interdiction module*”); EX1003, ¶66.

³ All structure identified below includes equivalents thereof.

identifier signal is not permitted to be in an airspace.” EX1001, 20:53-56; EX1003, ¶67. The ’199 Patent discloses that the permission module can be: “storage on-board the disruption module 105, storage on-board the identification receiver 102, a remote computing system connected to the disruption module..., or [] any other suitable computing system.” EX1001, 9:64-10:4. When describing the claimed functionality of the permissions module 103 (e.g., determining that the aerial system is not permitted to be in an airspace), the patent states that the aerial system parameter permission can be determined by “comparing the aerial system parameters (e.g., identifier, function, etc.) with the permissions for the airspace.” *Id.*, 18:21-42. Under a §112(f) application, comparing an aerial system parameter, such as an identifier, with the permissions for the airspace would therefore be the algorithm disclosed for performing the claimed function. EX1003, ¶37. *MS Gaming, Inc. v. Int’l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999) (“In a means-plus-function claim in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm”).

Thus, to the extent the claimed permission module is interpreted under §112(f), its function is “determining that the aerial system associated with the aerial system identifier signal is not permitted to be in an airspace;” and its corresponding

structure for performing that function is “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.”

VII. INSTITUTION IS PROPER

A. *The Fintiv Factors Favor Institution under §314(a)*

The factors described in *Apple, Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (P.T.A.B. May 13, 2020) (Precedential) (“*Fintiv-I*”) favor institution. Notably, the merits of this Petition are particularly strong, with compelling art and arguments.

A stay motion has not yet been filed in the Airspace Litigation, but Petitioners intend to file one. The Board has treated related factors as neutral after declining to speculate on the outcome of a stay motion. *See, e.g., HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 at 9 (P.T.A.B. Jan. 14, 2021).

The Airspace Litigation is just beginning. The district court has not set a trial date—or any deadlines—in the Airspace Litigation, which “weighs significantly against” exercising the Board’s discretion to deny institution. *Google LLC v. Uniloc 2017 LLC*, IPR2020-00755, Paper 14 (P.T.A.B. Oct. 15, 2020) (“The fact that no trial date has been set weighs significantly against exercising our discretion to deny institution of the proceeding”) (citing *Oticon Med. AB v. Cochlear Ltd.*, IPR2019-

00975, Paper 15 (P.T.A.B. Oct. 16, 2019) (precedential) (lack of trial date weighs against exercising discretion to deny institution, even when discovery is “well underway”).

Relatedly, the parties’ and the district court’s investment in the Airspace Litigation has been minimal. *Fintiv-I*, Paper 11 at 11. Although the district court denied plaintiff’s Rule 12(b)(6) motion to dismiss on February 10, 2025, no part of claim construction has occurred, no claim-by-claim infringement contentions have been provided, and the related district court litigation does not yet have scheduling order.

“[I]t is often reasonable for a petitioner to wait to file its petition until it learns which claims are being asserted against it in the parallel proceeding.” *Fintiv-I* at 11. Here, Petitioners promptly filed this Petition against Claims 1-9 of the ’199 Patent before receiving infringement contentions. The “diligent” filing favors institution. *See, e.g., Corning v. Dali Wireless*, IPR2021-00762, Paper 8 at 9-10 (P.T.A.B. October 31, 2021) (crediting petitioner’s diligent filing of the petition approximately four months after receiving infringement contentions). Due to Petitioners’ diligence, it would be premature at the time of this Petition to argue regarding the timing of respective milestones in this proceeding versus the Airspace Litigation. If PO raises 314(a) arguments in a Preliminary Response, Petitioners respectfully request the

opportunity to reply prior to institution to address expected schedules and whether a prior art stipulation would be appropriate.

B. *Institution is Proper under §325(d)*

Although *Viggiano* is cited on the face of the '199 Patent, it was not used in a rejection of the claims, as the only Office Action issued against the '199 Patent relied on other references in its prior art rejections. EX1002, 120-126; Ex. 1003, ¶¶58-61. The Board has declined to exercise its discretion to deny institution in situations where the petitioner relied upon prior art that was cited on the face of the challenged patent but was “not applied by the examiner ... in any rejection of claims.” *Comcast Cable Communs., LLC v. Promptu Sys. Corp.*, Case No. IPR2018-00342, Paper 13 at 17 (P.T.A.B. July 19, 2018).

VIII. THE CHALLENGED CLAIM IS UNPATENTABLE

A. *Ground 1: Whitmarsh Renders Obvious Claims 1-3 and 5-9*

1. Claim 1

a) 1[p]: A discrimination system comprising:

To the extent the preamble is limiting, *Whitmarsh* discloses the preamble. *Whitmarsh* describes a “UAV defense system” 10 that determines whether a UAV is authorized to be in a certain area. EX1005, [0002], [0013], [0028], [0033], [0050]; EX1006, [0001], [0009] (“The primary function of the RTSS [remote transmission security system] is to identified [sic] and detect unauthorized or hostile drones in and around the area or region that is to be protected.”), [0010], [0013] (“The DDS [drone

defense system] will be able to determine between friendly and hostile drones.”); EX1003, ¶114.

Accordingly, *Whitmarsh’s* system “*discriminates*” between authorized/friendly and unauthorized/hostile drones to provide security to a protected area, and therefore discloses Limitation 1[p].

b) 1[a]: 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;

Whitmarsh describes that its UAV defense system receives from nearby UAVs wireless communications that include information or signatures unique to the UAVs, such as a MAC address of the UAV, that is used to identify the transmitting UAV. *See* EX1005, [0020] (disclosing that UAVs include one or more wireless communications systems for periodically broadcasting a MAC address of the UAVs), [0027] (explaining that a UAV’s MAC address is “unique to each UAV 14” and allows the UAV defense system to “specifically identify the detected UAV 14”); EX1006, [0008], [0010], [0013] (“All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS [drone defense system] and can be used to identify the drone.”), [0015], [0016] (“The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. . . . All drones with definable MAC addresses are tagged by the DDS.”), [0017]; EX1003, ¶117.

A POSITA would have understood that because *Whitmarsh's* drone defense system receives wireless communications/signals from a UAV/UAS that indicate a MAC address of the UAV/UAS (which identifies the UAV/UAS), the UAVs disclosed by *Whitmarsh* include one or more components for transmitting such communications/signals. *Id.* Accordingly, a POSITA would have understood that *Whitmarsh's* UAVs are “*aerial systems*” that are “*coupled to*” an “*identifier transmission system*” that broadcasts a MAC address (“*identifier*”) of the UAV. *Id.*

In the alternative, it would have been obvious to a POSITA that *Whitmarsh's* UAVs would be coupled to “*an identifier transmission system*” in view of *Whitmarsh's* disclosure of receiving, from the UAVs, wireless communications/signals containing a MAC address of UAVs. EX1003, ¶118. A POSITA would have understood that such wireless communications would have involved the use of well-known, dedicated components, such as an antenna element and a signal processor. *Id.* Thus, a POSITA would have considered it obvious that a UAV would include (be “*coupled to*”) a transmission system in order to perform any wireless communication. *Id.*

Finally, the wireless communications/signals comprising MAC address information discloses “*an aerial system identifier signal unique to the aerial system,*” because these signals include a MAC address of the UAV, which *Whitmarsh* describes as unique information that is used to identify the associated

UAV. *See* EX1005, [0027] (“For example, by capturing the MAC address, which is unique to each UAV 14, the UAV defense system 10 will be able to specifically identify the detected UAV 14.”); EX1006, [0013] (“All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS and can be used to identify the drone.”).

Accordingly, *Whitmarsh’s* disclosure of transmitting the MAC address in wireless communications/signals to the UAV defense system discloses, or at least renders obvious, Limitation 1[a].

c) 1[b]: an identification receiver;

As discussed above with reference to Limitation 1[a], *Whitmarsh* describes that its UAV defense system receives from nearby UAVs wireless communications that include information or signatures unique to the UAVs, such as a MAC address of the UAV, that is used to identify the broadcasting UAV. *Supra*, VIII.A.1.(b); EX1005, [0020], [0027]; EX1006, [0008], [0010], [0013], [0015]-[0017]. Accordingly, a POSITA would have understood that *Whitmarsh’s* UAV defense system comprises “*an identification receiver*” that acts as the component for actually receiving these wireless communications and the identification information (*e.g.*, the MAC address) contained therein. EX1003, ¶121.

In the alternative, it would have been obvious to a POSITA that *Whitmarsh’s* UAV defense system includes an “*identification receiver*” in view of *Whitmarsh’s*

disclosure of receiving wireless communications/signals containing a MAC address that identifies the broadcasting UAV. EX1003, ¶122. A POSITA would have understood that receiving wireless communication signals would have involved using well-known, dedicated components, such as an antenna element and a signal processor. *Id.* Thus, it would have been obvious to a POSITA that *Whitmarsh's* UAV defense system comprises “an *identification receiver*” that acts as the component for actually receiving these wireless communications and the identification information (e.g., the MAC address) contained therein. *Id.* (citing EX1015, [0046]).

d) 1[c]: a permission module,

Whitmarsh discloses, or at least renders obvious, “a *permission module*,” as addressed in Limitation 1[e]. *See infra*, VIII.A.1.(f).

e) 1[d]: 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,

As discussed above with reference to Limitation 1[b] and below with reference to Limitation 1[e], *Whitmarsh* discloses, or at least renders obvious, a UAV defense system that comprises (1) an “*identification receiver*” that receives wireless communications that include a unique MAC address that identifies a transmitting UAV (“*wherein the identification receiver is configured to receive the aerial system identifier signal*”) and (2) a “*permission module*” that determines to

deploy a particular countermeasure based at least in part on the detected UAV's identity. *Supra*, VIII.A.1.(c); *infra*, VIII.A.1.(f). And as discussed above with reference to Limitation 1[a], the UAV's identity is determined based on the MAC address contained in the received wireless communication. *Supra*, VIII.A.1.(b). Accordingly, 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 aerial system identifier signal*") to the "*permission module*." EX1003, ¶124.

In the alternative, it would have been obvious to a POSITA that the UAV defense system's "*identification receiver*," which receives wireless communications that include a unique MAC address, would provide such communications to the "*permission module*," which determines to deploy a particular countermeasure based at least in part on the detected UAV's identity, because the MAC address contained in the received wireless communication indicates a transmitting UAV's identity. EX1003, ¶125; EX1005, [0027]; EX1006, [0013]. Accordingly, it would have been obvious to a POSITA that for the permission module to determine the UAV identity based on the MAC address, the "*identification receiver*" would have first provided the wireless communication comprising the MAC address ("*the aerial system identifier signal*") to the "*permission module*." EX1003, ¶125.

f) 1[e]: 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

Whitmarsh discloses, or at least renders obvious, this limitation, regardless of whether the “*permission module*” term is subject to §112(f). EX1003, ¶126.

