

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MERCEDES-BENZ GROUP AG,
Petitioner,

v.

THE PHELAN GROUP, LLC
Patent Owner.

Case (to be assigned)
U.S. Patent No. 11,472,427

**PETITION FOR *INTER PARTES* REVIEW OF
CLAIMS 1-20 OF U.S. PATENT NO. 11,472,427
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. §§42.100 *et seq.***

Filed on behalf of Petitioner:

Celine Jimenez Crowson (Reg. No. 40,357)
Joseph Raffetto (Reg. No. 66,218)
Scott Hughes (Reg. No. 68,385)
HOGAN LOVELLS US LLP
555 13th Street N.W.
Washington, D.C. 20004
Telephone: 202.637.5600
Facsimile: 202.637.5710

TABLE OF CONTENTS

	PAGE
I. INTRODUCTION	1
II. MANDATORY NOTICES (37 C.F.R. §42.8(A)(1)).....	2
A. Real Parties-in-Interest	2
B. Related Matters.....	2
C. Counsel and Service Information.....	4
III. NOTICE OF FEES PAID.....	4
IV. CERTIFICATION OF GROUNDS FOR STANDING	4
V. PRECISE RELIEF REQUESTED	5
VI. '427 Overview	5
A. Background	5
B. Prosecution	6
C. Priority Date	7
VII. CLAIM CONSTRUCTION AND POSITA.....	7
A. Claim Construction.....	7
B. Definition of a Person of Ordinary Skill in the Art.....	7
VIII. ANALYSIS OF GROUNDS FOR UNPATENTABILITY	8
A. Ground 1 – Murphy Anticipates or Renders Obvious Claims 1-6, 8-11, 13-20.....	8
B. Ground 2 – Murphy-Adams Renders Obvious Claim 10	38
C. Ground 3 – Murphy-Wu Renders Obvious Claims 7/12	39
D. Ground 4 – Arshad Renders Obvious Claims 1, 4-6, and 10.....	43
E. Ground 5 – Arshad-Petrik Renders Obvious Claims 2-4 8-9, 11, and 13-20.....	57
F. Ground 6 – Arshad (Alone or as Modified by Petrik) in View of Wu Renders Obvious Claims 7/12.....	70
IX. DISCRETIONARY CONSIDERATIONS UNDER 314(A) AND 325(D) STRONGLY FAVOR INSTITUTION.....	73
X. CONCLUSION.....	75
Appendix A.....	79

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH</i> IPR2019-01469	73
<i>Mercedes-Benz Group AG v. The Phelan Group, LLC,</i> IPR2025-00413	4
<i>Mercedes-Benz Group AG v. The Phelan Group, LLC,</i> IPR2025-00758	3
<i>Mercedes-Benz Group AG v. The Phelan Group, LLC,</i> IPR2025-00919	3
<i>Oticon Medical AB v. Cochlear Ltd.,</i> IPR2019-00975	74
<i>Sotera Wireless, Inc. v. Masimo Corp.,</i> IPR2020-01019	73
<i>The Phelan Group, LLC v. Honda Motor Co., Ltd.,</i> Case No. 2-23-cv-00606 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. Kia Corporation et al.,</i> Case No. 2-23-cv-00094 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. Mercedes-Benz Group AG,</i> No. 1-25-cv-01399 (N.D. Ga.).....	2
<i>The Phelan Group, LLC v. Mercedes-Benz Group AG,</i> No. 2-23-cv-00607 (E.D. Tex.).....	2
<i>The Phelan Group, LLC v. State Farm Mutual Automobile Insurance Co.,</i> Case No. 2-23-cv-00611 (E.D. Tex.).....	3

The Phelan Group, LLC v. Toyota Motor Corporation et al.,
Case No. 2-23-cv-00093 (E.D. Tex.).....3

Other Authorities

37 C.F.R. ¶ 42.100(b).....7

37 C.F.R. §42.8(A)(1).....2

I. INTRODUCTION

Mercedes-Benz Group AG (“**Petitioner**”) challenges Claims 1-20 of US11,472,427 (EX1001) (“**’427**”). The ’427 purportedly invents a “driver authentication and safety system” for “monitoring and controlling vehicle usage.” (’427, Abstract, 2:34-38.) A driver uses an “identification” interface to “authenticate” herself, after which she will be allowed operate the vehicle within her “operating profile,” *e.g.*, maximum speed, location, and hours of operation. (*Id.*, 7:3-29, Cl. 3, 5:63-65, Abstract.) If the driver violates her profile, the system provides feedback, including by generating alarm signals and controlling vehicle operations. (*Id.*)