(a) Function:

Whitmarsh discloses, or at least renders obvious, the claimed function “determin[ing] that the aerial system associated with 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.” EX1005, [0017]; EX1006, [0013], [0016], [0017] (“DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. . . . Only drones registered on the local registry as ‘friendly’ or ‘authorized’ will allowed to travel from x miles marks to point zero.”), [0018].

Upon receiving a UAV identity, the UAV defense system may “interface with a UAV registry database 36” to allow the UAV defense system to “correlate the unique MAC addresses of the UAV systems with information relating to the identity of the persons or entities that acquired the UAV 14,” as well as “update such a UAV

database 36 with information and data relating to prior detection and countermeasures activities, thereby allowing troublesome or suspect UAVs 14 to be identified so that appropriate action can be taken.” EX1005, [0029]; EX1006, [0010] (“Each tracking signature may be processed in conjunction with one or more information databases, including, for example a local database or a national database . . . to record the signature of each non-recognized signature and each event. . . . If the tracking signature matches a rule in the logic system that the unauthorized or hostile drone's identification signatures are a threat, the RTSS ‘tags’ the drone as unauthorized or even as hostile.”).

A determined countermeasure may be a “disable countermeasure” that is “used to actually disable the detected UAV.” EX1005, [0018], [0028] (“However, more robust countermeasures may be employed in other circumstances and may ultimately involve the immediate interception of the unauthorized UAV 14.”); EX1006, [0009]-[0010], [0011] (describing an “intercept” countermeasure wherein “armed drone systems” are configured to “intercept (e.g., shoot down) the unauthorized or hostile drone”), [0017]-[0018].

Accordingly, a POSITA would have understood, or at least considered it obvious, that *Whitmarsh*’s UAV defense system discloses the claimed determining functionality based on its description of determining to deploy a disabling countermeasure based at least in part on the detected identity of the unauthorized

UAV. EX1003, ¶130. That is, a POSITA would have understood, or at least considered it obvious, that by determining to deploy a disabling countermeasure based at least in part on the detected identity of the unauthorized UAV, the UAV defense system would have determined that the UAV does not have permission to be in a given area. *Id.*

(b) Structure:

Whitmarsh discloses, or at least renders obvious, the claimed “*permission module*” regardless of whether that term is subject to §112(f). As discussed above, *Whitmarsh*’s UAV defense system discloses, or at least renders obvious, the claimed determining functionality. *Supra*, VIII.A.1.(f).(a). POSITA would have understood, or considered it obvious, that *Whitmarsh*’s UAV defense system would comprise a “*permission module*” to perform its disclosed functionality of determining to deploy a particular countermeasure based at least in part on the detected UAV’s identity. EX1003, ¶131. A POSITA would have understood that this functionality—generally, computing a decision based on inputted information—is routinely performed by well-known computing and/or processing components of electronics systems, so that it would have been obvious to a POSITA that such functionality would be performed by a computer system, processor, or similar component of the UAV defense system that is configured to determine an outcome based on inputted data. *Id.* Such an understanding is consistent with the ’199 Patent’s disclosure that

its permission module could be “storage on-board the disruption module 105, storage on-board the identification receiver 102, a remote computing system connected to the disruption module..., or [] any other suitable computing system.” EX1001, 9:64-10:4; EX1003, ¶131.

And if “*permission module*” is subject to §112(f), *Whitmarsh* discloses, or at least renders obvious, the corresponding 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.” *See supra*, VI. As discussed above, *Whitmarsh* determines that the aerial system associated with the aerial system identifier signal is not permitted to be in an airspace by “interfac[ing] with a UAV registry database 36” to allow the UAV defense system to “correlate the unique MAC addresses of the UAV systems with information relating to the identity of the persons or entities that acquired the UAV 14,” such as “information and data relating to prior detection and countermeasures activities, thereby allowing troublesome or suspect UAVs 14 to be identified so that appropriate action can be taken.” *Supra*, VIII.A.1.(f).(a); EX1005, [0029]; EX1006, [0010]. A POSITA would have understood, or at least considered it obvious, that this correlation would involve “compar[ing]” the “unique MAC addresses of the UAVs” (*i.e.*, “aerial system parameter, such as an identifier”)

with “information and data relating to prior detection and countermeasures activities” (*i.e.*, “the permissions for the airspace”) to allow the system to identify “troublesome or suspect UAVs.” EX1003, ¶132. And it would be a computer system or processor of *Whitmarsh* programmed to perform this “comparing” step. *Id.* Accordingly, *Whitmarsh* discloses, or at least renders obvious, the corresponding structure for performing the claimed function.

g) 1[f]: 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.

Whitmarsh describes a countermeasures system that “develops one or more countermeasures based on the identity and/or position of the detected UAV 14,” where the identity of the detected UAV is determined based on a MAC address included in a wireless communication received by the UAV defense system. EX1005, [0017], [0027]; EX1006, [0010] (describing starting a series of processes “to determine what rule of engagement will be applied on the intruding drone” upon detecting a an unauthorized or hostile drone identification signature), [0016]-[0018] (describing activating “the countermeasures system” based on a received MAC address identifier of a UAV); *supra*, VIII.A.1.(b), VIII.A.1.(e) (describing the UAV defense system determining the detected UAV’s identity based on the received MAC address).

The determined countermeasure may be, for example, an “intercept countermeasure” wherein “the UAV defense system 10 may dispatch one or more security vehicles 44 and operate it so that it actually collides with the detected UAV 14.” EX1005, [0017]-[0018], [0028]; EX1006, [0010]-[0011] (describing that the intercept countermeasure may be used in response to determining that a detected UAV is unauthorized or hostile). Accordingly, *Whitmarsh*’s countermeasures system discloses “*a disruption system configured to disrupt an operation of the aerial system.*”

Further, *Whitmarsh* describes determining these countermeasures when a UAV is identified as many as five miles from a protected asset. EX1005, [0031] (“UAVs 14 located in the intermediate detection zone 26 may be more carefully scrutinized and limited countermeasures applied.”), [0036] (explaining that the “intermediate detection zone” may extend between the 5-mile and 1-mile radiuses from “the primary defense point 28 that is to be protected”); EX1006, [0017] (“Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as ‘friendly’ or ‘authorized’ will allowed to travel from x miles marks to point zero.”), [0018].

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,*” *see supra,*

VIII.A.1.(b), VIII.A.1.(e)) 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. EX1003, ¶136. Thus, *Whitmarsh* discloses “*preemptively enabl[ing]*” its countermeasures system. *Id.*

This preemptive enabling of *Whitmarsh's* countermeasure system based on the MAC address of an unauthorized UAV is consistent with the '199 Patent, which explains that the “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.).” EX1001, 19:16-20 (emphasis added).

Accordingly, *Whitmarsh* discloses Limitation 1[f].

2. Claim 2

a) 2: The system of claim 1, 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.

As discussed above with reference to Limitation 1[a], *Whitmarsh* discloses a drone defense system that monitors wireless communications for signals transmitted by UAVs that include information that identifies the UAVs. *Supra*, VIII.A.1.(b);

EX1005, [0020], [0027]; EX1006, [0008], [0013], [0015]-[0017]. *Whitmarsh* further describes that these signals may be transmitted according to the WiFi protocol. EX1005, [0039]-[0041] (“Supported medium range protocols include ZigBee, 802.15.4, DigiMesh, and WiFi.”); EX1006, [0015] (describing that the drone defense system “scans and surveys WIFI, RF, and sensor signals” to identify drones in an area).

Accordingly, a POSITA would have understood that *Whitmarsh*’s “*identifier transmission system*” (which transmits signals from a UAV to the UAV defense system, *see supra*, VIII.A.1.(b)) and “*identification receiver*” (which receives signals from the UAV, *see supra*, VIII.A.1.(c)) use a “radio chipset that is compatible with” the WiFi communication protocol in view of *Whitmarsh*’s disclosure of these components communicating via WiFi signals. EX1003, ¶140.

In the alternative, it would have been obvious to a POSITA that *Whitmarsh*’s “*identifier transmission system*” and “*identification receiver*” use a “*radio chipset that is compatible with*” the WiFi communication protocol in view of *Whitmarsh*’s disclosure of these components communicating via WiFi signals. *Id.*, ¶141.

3. Claim 3

a) 3: The system of claim 1, 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.” EX1005, [0066]; EX1006, [0004]. A POSITA would have understood that in such implementations, *Whitmarsh*’s “*identification receiver*” (*see supra*, VIII.A.1.(c)), which is a component of the UAV defense system, would be a “*mobile device*,” because it is located on a mobile vehicle such as an aircraft or a ship. EX1003, ¶142.

4. Claim 5

- a) 5: The system of claim 1, wherein when the disruption system is enabled the aerial system is caused to be removed from the airspace.

As discussed above with reference to Limitation 1[f], *Whitmarsh* discloses developing and deploying various countermeasures against a detected UAV, including an “intercept countermeasure” wherein the countermeasures system (“*the disruption system*”) “may dispatch one or more security vehicles 44 and operate it so that it actually collides with the detected UAV 14.” *Supra*, VIII.A.1.(g). 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 to the detected UAV such that it would have been “*removed from the airspace*” (*e.g.*, due to falling to the ground). EX1003, ¶143. Accordingly, *Whitmarsh* discloses Claim 5 when it executes the intercept countermeasure.

5. Claim 6

- a) 6: The system of claim 1, wherein the disruption system comprises of a projectile launcher and an interdiction module.

Whitmarsh Provisional (EX1006), which is 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.” EX1006, [0011]; EX1005, [0001] (incorporating by reference *Whitmarsh Provisional* and another provisional application “for all that they disclose”); *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (“To incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.”); *Biscotti Inc. v. Microsoft Corp.*, 2017 WL 2526231, at *2 (E.D. Tex. May 11, 2017) (denying motion to prevent defendant’s expert from relying on material from provisional applications that were incorporated by reference in asserted prior art reference). A POSITA would have understood that when implementing the intercept countermeasure, *Whitmarsh*’s UAV defense system (“*the disruption system*”) comprises armed drone systems that include a “*projectile launcher*” and projectiles (“*interdiction module[s]*”) that are used to “shoot down” the detected UAV.

In the alternative, it would have been obvious to a POSITA that in order for *Whitmarsh*’s “armed drone systems” to “shoot down” a detected UAV, these drones would need to be equipped with projectiles (e.g., bullets) as well as a “*projectile*

launcher” for shooting the projectiles. EX1003, ¶145. Accordingly, it would have been obvious that when implementing the intercept countermeasure, *Whitmarsh*’s UAV defense system (“*the disruption system*”) comprises armed drone systems that include a “*projectile launcher*” and projectiles (“*interdiction module[s]*”) that are used to “shoot down” the detected UAV.

This understanding of *Whitmarsh*’s projectiles used to “shoot down” a detected UAV as “*interdiction module[s]*” 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.” See EX1001, 11:58-60; see also *id.*, 11:61-63. Accordingly, *Whitmarsh* discloses Claim 6.

6. Claim 7

a) 7: The system of claim 1, wherein the disruption system comprises of an interceptor drone coupled with an interdiction module.

As discussed above with reference to Claim 6, *Whitmarsh*’s countermeasures system (“*the disruption system*”) comprises an armed drone system that shoots down a detected UAV. See *supra*, VIII.A.5; EX1006, [0011]; EX1005, [0001]. And as discussed with reference to Claim 6, 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. *See supra*, VIII.A.5. Accordingly, *Whitmarsh* discloses, or at least renders obvious, Claim 7 for the same reasons.

7. Claim 8

- a) 8: The system of claim 1, further comprising a control system for controlling the disruption system.

Whitmarsh's countermeasures system (“*disruption 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.” EX1005, [0017]; EX1006, [0011]. A POSITA would have understood that to control a detected UAV in such a manner, the UAV defense system would also implement a “*control system*” that would provide instructions to the detected UAV through the countermeasure system, effectively controlling both the countermeasures system and the detected UAV. EX1003, ¶148.

In the alternative, it would have been obvious to a POSITA that *Whitmarsh's* UAV defense system would comprise a “control system” that would provide instructions to the countermeasures system (“*control the disruption system*”) for controlling the commandeered UAV. EX1003, ¶149. As discussed above with reference to Limitation 1[f], *Whitmarsh's* countermeasures system (“*the disruption system*”) is configured to develop a countermeasure to enforce against a detected UAV. *Supra*, VIII.A.1.(g). It would have been obvious to a POSITA to implement additional components, such as a “*control system*,” to control the countermeasures

system when it is implementing the commandeering countermeasure, as this measure involves additional functionality of providing to the commandeered UAV instructions, which a POSITA would have recognized is better handled by a distinct component of the UAV defense system (e.g., a separate computing system or processor).

Accordingly, *Whitmarsh* discloses, or at least renders obvious, Claim 8.

8. Claim 9

- a) 9: The system of claim 8, 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), which is incorporated by reference in *Whitmarsh*, discloses recording “the signature of each non-recognized signature” received from a detected UAV. *See* EX1006, [0010]; EX1005, [0001]; *Advanced Display Sys.*, 212 F.3d at 1282; *Biscotti Inc.*, 2017 WL 2526231, at *2. And as discussed above with reference to Limitation 1[b], *Whitmarsh* discloses, or at least renders obvious, an “*identification receiver*” that receives wireless communications that include a MAC address, where the MAC address operates as an identifier, or signature, of the associated UAV. *See supra*, VIII.A.1.(c). Accordingly, 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*” (i.e., the “*activity of . . . the identification receiver*”). EX1003, ¶151.

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.” EX1005, [0046]; EX1006, [0010] (describing the recording of non-recognized signatures received from a detected UAV). A POSITA would have understood that in this role, the local database 32 operates as a “*logging system*” that is configured to record activity of the UAV defense system and its components (e.g., “*the identification receiver*,” “*the permission module*,” and “*the control system*”) and therefore discloses Claim 9. EX1003, ¶152.

In the alternative, it would have been obvious to a POSITA that *Whitmarsh*’s UAV defense system would comprise a “*logging system*,” such as a memory component, for recording the activity of the “*identification receiver*” (i.e., the reception of any non-recognized signatures, such as MAC addresses), because recording information is a distinct function that is handled by memory components of a system. EX1003, ¶153. Thus, *Whitmarsh* discloses, or at least renders obvious, Claim 9.

This understanding is consistent with the ’199 Patent, which explains that the “*logging system*” “functions to store and/or provide histories for aerial system

identifiers 310,” wherein said histories may be generated “in response to aerial system identification within the airspace (e.g., wherein the logging system can be coupled to the identification receiver).” EX1001, 13:34-52.

B. Ground 2: The Combination of Whitmarsh and Falk Renders Obvious Claim 4

1. Motivation to Combine

a) Whitmarsh with Falk

Whitmarsh discloses a UAV defense system that receives wireless communications from nearby UAVs that include information or signatures unique to the UAVs, such as a MAC address of the UAV, that is used to identify the transmitting UAV. *See* EX1005, [0020], [0027]; EX1006, [0008], [0010], [0013], [0015]-[0017]. *Falk* discloses a “beacon” that is removably attachable to a UAV and is configured to transmit “indicia” (*i.e.*, information identifying a particular unmanned aerial vehicle) via wireless communications resources. EX1011, 3:42-64, 7:65-8:12; EX1012, [0009]-[0011], [0024].

A POSITA would have been motivated for several reasons to implement *Falk*’s “beacon” as the mechanism used by UAVs to transmit their identification information (*e.g.*, MAC addresses) to *Whitmarsh*’s UAV defense system.

First, design incentives and market forces would have motivated a POSITA to implement *Falk*’s beacon alongside *Whitmarsh*’s UAV defense system. A POSITA implementing *Whitmarsh*’s UAV defense system would have understood

that its underlying authentication mechanism relies on receiving an identifier from a UAV via wireless communication resources. EX1003, ¶159. Accordingly, a POSITA would have recognized that to improve the viability and effectiveness of the UAV defense system, they would need to outfit UAVs that are not manufactured with the ability to communicate their identifiers (or other identification information) over wireless resources with some mechanism for performing such communications, such as *Falk*'s beacon. *Id.* As explained in *Falk*, this is particularly relevant because UAVs utilize different communication protocols, which inherently limits their ability to communicate with systems that rely on different communication protocols. EX1011, [0007]; EX1012, [0006]. Accordingly, 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. EX1011, [0034]; EX1012, [0027]-[0028]; EX1003, ¶159. Indeed, one of *Falk*'s design goals is to provide a more accessible solution for UAVs to identify themselves in an effort to improve UAV regulation and security. EX1011, [0003]-[0009]; EX1012, [0002]-[0008].

A POSITA would have also recognized that UAV owners often own multiple UAVs, such that *Falk*'s beacon, which can be removed and attached to multiple UAVs, would have been an attractive mechanism for UAV identification for a considerable customer base. EX1003, ¶160.

Second, 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. EX1003, ¶161; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). The results of the combination would be predictable: UAVs that are configured with attachable (and removable) beacons for transmitting UAV identity information. EX1003, ¶161. Indeed, this functionality is entirely consistent with *Falk*'s beacon operation, which is further configured for Wi-Fi-based wireless communication as is done in *Whitmarsh*. EX1011, [0029], [0034] (describing beacon's wireless communication via Wi-Fi networks); EX1012, [0024], [0028] (describing beacon's wireless communication via Wi-Fi networks); EX1003, ¶161.

Accordingly, a POSITA would have been motivated to combine *Whitmarsh* with *Falk* and would have reasonably expected success in doing so.

2. Claim 4

a) 4: The system of claim 1, 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.” EX1011, 3:35-36; EX1012 [0009]. The

beacon includes “indicia” that identifies an owner or responsible party of the UAV and as well as the UAV itself. EX1011, 3:42-47; EX1012, [0010]. The beacon also includes a “remote communications module” that facilitates wireless communication “to and from a remote operator.” EX1011, 3:56-64; EX1012, [0011]. The “indicia” (*e.g.*, the information identifying a particular unmanned aerial vehicle) may be encoded into transmissions to a remote operator along with other data collected by a “sensory package,” which a POSITA would have understood to occur via wireless communications. EX1011, 7:65-8:11; EX1012, [0024]; EX1003, ¶163.

Further, *Falk* explains that “once information is encoded in the indicia 120, including first or second indicia 121, 122, the information cannot be easily changed without detectible modifications to the beacon 100. This type of indicia is particularly useful when it is desirable to associate certain information with the particular owner or the UAV 10 that was used to collect the information.” EX1011, 6:63-7:2; EX1012, [0022].

In the *Whitmarsh-Falk* combination, a POSITA would have understood that *Falk*’s beacon would be incorporated into *Whitmarsh*’s UAV defense system to act as the “*identifier transmission system*” that wirelessly transmits a MAC address of an associated UAV, consistent with *Falk*’s description of the beacon as a component

that is configured to transmit information identifying a UAV to a remote operator via wireless communications.

Under this combination, a POSITA would have understood that the beacon (“*the identifier transmission system*”) is “*configured to be reassigned from a first aerial system to a second aerial system.*” First, the beacon is configured to “securely and removably attach” to a UAV, which a POSITA would have understood to mean it can attach (and reattach) to multiple different UAVs. EX1011, 3:38-41; EX1012 [0009]; EX1003, ¶166. Accordingly, a POSITA would have understood that the beacon is able to be physically reassigned from one UAV (“*aerial system*”) to another. EX1003, ¶166.