This was not new at the time of the ’427. For example, US6,225,890 (EX1006) (“**Murphy**”) discloses a near-identical “system for restricting use of a vehicle by a selected vehicle operator.” (Murphy, Abstract, 3:20-40, 11:60-63.) In Murphy, (1) the driver provides “ident indicium” (*e.g.*, unique biometric samples, token or card, keypad code); (2) the system “identifies the driver” and allows vehicle operation within “operation restrictions”; and (3) if the driver does not adhere to such profile, an “alarm signal is transmitted” or “appropriate control actions are taken,” such as “reduc[ing] the vehicle speed.” (*Id.*, Abstract, 5:12-60, 13:28-15:8, 15:9--16:11, 16:50-17:63, Figs. 6-7.)

Similarly, US2003/0189482 (EX1007) (“**Arshad**”) discloses a system for “authoriz[ing]” and monitoring drivers. (Arshad, Abstract, [0028].) In Arshad, a “transponder” is used to identify the driver and transmit “operational limits,” such as “maximum speed,” authorized “geographical area,” and “hours of authorized use.” (*Id.*, [0019], [0033], [0043], [0057].) If these are violated, Arshad can “limit the speed” or disable the vehicle, “display a message,” or sound an “alarm.” (*Id.*, [0043]-[0045], [0063].)

These references, alone and with additional references, invalidate the ’427.

II. MANDATORY NOTICES (37 C.F.R. §42.8(A)(1))

A. Real Parties-in-Interest

The real parties-in-interest are Petitioner Mercedes-Benz Group AG; Mercedes-Benz USA, LLC; Mercedes-Benz AG; and Mercedes-Benz Intellectual Property GmbH & Co. KG.

B. Related Matters

Assignee-of-record The Phelan Group, LLC (“**Phelan**”) asserted the ’427 in the following active proceedings:

- *The Phelan Group, LLC v. Mercedes-Benz Group AG*, No. 1-25-cv-01399 (N.D. Ga.), filed Mar. 17, 2025, transferred from *The Phelan Group, LLC v. Mercedes-Benz Group AG*, No. 2-23-cv-00607 (E.D. Tex.), filed December 15, 2023;

The Georgia court has not set a status conference or entered a case schedule.

Phelan also asserted the '427 in the following proceedings which have been dismissed or stayed:

- *The Phelan Group, LLC v. Toyota Motor Corporation et al.*, Case No. 2-23-cv-00093 (E.D. Tex.), filed March 7, 2023, dismissed with prejudice;
- *The Phelan Group, LLC v. Kia Corporation et al.*, Case No. 2-23-cv-00094 (E.D. Tex.), filed March 7, 2023, dismissed with prejudice.
- *The Phelan Group, LLC v. Honda Motor Co., Ltd.*, Case No. 2-23-cv-00606 (E.D. Tex.), filed December 15, 2023, dismissed with prejudice;
- *The Phelan Group, LLC v. State Farm Mutual Automobile Insurance Co.*, Case No. 2-23-cv-00611 (E.D. Tex.), filed December 18, 2023, stayed based on notice of settlement;

Petitioner has also filed *inter partes* reviews against the following patents which are in the same patent family as the '427:

- *Mercedes-Benz Group AG v. The Phelan Group, LLC*, IPR2025-00919 regarding US10,259,465 (P.T.A.B. Apr. 23, 2025);
- *Mercedes-Benz Group AG v. The Phelan Group, LLC*, IPR2025-00758 regarding US9,908,508 (P.T.A.B. Mar. 21, 2025);

- *Mercedes-Benz Group AG v. The Phelan Group, LLC*, IPR2025-00413 regarding US9,045,101 (P.T.A.B. Jan. 6, 2025).

C. Counsel and Service Information

Lead counsel is Celine Crowson (Reg. No. 40,357). Backup counsel are Joe Raffetto (Reg. No. 66,218), and Scott Hughes (Reg. No. 68,385). Service information is as follows:

Post and Hand Delivery	Hogan Lovells US LLP 555 13th Street N.W. Washington, D.C. 20004
Email	celine.crowson@hoganlovells.com joseph.raffetto@hoganlovells.com scott.hughes@hoganlovells.com
Telephone / Facsimile	202.637.5600 / 202.637.5910

III. NOTICE OF FEES PAID

Fees are submitted herewith. The undersigned authorizes charging additional fees due during the proceeding to Deposit Account No. 50-1349.