Second, it would have been obvious to a POSITA that the beacon would be reassigned electronically from one UAV to another. Although *Falk* explains that information associated with indicia of the beacon (*e.g.*, the UAV identity information) is not “easily” changeable, a POSITA would have understood that nothing in *Falk* suggests that the information associated with the indicia cannot be changed or reconfigured. *Id.*, ¶167. Indeed, *Falk*’s explanation that it is not desirable to change a beacon’s indicia when one wants to “associate certain information with the *particular* owner or the *UAV that was used to collect the information,*” suggests to a POSITA that changing the indicia (*e.g.*, UAV identity

information) **would be** warranted when *Falk*'s beacon is removed from a first UAV and attached to a second UAV. *Id.*

Accordingly, it would have been obvious that under the *Whitmarsh-Falk* combination, the “*identifier transmission system*” (implemented as *Falk*'s beacon) would “*configured to be reassigned from a first aerial system to a second aerial system.*” *Id.*

C. Ground 3: The Combination of *Whitmarsh* and *Goodrich* Renders Obvious Claims 1-3 and 5-9

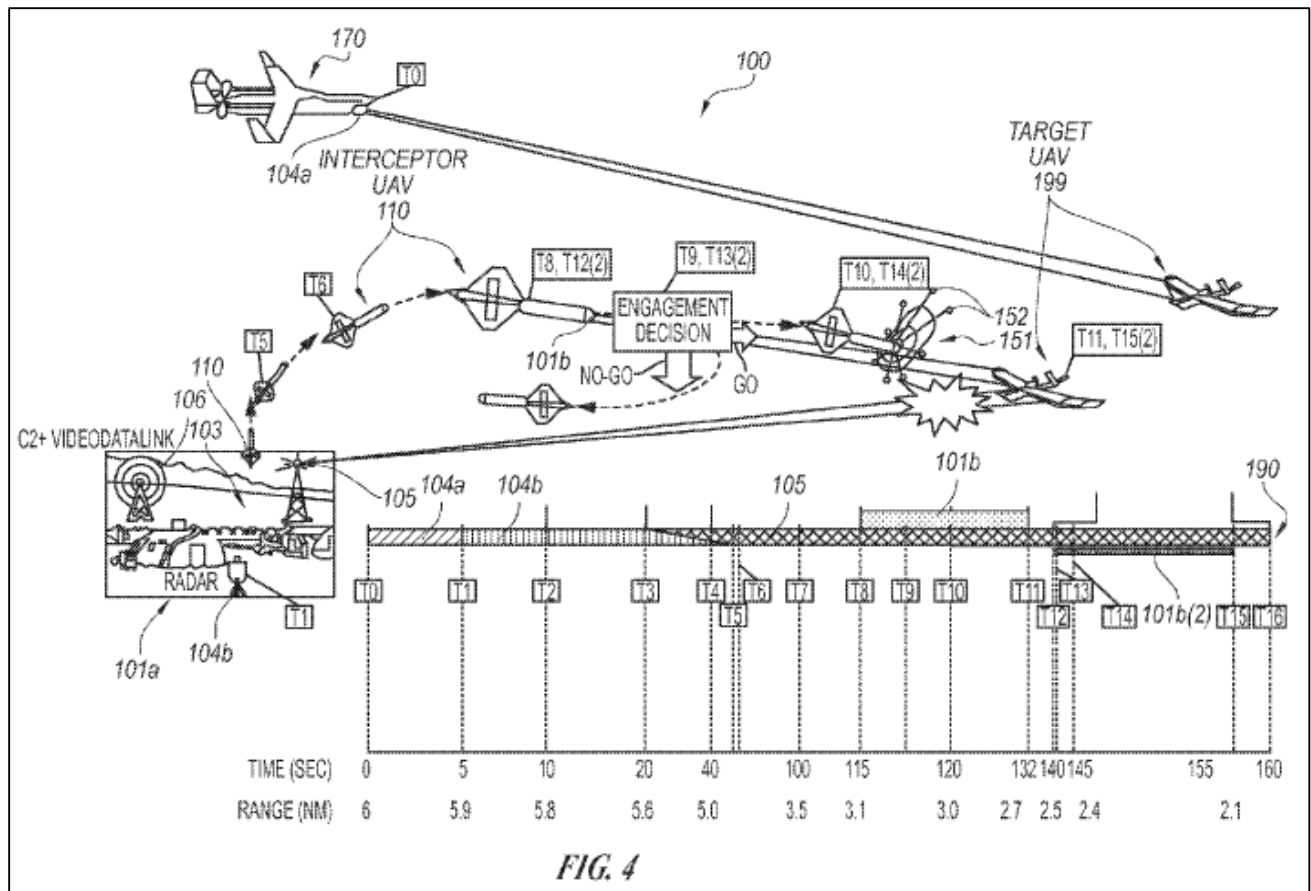
1. Motivation to Combine

a) *Whitmarsh* with *Goodrich*

Whitmarsh discloses a UAV defense system that receives wireless communications from nearby UAVs that include information or signatures unique to the UAVs, such as a MAC address of the UAV, that is used to identify the transmitting UAV. *See* EX1005, [0020], [0027]; EX1006, [0008], [0010], [0013], [0015]-[0017]. Upon determining that the transmitting UAV is unauthorized or hostile, the UAV defense system “develops one or more countermeasures based on the identity and/or position of the detected UAV 14.” EX1005, [0017], [0027]; EX1006, [0010], [0016]-[0018]. For example, the countermeasure system may employ an “intercept countermeasure” wherein “the UAV defense system 10 may dispatch one or more security vehicles 44 and operate it so that it actually collides with the detected UAV 14.” EX1005, [0017]-[0018]; EX1006, [0011]. Similarly,

Whitmarsh Provisional (EX1006), which is incorporated by reference in *Whitmarsh*, discloses an intercept countermeasure wherein “armed drone systems” are deployed to “intercept (e.g., shoot down) the unauthorized or hostile drone.” EX1006, [0011]; EX1005, [0001] (incorporating by reference *Whitmarsh Provisional*).

Goodrich discloses a counter-UAV system that deploys “an interceptor UAV 110 configured to disable or destroy a target UAV 199.” EX1008, [0011], [0014]. Upon detecting a “target UAV,” the counter-UAV system calculates an “intercept track for the interceptor UAV 110,” and then “launch[es]” the interceptor UAV. *Id.*, [0024]. When the interceptor UAV is in range of the target UAV, an “engagement decision” is made to direct the interceptor UAV to either “abort” the intercept track and return to its base or engage the target UAV by executing a “terminal maneuver,” such as deploying a “disabling system 150 . . . that make[s] contact with, tangle with, and/or otherwise disable the target UAV.” UAV. *Id.*, [0027]-[0031]. Figure 4 of *Goodrich*, copied below, depicts the process of deploying an interceptor UAV and executing an engagement decision:



EX1008, Fig. 4.

A POSITA would have been motivated for several reasons to implement *Goodrich's* counter-UAV system, including the interceptor UAV and its disabling system 150, alongside *Whitmarsh's* UAV defense system to disable any UAV that do not pass *Whitmarsh's* authentication check. EX1003, ¶171.

First, a POSITA implementing *Whitmarsh's* UAV defense system and intercept countermeasure would have recognized that *Whitmarsh* (and *Whitmarsh Provisional*) does not provide all details about implementing the intercept countermeasure. *Id.*, ¶172. Accordingly, a POSITA would have been motivated to

look for other sources providing particular details for launching an interceptor UAV/drone and executing an intercept countermeasure, such as *Goodrich*. *Id.*

Second, market forces and design incentives would have motivated a POSITA to implement *Whitmarsh*'s intercept countermeasure as described by *Goodrich*. As discussed above, *Whitmarsh*'s intercept countermeasure may involve "dispatch[ing] one or more security vehicles 44 and operat[ing] it so that it actually collides with the detected UAV 14." EX1005, [0017]-[0018]; EX1006, [0011]. A POSITA would have recognized that by operating the "security vehicle" in such a manner, there is a risk that the security vehicle is destroyed or otherwise damaged in the process, thereby introducing additional cost to *Whitmarsh*'s solution to account for repairing or replacing the damaged security vehicle. EX1003, ¶173. Accordingly, a POSITA implementing *Whitmarsh*'s countermeasures system would have been motivated to look for other solutions for deploying an interceptor UAV, such as that provided by *Goodrich*, wherein an intercepting drone can be reused multiple times because it is, for example, capable of launching a net to disable a target UAV and returning to base in when engagement is abandoned. *Id.*

Third, incorporating *Goodrich*'s counter-UAV system and its use of interceptor UAVs with *Whitmarsh*'s UAV defense system is applying a known technique (*Goodrich*'s counter-UAV system and intercepting drone) to improve similar devices (*Whitmarsh*'s UAV defense system and countermeasures system) in

the same way. EX1003, ¶174; *KSR Int'l*, 550 U.S. at 417. The results of the combination would be predictable: launching interceptor UAVs (as taught by *Goodrich*) to disable detected UAV if the authentication of the detected UAV fails (as taught by *Whitmarsh*). EX1003, ¶174.

Accordingly, a POSITA would have been motivated to combine *Whitmarsh* and *Goodrich* and would have had a reasonable expectation of success in doing so. EX1003, ¶175

2. Claim 1

a) 1[p]

See supra, VIII.A.1.(a).

b) 1[a]

See supra, VIII.A.1.(b).

c) 1[b]

See supra, VIII.A.1.(c).

d) 1[c]:

See supra, VIII.A.1.(d).

e) 1[d]

See supra, VIII.A.1.(e).

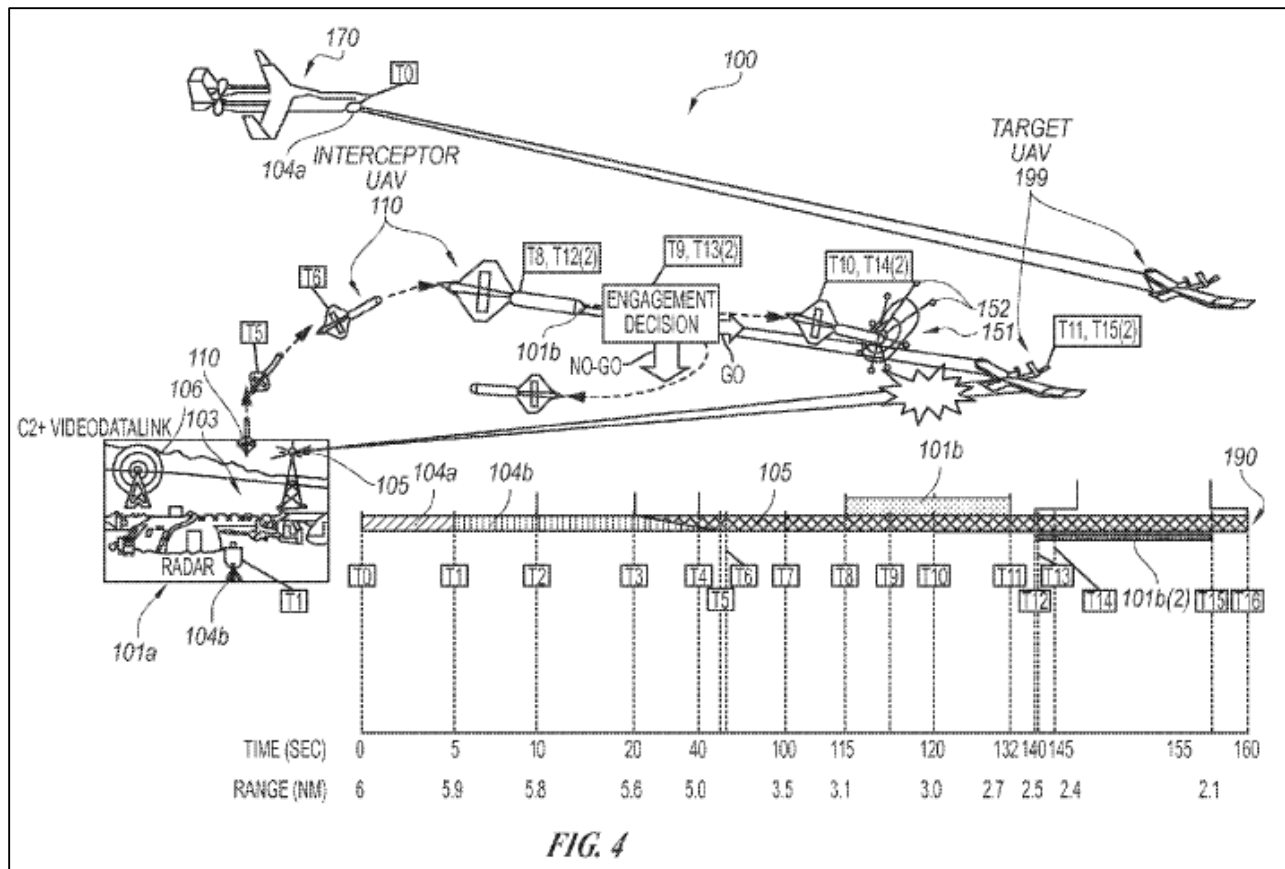
f) 1[e]

See supra, VIII.A.1.(a).

g) 1[f]

For the same reasons discussed above for Ground 1, Limitation 1[f], *Whitmarsh* discloses Limitation 1[f]. *Supra*, VIII.A.1.(g).

In the alternative, the *Whitmarsh-Goodrich* combination renders obvious this limitation. *Goodrich* discloses a counter-UAV system that deploys “an interceptor UAV 110 configured to disable or destroy a target UAV 199.” EX1008, [0011], [0014]. Upon detecting a “target UAV,” the counter-UAV system calculates an “intercept track for the interceptor UAV 110” and then “launch[es]” the interceptor UAV. *Id.*, [0024]. When the interceptor UAV is in range of the target UAV, an “engagement decision” is made to direct the interceptor UAV to either “abort” the intercept track and return to its base or engage the target UAV by executing a “terminal maneuver.” *Id.*, [0027]-[0030]. Figure 4 of *Goodrich*, copied below, depicts the process of deploying an interceptor UAV and executing an engagement decision:



EX1008, Fig. 4.

A “terminal maneuver” may comprise various techniques for disabling the target UAV, including deploying a “disabling system 150 . . . that make[s] contact with, tangle with, and/or otherwise disable the target UAV.” *Id.*, [0031]. Examples of the disabling system 150 include a “net gun 153” that “directs a net 151” with “weights 152,” as well as “projectile, explosive, and/or energy-based components (e.g., lasers and/or high-powered RF generators).” *Id.*, [0037]. Because *Goodrich’s* interceptor UAV is configured to disable a target UAV as described, the interceptor UAV discloses “a disruption system.”

In the combined *Whitmarsh-Goodrich* system, a POSITA would have understood that *Goodrich*'s counter-UAV system, including the interceptor UAV and its disabling system 150, would be implemented alongside *Whitmarsh*'s UAV defense system to disable UAVs that do not pass *Whitmarsh*'s authentication check. EX1003, ¶185. In particular, in the combined *Whitmarsh-Goodrich* system, *Goodrich*'s interceptor UAV would be launched when *Whitmarsh*'s UAV defense system first detects a UAV upon receiving the UAV's signature (e.g., MAC address) from the UAV (as described above with reference to Limitations 1[a]-[b], *see supra*, VIII.C.2.(b)-(c)). EX1003, ¶185.

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.

Accordingly, the *Whitmarsh-Goodrich* combination renders obvious this limitation.

3. Claim 2

See supra, VIII.A.2.

4. Claim 3

See supra, VIII.A.3.

5. Claim 5

As discussed above with reference to Ground 1, *Whitmarsh* discloses Claim 5 when its intercept countermeasure is deployed. *See supra*, VIII.A.4. Thus, Claim 5 is disclosed for at least the same reasons.

In the alternative, when the “*disruption system*” is rendered obvious by the *Whitmarsh-Goodrich* combination (as discussed above with reference to Limitation 1[f], *supra* VIII.C.2.(g)), Claim 5 is taught by *Goodrich*’s disclosure of executing a terminal maneuver to disable a target UAV. As discussed above with reference to Limitation 1[f], after *Goodrich*’s interceptor UAV is launched, an “engagement decision” is made to direct the interceptor UAV to perform a “terminal maneuver,” which includes deploying a “disabling system 150 . . . that make[s] contact with, tangle with, and/or otherwise disable the target UAV.” *Supra*, VIII.C.2.(g); EX1008, [0031]. An example of the disabling system 150 includes a “net gun 153” that “directs a net 151” with “weights 152” at the target UAV. *Id.*, [0037]. When implemented as a net gun, the disabling system causes the net to “tangle with or otherwise become caught in the propeller(s), fuselage, lifting surfaces and/or other elements of the target UAV 199, so as to interfere with and disable the controlled flight of the target UAV 199.” *Id.*, [0032]. A POSITA would have understood that

disabling the controlled flight of a target UAV would cause the target UAV to be “*removed from the airspace*,” e.g., due to the UAV falling to the ground due because it is unable to fly. EX1003, ¶192.

Accordingly, when *Goodrich*’s interceptor UAV is configured by an engagement decision to perform a terminal maneuver, the interceptor UAV (“*the disruption system*”) is enabled to remove a target UAV (e.g., an unauthenticated UAV as taught by *Whitmarsh*) from an airspace. Thus, the *Whitmarsh-Goodrich* combination renders Claim 5 obvious.

6. Claim 6

As discussed above with reference to Ground 1, *Whitmarsh* discloses Claim 6. *See supra*, VIII.A.5. Thus, Claim 6 is disclosed for at least the same reasons.

In the alternative, when the “*disruption system*” is rendered obvious by the *Whitmarsh-Goodrich* combination (as discussed above with reference to Limitation 1[f] and Claim 5, *supra* VIII.C.2.(g) and VIII.C.5), Claim 6 is taught by *Goodrich*’s interceptor UAV including a disabling system such as a “net gun 153” (“*a projectile launcher*”) that launches a “net 151.” (“*an interdiction module*”). *See supra*, VIII.C.2.(g), VIII.C.5; EX1008, [0037]. This understanding of *Goodrich*’s net 151 as an “*interdiction module*” is consistent with the ’199 Patent, which identifies “a net that entangles the aerial system motive mechanism” as “a first variation” of “the

interdiction module.” See EX1001, 11:40-41. Accordingly, *Goodrich* discloses Claim 6, and the *Whitmarsh-Goodrich* combination renders Claim 6 obvious.

7. Claim 7

As discussed above with reference to Ground 1, *Whitmarsh* discloses, or at least renders obvious, Claim 7. See *supra*, VIII.A.6. Thus, Claim 7 is disclosed, or at least rendered obvious, for at least the same reasons.

In the alternative, when the “*disruption system*” is rendered obvious by the *Whitmarsh-Goodrich* combination (as discussed above with reference to Limitation 1[f] and Claim 5, *supra* VIII.C.2.(g) and VIII.C.5), Claim 7 is taught by *Goodrich*’s “interceptor drone” that is equipped with (“*coupled to*”) a “net gun 153” that launches a “net 151” (“*an interdiction module*”), as discussed above with reference to Limitation 1[f] and Claims 5 and 6. See *supra*, VIII.C.2.(g), VIII.C.5-6; EX1008, [0037]. Accordingly, *Goodrich* discloses Claim 7 for the same reasons, and the *Whitmarsh-Goodrich* combination renders Claim 7 obvious.

8. Claim 8

As discussed above with reference to Ground 1, *Whitmarsh* discloses, or at least renders obvious, Claim 8. See *supra*, VIII.A.7. Thus, Claim 8 is disclosed, or at least rendered obvious, for at least the same reasons.

In the alternative, when the “*disruption system*” is rendered obvious by the *Whitmarsh-Goodrich* combination (as discussed above with reference to Limitation

1[f], *supra* VIII.C.2.(g)), Claim 8 is taught by *Goodrich*'s guidance system. *Goodrich*'s interceptor UAV (“*the disruption system*”) includes a “guidance system 130 (e.g., computer-based or controlled)” that “control[s] and guide[s] the interceptor UAV 110 toward its target” (“*a control system for controlling the disruption system*”). EX1008, [0014], [0019]. Accordingly, *Goodrich* discloses Claim 8, and the *Whitmarsh-Goodrich* combination renders Claim 8 obvious.

9. Claim 9

See supra, VIII.A.8.

D. Ground 4: The Combination of *Whitmarsh*, *Goodrich*, and *Falk* Renders Obvious Claim 4

1. Motivation to Combine

a) *Whitmarsh* with *Goodrich*

See supra, VIII.C.1.(a).

b) *Whitmarsh* with *Falk*

See supra, VIII.B.1.(a).

2. Claim 4

See supra, VIII.B.2.

E. Ground 5: The Combination of *Viggiano* and *Goodrich* Renders Obvious Claims 1, 3, and 5-9

1. Motivation to Combine

a) *Viggiano* with *Goodrich*

Viggiano discloses an “authentication apparatus” that “employs an authentication challenge-response methodology and encryption techniques to authenticate the identity of an ADS-B [Automatic Dependent Surveillance-Broadcast] equipped aircraft, vehicle or station.” EX1007, [0012]. The employed authentication challenge-response methodology generally comprises issuing, by an “Authenticator,” an authentication challenge to the ADS-B equipped aircraft/vehicle. *Id.*, [0012]-[0013]. The ADS-B equipped aircraft/vehicle generates and returns an “authentication response” to the Authenticator, which then compares information included in the authentication response with an expected response—if the values match, the identity of the ADS-B equipped aircraft/vehicle is authenticated. *Id.*

As discussed above with reference to Ground 3, Limitation 1[f], *Goodrich* discloses a counter-UAV system that includes “an interceptor UAV” configured to deploy a “disabling system 150,” such as a “net gun” that shoots a net at a target UAV, to disable a target UAV in response to an “engagement decision” that is made after the interceptor UAV is launched. *Supra*, VIII.C.1.(a), VIII.C.2.(g).

A POSITA would have been motivated for several reasons to implement *Goodrich*’s counter-UAV system, including the interceptor UAV and its disabling system 150, alongside *Viggiano*’s authentication apparatus to disable any ADS-B equipped aircraft/vehicle that do not pass *Viggiano*’s authentication check. EX1003,

¶207. Further, a POSITA would have understood that a UAV, such as a “target UAV” as taught by *Goodrich*, could be one of *Viggiano*’s “ADS-B equipped aircraft[s], vehicle[s], or station[s],” as it was known in the art that UAVs (also referred to as UASs or drones) could be equipped with ADS-B transceivers. *Id.* (citing EX1009-EX1012 and EX1017, which describe UAV/UAS configured for ADS-B-based communication).