IV. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies the '427 is available for *inter partes* review and that it is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Ground	References	Claims	Basis
1	Murphy	1-6, 8-11, 13-20	102/103
2	Murphy with Adams ¹	10	103
3	Murphy with Wu ²	7, 12	103
4	Arshad	1, 4-6, 10	103
5	Arshad with Petrik ³	2-4, 8-9, 11, 13-20	103
6	Arshad (alone or with Petrik) in view of Wu	7, 12	103

VI. '427 OVERVIEW

A. Background

The '427 relates to a “driver authentication and safety system” for “monitoring and controlling vehicle usage.” ('427, Abstract.) An “authorized vehicle owner” can create an “operating profile” for “high-risk drivers.” (*Id.*, 6:39-7:7, 2:34-

¹ “Adams” is US2008/0046739 (EX1009).

² “Wu” is US2008/0114501 (EX1010).

³ “Petrik” is US2007/0168125 (EX1008).

38.) The profile, which can include restrictions like allowable vehicle “speed,” “vehicle location,” and “hours of operation,” is enforced by a “master control unit,” “slave control unit,” and “at least one computer” associated therewith. (*Id.* at 2:32-51, 5:68-6:4, Fig. 6, Cls. 1, 3.)

Drivers authenticate themselves via a “driver identification” interface. (*Id.*, 6:64-7:2, Cl. 1, 2:64-3:1.) Once authenticated, the system monitors vehicle operation, *e.g.*, using GPS “time of day, speed and location” data, and compares this to the driver’s profile. (*Id.*, 7:13-29, Cl. 11.) If the driver violates her profile, the system can provide feedback by generating an “alarm” or governing operation like limiting speed. (*Id.*, 7:13-29, 2:47-51.)

B. Prosecution

The ’427 was filed February 28, 2019 as a continuation of US10,259,465,⁴ filed February 16, 2018, which is a continuation of US9,908,508, filed May 14, 2015, which is a continuation of US9,045,101, filed April 8, 2013, which is a continuation of US8,417,415, filed July 1, 2009, and claims priority to US61/077,568, filed July 2, 2008.

⁴ The original ADS lists the ’427 as a continuation of U.S. App. No. 15/336,110, later US10,259,470, filed October 27, 2016. (EX1002, 219-221). Applicant filed a corrected ADS adding that the ’427 is a continuation of U.S. App. No. 15/898,322, later US10,259,465, which is consistent with the patent’s text and priority chain. (’427, 1:7-10; EX1002, 176-179.)

The '427 received one substantive Office Action, in which Claims 1-20 were rejected for double-patenting. (EX1002, 130-133.) Applicant filed a terminal disclaimer in response. (*Id.*, 112-114.) After corrections to the terminal disclaimer for formalities, a Notice of Allowance issued. (*Id.*, 79-83, 69, 62, 24.)

C. Priority Date

Petitioner assumes, but does not concede, a priority date of July 2, 2008.

VII. CLAIM CONSTRUCTION AND POSITA

A. Claim Construction

Unless indicated otherwise, all claim terms herein are given the ordinary and customary meaning of such term as understood by one of ordinary skill in the art and the prosecution history pertaining to the '427. 37 C.F.R. ¶ 42.100(b).

B. Definition of a Person of Ordinary Skill in the Art

A POSITA would have at least a bachelor's degree in electrical engineering, computer science, or similar disciplines, and at least two years of experience in the automotive industry with research, design, and/or development of automotive electrical and control systems or an equivalent level of skill, knowledge, and experience. (Declaration of Dr. Mark Ehsani (EX1004) (“**Ehsani**”), ¶23.) The more education one has, the less experience needed to attain an ordinary level of skill. (*Id.*) Similarly, more field experience may substitute for formal education. (*Id.*)

VIII. ANALYSIS OF GROUNDS FOR UNPATENTABILITY

A. Ground 1 – Murphy Anticipates or Renders Obvious Claims 1-6, 8-11, 13-20

Murphy anticipates or renders obvious Claims 1-6, 8-11, and 13-20. (Ehsani, ¶¶36-163.) Murphy was filed March 20, 1998, issued May 1, 2001, and is prior art under pre-AIA §102(b).

1. Independent Claims

a) Claim 1

Murphy renders obvious Claim 1. (*Id.*, ¶¶39-77.)

1[pre]: A driver authentication and monitoring system, comprising:

If limiting, Murphy discloses Claim 1[pre]. (*Id.*, ¶40.)

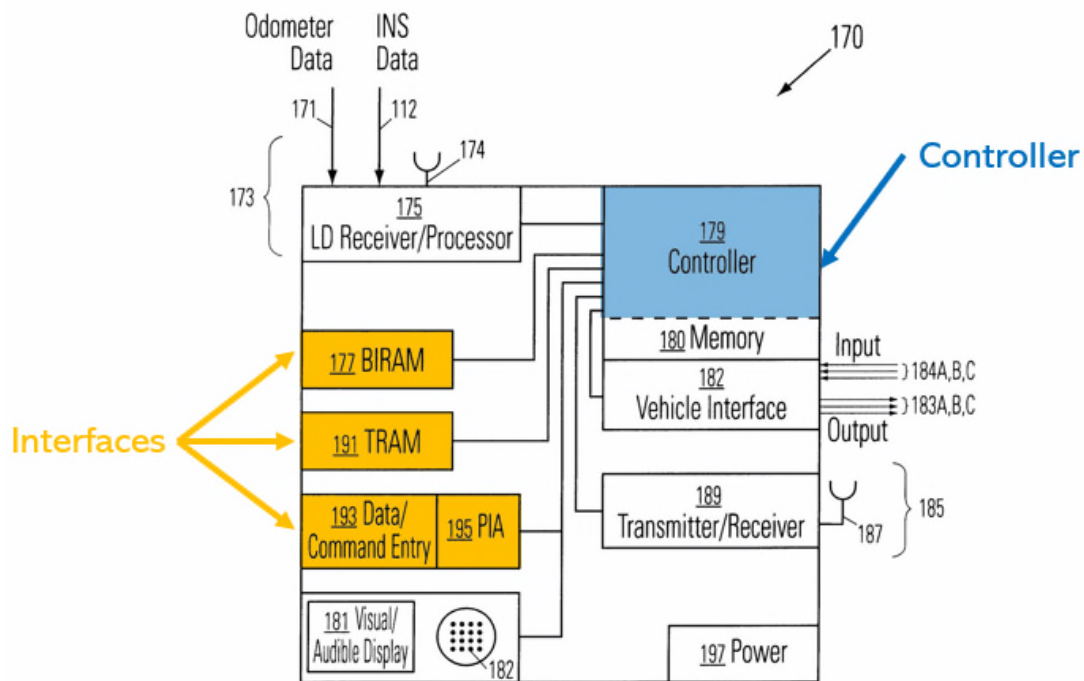
Murphy discloses “[a] *system* for restricting use of a vehicle by a selected vehicle operator” that can be “installed in [the] vehicle dashboard or elsewhere” and “used to *monitor* operation of the vehicle by a teenager or other inexperienced *driver*, with restrictions imposed upon... vehicle maximum speed...,” among other things. (Murphy, Abstract, 15:1-8, 11:60-64, 19:3-12; *see also* Figs. 1, 6-7.)⁵ Murphy’s system includes a “controller” that can “*authenticate*” drivers. (*Id.*, 13:28-42, 14:46-15:31, 6:55-7:29, Figs. 6-7.) *See infra* Claim 1[A].

⁵ All emphasis added unless otherwise indicated.

1[A]: a master control unit operating in a motor vehicle for authenticating at least one driver via a driver identification interface,

Murphy discloses Claim 1[A]. (Ehsani, ¶¶41-46.)

Murphy’s “master control unit” includes a “controller” in a vehicle that “authenticates” drivers via: (1) “biometric indicium receiving and analysis mechanism” (BIRAM); (2) “token receiving analysis mechanism” (TRAM) and “token or smart card”; and (3) “data entry module” (e.g., keypad) and “personal information analysis (PIA) module”:



(Murphy, Fig. 6 (annotated), 13:28-42, 14:46-15:31, 6:55-7:29, Fig. 7.)⁶

When a driver “turn[s] on the ignition,” the system prompts for “a sample of his/her ident indicium (a biometric indicium and/or token or keypad entries).” (*Id.*, 7:49-54, Fig. 2, Abstract.) This information is then “sent to the *controller* module 179 and associated memory module 180” for “*authenticating* the identity” of the driver. (*Id.*, 7:22-24, 13:36-40, 14:51-65, 15:8-54, Figs. 6-7.) The controller “*compares* [this] indicium *with indicia stored*” in the system (*e.g.*, in a “database with identities and matching indicia”) to identify the driver. (*Id.*, 5:12-24, 15:8-21; *see also* 2:26-38, 7:49-63, 10:45-11:27, 14:46-65, 15:55-16:11, 16:50-17:62, Figs. 2-3, 6.) *See infra* Claim 1[B].