First, *Viggiano* provides an express motivation to implement *Goodrich*’s counter-UAV system for disabling aircraft. One of *Viggiano*’s goals is to develop a “method of authenticating an aircraft’s identity, thereby making it more difficult for unauthorized third parties to enter a given air traffic control region by broadcasting false identification data for an aircraft.” EX1007, [0004]. However, *Viggiano*’s solution only aids in the identification of authorized or unauthorized UAVs—it does not describe the prevention or removal of unauthorized UAVs upon their detection. *See generally*, EX1007. Accordingly, a POSITA would have been motivated to look for solutions for protecting a given air traffic control region against unauthorized aircraft and would have understood that *Goodrich* offers one such solution. EX1003, ¶208.

Second, design incentives and market forces would have motivated a POSITA to incorporate *Goodrich*’s counter-UAV system alongside *Viggiano*’s authentication apparatus. At the time of the alleged invention, operators of an airspace, such as an

“air traffic control region” disclosed by *Viggiano*, would have been motivated to protect the airspace and its occupants (*e.g.*, personnel and equipment) from exposure to unauthorized aircraft (*e.g.*, certain ADS-B equipped UAVs or drones), which could improperly survey or otherwise damage the airspace’s occupants. EX1003, ¶209. Accordingly, in addition to identifying such unauthorized aircraft (as taught by *Viggiano*), a POSITA would have understood that having a system for disabling such unauthorized aircraft (as taught by *Goodrich*) would improve the security and overall viability of an airspace. *Id.*

Third, incorporating *Goodrich*’s counter-UAV system and its use of interceptor UAVs with *Viggiano*’s authentication apparatus is applying a known technique (*Goodrich*’s counter-UAV system) to improve similar devices (*Viggiano*’s authentication apparatus) in the same way. EX1003, ¶210; *KSR Int’l*, 550 U.S. at 417. The results of the combination would be predictable: launching interceptor UAVs (as taught by *Goodrich*) to disable detected ADS-B equipped aircraft (*e.g.*, an ADS-B equipped UAV or drone) if the authentication of the detected ADS-B equipped aircraft fails (as taught by *Viggiano*). EX1003, ¶210.

Accordingly, a POSITA would have been motivated to combine *Viggiano* and *Goodrich* and would have had a reasonable expectation of success in doing so. EX1003, ¶211.

2. Claim 1

a) 1[p]

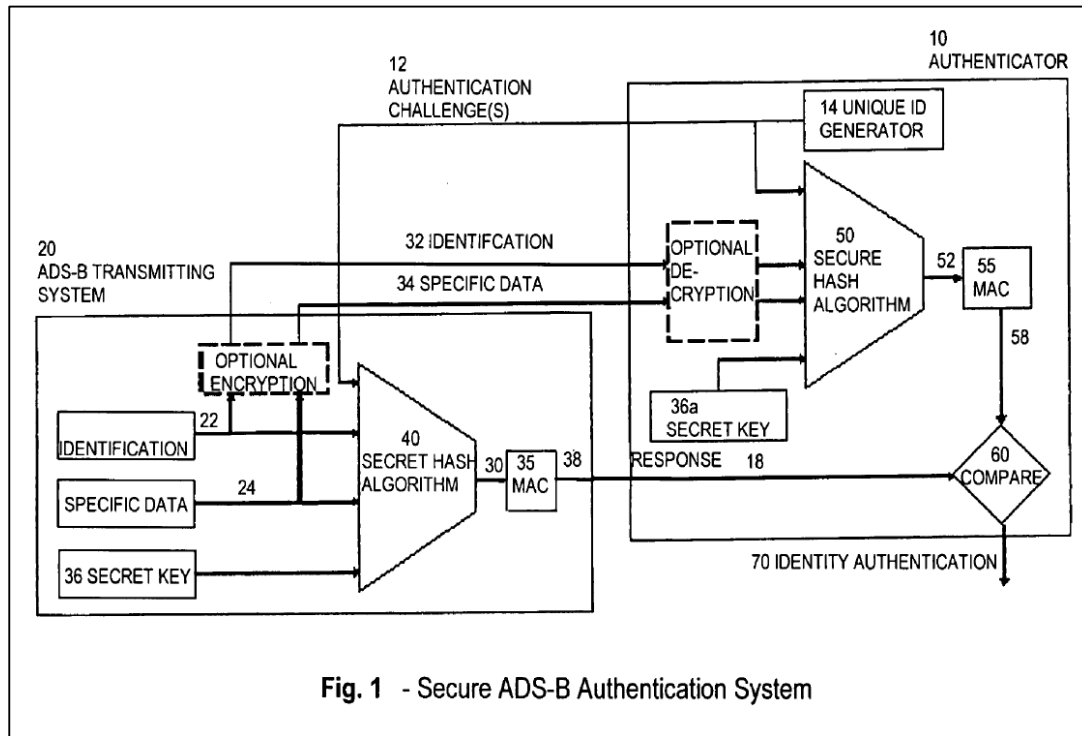
To the extent the preamble is limiting, *Viggiano* discloses the preamble. *Viggiano* describes an “authentication apparatus” that “employs an authentication challenge-response methodology and encryption techniques to authenticate the identity of an ADS-B equipped aircraft.” EX1007, [0012]. The employed authentication challenge-response methodology generally comprises issuing, by an “Authenticator,” an authentication challenge to the ADS-B equipped aircraft. *Id.*, [0012]-[0013] (explaining that the “Authenticator” may be another “ADS-B equipped aircraft, vehicle, vessel or ground station”). Based on information included in the authentication challenge, as well as other information unique to the ADS-B equipped aircraft, the ADS-B equipped aircraft generates and returns an “authentication response” to the authenticator. *Id.*, [0015]. The authenticator then processes the authentication response to determine if “the identity of the ADS-B transmitter” (*i.e.*, the ADS-B equipped aircraft) is “authenticated.” *Id.*

Accordingly, *Viggiano*’s authentication apparatus, which discriminates between authenticated and unauthenticated aircraft, discloses a “*discrimination system.*”

b) 1[a]

Viggiano describes an “ADS-B equipped aircraft” “transiting through an airspace [that] is broadcasting its specific position data 24 and a unique ID 22, for

example, a Mode S address.” EX1007, [0012]; *see also id.*, [0024] (referring to “ADS-B transmitter ID, 22 and 32”). The aircraft (“*aerial system*”) broadcasts the unique ID via an “ADS-B transmitting system.” *Id.*, [0013], Fig. 1 (depicting “ADS-B transmitting system 20”).



EX1007, Fig. 1.

The unique ID, along with other information, such as a Message Authentication Code (MAC) 38, specific data 24 (which may include “such data as position, velocity, and intent” of an aircraft), are transmitted in an “authentication response 18,” which “is broadcast as part of the Mode S ADS-B message.” *Id.*, [0013], [0016] (“In a preferred embodiment, . . . the authentication response 18 is broadcast as part of the Mode S ADS-B message, using unused and/or reserved bits

in the Mode S ADS-B message.”). The MAC 38 included in the authentication response is produced based in part on a unique identifier received in an authentication challenge from a ground-based Authenticator, such that a POSITA would have understood the MAC 38 itself to be unique. *Id.*, [0012]-[0013]; EX1003, ¶215. The MAC 38 is then compared against an “Authenticator-generated MAC 58” to authenticate the identity of the transmitting ADS-B transmitting system. EX1007, [0015]. The unique identifier received in the authentication challenge “can be random values, [but] it need only be unique so that attackers cannot ‘learn’ a valid response by observing the challenges 12 of the authenticator and the corresponding responses 38.” *Id.*, [0013].

Accordingly, the authentication response is an “*aerial system identifier signal*,” because it is a signal broadcast by the ADS-B transmission system that includes a unique ID 22 associated with the aircraft. Further, the authentication response is “*unique to the aerial system*” because it includes both the unique ID 22—which is unique to the transmitting aircraft—and the MAC 38—which is generated based on data unique to the transmitting system (*e.g.*, the unique identifier received in an authentication challenge) in a manner that is designed to prevent illicit duplication. *See id.*, [0012]-[0013].

Finally, *Viggiano*’s “ADS-B transmitting system” is “*coupled*” to its associated aircraft. As noted above, *Viggiano*’s system and methods are employed

to “authenticate the identity of an *ADS-B equipped aircraft, vehicle, or station.*” EX1007, [0012]. A POSITA would have understood that the ADS-B transmitting system is the component with which the “ADS-B equipped aircraft” is equipped, because ADS-B transmitters were well-known components added to aircrafts as part of aviation surveillance solutions. EX1003, ¶217. Accordingly, a POSITA would have understood that the ADS-B transmitting system (“*identifier transmission system*”) is coupled to the ADS-B equipped aircraft (“*aerial system*”).

Accordingly, *Viggiano*’s ADS-B transmission system (“*an identifier transmission system coupled to an aerial system*”), which broadcasts an authentication response that comprises a unique ID and a MAC unique to the ADS-B transmission system (“*is configured to broadcast an aerial system identifier signal unique to the aerial system*”) teaches Limitation 1[a].

c) 1[b]

Viggiano discloses Limitation 1[b] at least through its disclosure of an Authenticator (e.g., “Authenticator 10”). As discussed above with reference to Limitations 1[p] and 1[a], *Viggiano*’s authentication apparatus comprises an “Authenticator” that issues an authentication challenge to ADS-B equipped aircraft and receives an authentication response from the ADS-B transmitting system of the ADS-B equipped aircraft. *Supra*, VIII.E.2.(a)-(b); EX1007, [0012]-[0015]. And as discussed above with reference to Limitation 1[a], the authentication response