1[B]: wherein the master control unit receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver and accessible by the master control unit;

Murphy discloses Claim 1[B]. (Ehsani, ¶¶47-57.)

In Murphy, drivers have different “operating profiles.” For example, they can be divided into categories, with “[*d*]ifferent driving restrictions... imposed[] depending upon the category,” such as different permitted “time intervals and... travel corridor(s) and speeds for travel.” (Murphy, 7:64-8:2, 2:35-53; *see also* 1:66-

⁶ The BIRAM, TRAM and token, and data entry device and PIA can be used alone or in combination. (Murphy, 6:55-61, 7:22-24, 13:28-42, 14:45-15:15, Figs. 6-7.)

2:16, Fig. 2, 7:49-9:44, 5:18-26, 7:3-13, 3:20-47, 11:60-67.) Drivers can also have “*individualized*” restrictions, such as “maximum speed,” “geographic region” and “routes,” “maximum accumulated” mileage and time, and “time intervals” when the vehicle can be driven. (*Id.*, 6:8-17, 17:14-29; *see also* 15:66-16:11, 6:55-7:14, 8:29-53, 10:45-11, Figs. 2-3, Abstract, Cls. 3, 10.) Drivers’ “operating profiles” can be stored in a “database” or “memory” the controller can access. (*Id.*, Figs. 6-7, 13:35-41, 14:51-16:11.)

Further, Murphy receives a “unique identification code” allowing drivers to operate the vehicle using their “operating profile.” Murphy’s token (used with the TRAM) can be “*specific to the person* who presents” it; has “built into it a *circuit or pre-programmed information* in a storage medium that imposes selected restrictions on operation of the vehicle and/or *that identifies the token holder*”; and may rely upon “digitized data” that is “*encoded* or encrypted” and stored in memory. (*Id.*, 6:55-7:14; *see also* 2:32-34, 14:46-61, Cl. 38.)

Similarly, when “identification indicium” is presented through the data entry device and PIA, “information *that is specific to* and known to only *the individual* who presents the information” is used, like a “*coded sequence* of characters...” (*Id.*, 7:15-24; *see also* 14:55-65, Cl. 39.) Finally, the BIRAM can receive “*samples* of an *ident indicium*” unique to the driver, such as a “handprint,” “facial scan,” or “voice sample.” (*Id.*, Abstract, Cl. 37; *see also* 2:20-45, 4:39-5:28, 6:46-54, 15:55-17:2,

17:63-18:19.)⁷

Once a driver is authenticated, *see* Ground 1, Claim 1[A], Murphy accesses her profile to permit her to operate the vehicle in accordance with it. Specifically, when “[ident] indicium is satisfactorily presented and analyzed, the system allows operation of the vehicle” but will monitor “whether the vehicle location and/or speed are within *permitted ranges for the driver* and... whether the present time and/or accumulated time or mileage are within *permitted ranges for the driver*.” (Murphy, Abstract, 8:28-49, Fig. 2; *see also* 2:46-53, 5:13-28, 6:55-7:14, 7:49-8:14, 8:54-61, Fig. 3, 10:45-11:19.) The controller can access the “*limitations* on vehicle operation *for each* authorized vehicle *operator*” and can use this and vehicle information to “determine[] which Control Action(s), if any, should be imposed.” (*Id.*, 15:9-42, Fig. 7; *see also* 13:53-16:17, Fig. 6, 15:66-16:11, 17:14-62, 12:6-27, 14:46-65.)