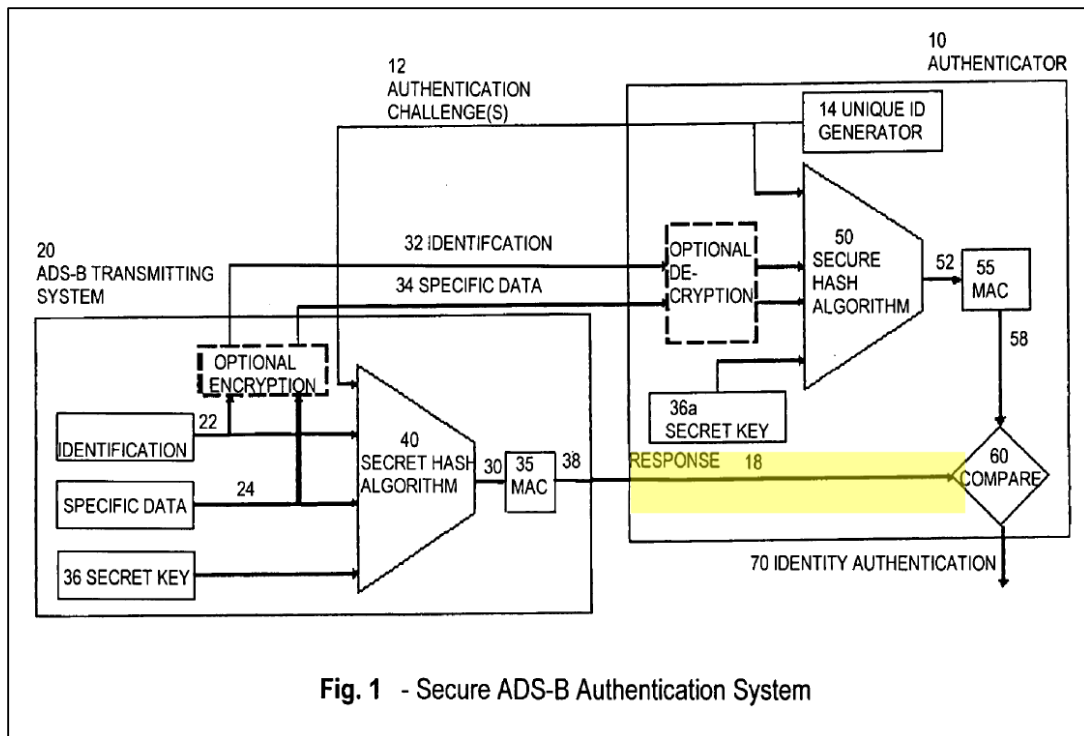
comprises, among other information, a “unique ID” of the ADS-B transmitting system. *Supra*, VIII.E.2.(b); EX1007, [0013]. Accordingly, *Viggiano*’s Authenticator, which receives a unique ID of an ADS-B transmitting system of an ADS-B equipped aircraft, discloses an “*identification receiver*.”

d) 1[c]

The *Viggiano-Goodrich* combination discloses, or at least renders obvious, “a *permission module*,” as addressed in Limitation 1[e]. *See infra*, VIII.E.2.(f).

e) 1[d]

As discussed above with reference to Limitations 1[a] and 1[b], *Viggiano*’s authenticator (“*the identification receiver*”) is configured to receive the authentication response (“*the aerial system identifier signal*”) from the ADS-B transmitting system. *Supra*, VIII.E.2.(b)-(c); EX1007, [0015] (describing authenticator 10’s reception of authentication response 18). As depicted in Figure 1, annotated below, authenticator 10 passes authentication response 18 (“*provide[s] the aerial system identifier signal*”) to comparator 60 (“*to the permission module*”):



EX1007, Fig. 1.

Accordingly, *Viggiano* discloses this limitation.

f) 1[e]

The *Viggiano-Goodrich* combination discloses this limitation, regardless of whether the “*permission module*” term is subject to §112(f). EX1003, ¶223.

(a) Function:

Viggiano discloses the claimed function “*determin[ing] that the aerial system associated with the aerial system identifier signal is not permitted to be in an airspace.*” As discussed above with reference to Limitation 1[p], *Viggiano*’s authenticator is configured to process the authentication response received from the ADS-B transmitting system to authenticate the ADS-B transmitter’s identity. *Supra*,

VIII.E.2.(a); EX1007, [0015]. This processing is performed by “comparator 60” included in the authenticator. In particular, comparator 60 is configured to compare MAC 38, which is received in the authentication response sent by the ADS-B transmitting system (*see supra*, VIII.E.2.(b), EX1007, [0013]-[0014]), with an “Authenticator-generated MAC 58;” if these values match, “the identity of the ADS-B transmitter is authenticated” (EX1007, [0015]). If “two or more consecutive authentication response comparisons” are failed, however, then “authenticator 10 notifies a responsible higher command authority” or otherwise issues a notification to other ADS-B equipped devices. *Id.*

Authenticating an aircraft’s identity in this manner addresses its goal of “making it more difficult for unauthorized third parties to enter a given air traffic control region by broadcasting false identification data for an aircraft.” EX1007, [0004]-[0005]. Thus, when comparator 60 authenticates an aircraft’s identity through the method just described, it also determines whether the aircraft permitted to enter (“*to be in*”) a given air traffic region (“*an airspace*”), where two consecutive authentication failures indicate that the aircraft does ***not*** have permission to be in the air traffic region. Accordingly, *Viggiano* discloses the claimed determining functionality.

(b) Structure:

Viggiano discloses the claimed “*permission module*” regardless of whether that term is subject to §112(f). As discussed above, *Viggiano*’s “comparator” is the component that compares received MAC 38 with Authenticator-generated MAC 58, thereby determining an aircraft’s identity and permission to enter a given air traffic region. *See supra*, VIII.E.2.(f).(a). It “compares” two values—a MAC 38 and an Authenticator-generated MAC 58—to determine whether they match. MAC 38 may be “the last 8-bits of [a] computed hash value 30,” which a POSITA would have understood to mean that the MAC 38 (and, by extension, the Authenticator-generated MAC 58) is a digital signal. EX1007, [0018]; EX1003, ¶226. Accordingly, a POSITA would have understood that *Viggiano*’s comparator is, or at least renders obvious, a “computing system” capable of comparing digital signals, which is a well-known functionality of such a component. *Id.* Further, the comparator’s functionality may be performed by “identity authentication processing including comparison processing for comparing the independently generated authentication codes,” which a POSITA would have understood to mean that the “comparator” may be a “processor” (*i.e.*, “computing system”) for performing the comparing function. EX1007, [0011]; EX1003, ¶226.

If “*permission module*” is subject to §112(f), *Viggiano*’s comparator also discloses, or at least renders obvious, the corresponding structure identified above. *See supra*, VI. As discussed above, the comparator compares a received MAC 38

with an Authenticator-generated MAC 58 to determine if the two values match, thereby indicating whether the transmitting aircraft is authenticated and permitted to be in an airspace. *See supra*, VIII.E.2.(f).(a). And as discussed above with reference to Limitation 1[a], the MAC 38 is generated based on data unique to the transmitting system (*e.g.*, the unique identifier received in an authentication challenge), such that a POSITA would have understood that the MAC 38 is an “aerial system parameter.” *Supra*, VIII.E.2.(b); EX1007, [0012]-[0013]; EX1003, ¶227. The Authenticator-generated MAC 58 is generated by *Viggiano*’s authenticator and is the value that the authenticator expects MAC 38 to be if the transmitting aircraft is an authentic (and, therefore, permitted), such that a POSITA would have understood Authenticator-generated MAC 58 to be a “permission of the airspace.” EX1007, [0015]; EX1003, ¶227. Thus, *Viggiano*’s comparator discloses, or at least renders obvious, a computing system programmed to compare an aerial system parameter, such as an identifier, with the permissions for the airspace. EX1003, ¶227.

g) 1[f]

As discussed above with reference to Ground 3, Limitation 1[f], *Goodrich* discloses “*a disruption system*” through its teaching of a counter-UAV system that includes “an interceptor UAV” configured to deploy a “disabling system 150,” such as a “net gun” that shoots a net at a target UAV, to disable a target UAV in response

to an “engagement decision” that is made after the interceptor UAV is launched. *Supra*, VII.C.2.(g).

In the combined *Viggiano-Goodrich* system, a POSITA would have understood that *Goodrich*’s counter-UAV system, including the interceptor UAV and its disabling system 150, would be implemented alongside *Viggiano*’s authentication apparatus to disable any ADS-B equipped aircraft that do not pass *Viggiano*’s authentication check. EX1003, ¶230. In particular, in the combined *Viggiano-Goodrich* system, *Goodrich*’s interceptor UAV would be launched when *Viggiano*’s authenticator first detects an ADS-B equipped aircraft upon receiving an authentication response from the aircraft (as described above with reference to Limitations 1[a]-[b], *see supra*, VIII.E.2.(b)-(c)). EX1003, ¶230.

In the combined *Viggiano-Goodrich* system, the process of launching interceptor UAV 110 (as described by *Goodrich*) upon receiving an authentication response (“*the received aerial system identifier signal*”) from an ADS-B equipped aircraft (as described by *Viggiano*) constitutes “*preemptively enabl[ing]*” interceptor UAV 110 “*based [on] the received aerial system identifier signal,*” because interceptor UAV 110 is deployed (*i.e.*, launched) before it engages in disrupting the ADS-B equipped aircraft. Only when the additional step of making an “engagement decision” occurs does the interceptor UAV disrupt the detected ADS-B equipped aircraft, as taught by *Goodrich*. EX1003, ¶232.

Accordingly, the *Viggiano-Goodrich* combination renders obvious this limitation.

3. Claim 3

As discussed above with reference to Limitation 1[b], *Viggiano's* Authenticator, which receives a unique ID of an ADS-B transmitting system of an ADS-B equipped aircraft, discloses an “*identification receiver*.” *Supra*, VIII.E.2.(c). And as discussed above with reference to Limitation 1[p], the Authenticator may be another “ADS-B equipped aircraft, vehicle, vessel or ground station.” *Supra*, VIII.E.2.(a). When implemented as an “ADS-B equipped aircraft, vehicle, [or] vessel,” *Viggiano's* Authenticator (“*identification receiver*”) is a “*mobile device*,” and therefore discloses Claim 3.

4. Claim 5

As discussed above with reference to Ground 3, *Goodrich* discloses Claim 5 when its interceptor UAV deploys disabling system 150. *See supra*, VIII.C.5. For at least the same reasons, when *Goodrich's* interceptor UAV is configured by an engagement decision to perform a terminal maneuver, the interceptor UAV (“*the disruption system*”) is enabled to remove a target UAV (*e.g.*, an ADS-B equipped aircraft as taught by *Viggiano*) from an airspace. EX1003, ¶¶236-237. Thus, the *Viggiano-Goodrich* combination renders this limitation obvious.

5. Claim 6

As discussed above with reference to Limitation 1[f] and Claim 5, *Goodrich's* interceptor UAV includes disabling system such as a “net gun 153” (“*a projectile launcher*”) that launches a “net 151.” (“*an interdiction module*”). *See supra*, VIII.E.2.(g), VIII.C.4; EX1008, [0037]. This understanding of *Goodrich's* net 151 as an “*interdiction module*” is consistent with the '199 Patent, which identifies “a net that entangles the aerial system motive mechanism” as “a first variation” of “the interdiction module.” *See* EX1001, 11:40-41. *Goodrich* therefore discloses Claim 6, and the *Viggiano-Goodrich* combination renders Claim 6 obvious.

6. Claim 7

As discussed above with reference to Limitation 1[f] and Claims 5 and 6, *Goodrich's* interceptor UAV (“*disruption system*”) is an “interceptor drone” that is equipped with (“*coupled to*”) a “net gun 153” that launches a “net 151” (“*an interdiction module*”). *See supra*, VIII.E.2.(g), VIII.E.4, VIII.E.5; EX1008, [0037]. *Goodrich* discloses Claim 7 for the same reasons, and the *Viggiano-Goodrich* combination renders Claim 7 obvious.

7. Claim 8

Goodrich's interceptor UAV (“*the disruption system*”) includes a “guidance system 130 (e.g., computer-based or controlled)” that “control[s] and guide[s] the interceptor UAV 110 toward its target” (“*a control system for controlling the*

disruption system”). EX1008, [0014], [0019]. Accordingly, *Goodrich* discloses Claim 8, and the *Viggiano-Goodrich* combination renders obvious Claim 8.

8. Claim 9

As discussed above with reference to Limitation 1[e], *Viggiano* describes that if “two or more consecutive authentication response comparisons” are failed, “authenticator 10” (*“the identification receiver,” see supra, VIII.E.2.(c)*) authenticator 10 notifies a responsible higher command authority” or otherwise issues a notification to other ADS-B equipped devices. *See supra, VIII.E.2.(f).(a);* EX1007, [0015]. A POSITA would have understood that authenticator 10 operates as a “*logging system*” that “*records*” the comparisons made by comparator 60 (*“the activity of . . . the permission module,” see supra, VIII.E.2.(d)*), to track the occurrence of “**two or more** consecutive” failed authentication comparisons. EX1003, ¶241.

In addition, it would have been obvious to a POSITA that for authenticator 10 to recognize that “two or more consecutive authentication response comparisons” are failed, authenticator 10 would have to record each failed comparison. EX1003, ¶242. Without such recording, every failed comparison would be interpreted as the first (or only) failure, and the detection of consecutive failures would not be possible. *Id.* Thus, it would have been obvious that authenticator 10 operates as a “*logging system*” that “*records*” the comparisons made by comparator 60 (*“the activity*

of . . . the permission module,” see *supra*, VIII.E.2.(d)), to track the occurrence of “**two or more** consecutive” failed authentication comparisons.

Moreover, *Viggiano* explains that “if the ADS-B transmitter's message fails the MAC comparison, the authenticator recomputes the MAC using the last challenge unique identifier for the ADS-B transmitter, thereby reducing false identity authentication comparisons.” EX1007, [0029]. A POSITA would have understood that the authenticator operates as a “*logging system*” that “*records*” the “last challenge unique identifier” sent by the authenticator (“*the activity of . . . the identification receiver,*” see *supra*, VIII.E.2.(c)) to re-use that information in the case of a failed MAC comparison. EX1003, ¶243.

In addition, it would have been obvious to a POSITA that for the authenticator to use the last challenge unique identifier to recompute the MAC, the authenticator would have to record the last challenge unique identifier. EX1003, ¶244. Without such recording, it would not be possible for the authenticator to use that identifier to recompute the MAC. *Id.* Thus, it would have been obvious that the authenticator operates as a “*logging system*” that “*records*” the “last challenge unique identifier” sent by the authenticator to later use it as needed. *Id.*

Accordingly, *Viggiano* discloses, or at least renders obvious, Claim 9.

F. Ground 6: The Combination of Viggiano, Goodrich, and Falk Renders Obvious Claim 4

1. Motivation to Combine

a) Viggiano with Goodrich

See supra, VIII.E.1.(a).

b) Viggiano and Goodrich with Falk

A POSITA would have been motivated to combine and had a reasonable expectation of success in combining *Viggiano* and *Goodrich* as described above. *Supra*, VIII.E.1, VIII.F.1.(a). A POSITA would have been motivated to also combine those references with *Falk*. EX1003, ¶247. As discussed above with reference to Ground 5, *Viggiano* discloses an ADS-B equipped aircraft that includes an ADS-B transmission system, which is used to broadcast the aircraft’s “specific position data 24 and a unique ID 22,” along with other information, such as a Message Authentication Code (MAC) 38, in an “authentication response 18” that “is broadcast as part of the Mode S ADS-B message.” *Supra*, VIII.E.2.(b) (citing EX1007, [0013], [0016]). And as discussed above with reference to Ground 2, *Falk* discloses a “beacon” that is removably attachable to a UAV and is configured to transmit “indicia” (*i.e.*, information identifying a particular unmanned aerial vehicle) via wireless communications resources. *See supra*, VIII.B.1.(a).

A POSITA would have been motivated for several reasons to implement *Falk*’s “beacon” as the “ADS-B transmission system” used by *Viggiano*’s aircraft to

transmit their identification information (e.g., unique IDs) to *Viggiano's* authentication apparatus. EX1003, ¶249.

First, design incentives and market forces would have motivated a POSITA to implement *Falk's* beacon alongside *Viggiano's* authentication apparatus. A POSITA implementing *Viggiano's* authentication apparatus would have understood that its underlying authentication mechanism relies on receiving information, such as a unique ID and a MAC, from an “ADS-B equipped aircraft.” *Id.*, ¶250. Accordingly, a POSITA would have recognized that to improve the viability and effectiveness of the authentication apparatus, they would need to outfit aircrafts that are not manufactured with the ability to communicate over wireless resources (e.g., ADS-B resources) with some mechanism for performing such communications, such as *Falk's* beacon. *Id.* Indeed, one of *Falk's* design goals is to provide a more accessible solution for aircrafts (e.g., UAVs) to identify themselves in an effort to improve UAV regulation and security. EX1011, [0003]-[0009]; EX1012, [0002]-[0008].

A POSITA would have also recognized that UAV owners often own multiple UAVs, such that *Falk's* beacon, which can be removed and attached to multiple UAVs, would have been an attractive mechanism for UAV identification for a considerable customer base. EX1003, ¶251.

Second, incorporating *Falk*'s beacon to transmit aircraft identity information is applying a known technique (*Falk*'s beacon for wireless communication of UAV identity information) to improve similar devices (*Viggiano*'s ADS-B equipped aircraft transmitting information such as a unique ID and MAC) in the same way. EX1003, ¶252; *KSR Int'l*, 550 U.S. at 417. The results of the combination would be predictable: aircrafts that are configured with attachable (and removable) beacons for transmitting aircraft information. EX1003, ¶252. Indeed, this functionality is entirely consistent with *Falk*'s beacon operation, which is further configured for ADS-B-based wireless communication as is done in *Viggiano*. EX1011, [0029], [0046] (describing beacon's compliance with ADS-B standard); EX1012, [0024], [0027] (describing beacon's use of wireless communications networks operating on "frequencies from 500-980 MHz"); EX1003, ¶252 (explaining that the 978 MHz UAT frequency band is a well-known ADS-B resource).

Accordingly, a POSITA would have been motivated to combine *Viggiano*, *Goodrich*, and *Falk* and would have reasonably expected success in doing so.

2. Claim 4

As discussed above with reference to Ground 2, *Falk* discloses a "beacon" that is removably attachable to a UAV and is configured to transmit "indicia" (*i.e.*, information identifying a particular unmanned aerial vehicle) via wireless communications resources. *See supra*, VIII.B.2.

In the *Viggiano-Goodrich-Falk* combination, a POSITA would have understood that *Falk*'s beacon would be incorporated into *Viggiano*'s UAV defense system to act as the ADS-B transmitting system (“*identifier transmission system*”) that wirelessly transmits an associated ADS-B equipped aircraft's information, such as unique ID and MAC, consistent with *Falk*'s description of the beacon as a component that configured to transmit information identifying an aircraft (e.g., UAV) to a remote operator via wireless communications. EX1003, ¶256.

Under this combination, a POSITA would have understood that the beacon (“*the identifier transmission system*”) is “*configured to be reassigned from a first aerial system to a second aerial system.*” First, the beacon is configured to “securely and removably attach” to an aircraft, which a POSITA would have understood to mean it can attach (and reattach) to multiple different aircrafts. EX1011, 3:38-41; EX1012 [0009]; EX1003, ¶257. Accordingly, a POSITA would have understood that the beacon is able to be physically reassigned from one UAV (“*aerial system*”) to another. EX1003, ¶257.

Second, it would have been obvious to a POSITA that the beacon would be reassigned electronically from one UAV to another. Although *Falk* explains that information associated with indicia of the beacon (e.g., the UAV identity information) is not “easily” changeable, a POSITA would have understood that nothing in *Falk* suggests that the information associated with the indicia cannot be

changed or reconfigured. *See supra*, VIII.B.2; EX1011, 6:63-7:2; EX1012, [0022]; EX1003, ¶258. Indeed, *Falk*'s explanation that it is not desirable to change a beacon's indicia when one wants to "associate certain information with the *particular* owner or the *UAV that was used to collect the information*," suggests to a POSITA that changing the indicia (e.g., UAV identity information) *would be* warranted when *Falk*'s beacon is removed from a first aircraft and attached to a second aircraft. *Id.* Accordingly, it would have been obvious that under the *Viggiano-Goodrich-Falk* combination, the "identifier transmission system" (implemented as *Falk*'s beacon) would be "configured to be reassigned from a first aerial system to a second aerial system." *Id.*

IX. OBJECTIVE INDICIA DO NOT SUPPORT PATENTABILITY

Petitioners are unaware of any evidence of secondary considerations of non-obviousness tied to the claimed invention of the '199 Patent identified by PO. Petitioners reserve the right to address any such alleged evidence should PO identify it.

X. CONCLUSION

Petitioners respectfully request that *inter partes* review of the '199 Patent be instituted and that the challenged claim be cancelled as unpatentable under 35 U.S.C. §318(b).

Respectfully submitted,

BAKER BOTTS L.L.P.

A handwritten signature in black ink, appearing to read "Chad C. Walters". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Chad C. Walters (Reg. No. 48,022)

Lead Counsel for Petitioners

Date: February 10, 2025

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies on this 10th day of February 2025, that true and correct copies of the foregoing PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,249,199, Exhibits 1001-1019, and Petitioners' power of attorney were served in their entirety to Patent Owner via FedEx Express® or Express Mail:

Van Pelt, Yi, & James LLP and Airspace Systems, Inc.

1 1st St. Ste. 12

Los Altos, CA 94022

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Counsel for Petitioners

Date: February 10, 2025

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE
REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,998 words, excluding the parts exempted by 37 C.F.R. § 42.24(a).
2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word in 14-point Times New Roman.

Respectfully submitted,

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Counsel for Petitioners

Date: February 10, 2025

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com