For example, if the driver violates her profile, the controller can issue a “control action” or command to a vehicle (or control action) interface module, which uses such information to control “the vehicle engine, transmission, fuel supply, braking system... or other appropriate system.” (*Id.*, Fig. 7, 15:32-54, Fig. 6, 13:54-

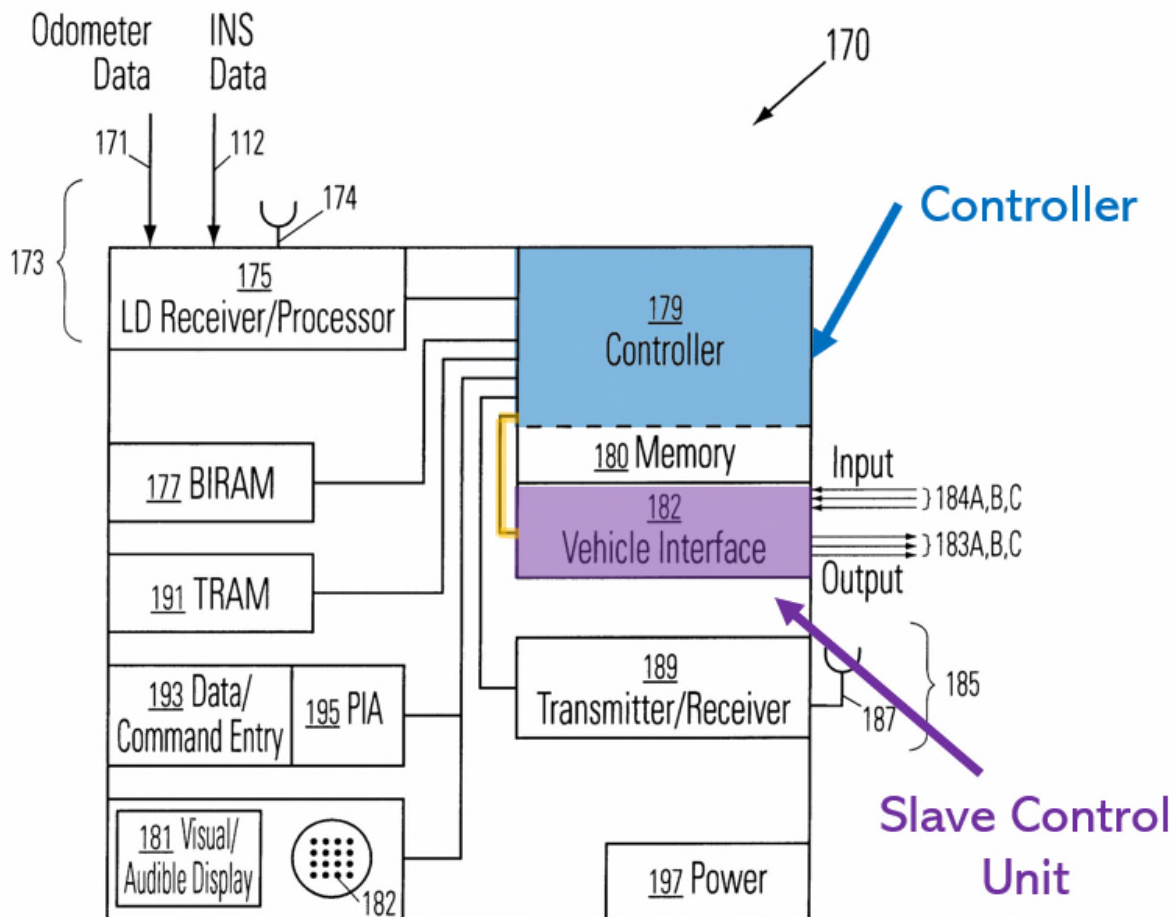
⁷ After Murphy receives “ident indicium” from the BIRAM, TRAM, or PIA, it transmits the “ident information, *or a representation thereof*,” to the controller for comparison. (Murphy, 15:9-21.)

14:17.) Control actions can include “disabl[ing] the vehicle” or “accessories” and “reduc[ing] vehicle speed.” (*Id.*, 5:29-60, Abstract, Fig. 2.) See *infra* Claim 1[D].

1[C]: [i] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, [ii] said slave control unit in communication with said master control unit and...

Murphy discloses Claim 1[C]. (Ehsani, ¶¶58-63.)

First, Murphy discloses a “slave control unit” installed in its in-vehicle system in “communication” with the master control unit. Murphy includes a “*vehicle [or control action] interface module*” “connected to” its “controller”:



(Murphy, Fig. 6 (annotated), 13:28-15:8; *see also* Fig. 7, 15:1-15:54.) The vehicle interface module and controller are “in communication” with each other, including about “which Control Action(s), if any, should be imposed” and whether “vehicle components” have been “activat[ed].” (*Id.*) *See infra* Claim 1[D].

Second, the vehicle interface module (*e.g.*, slave control unit) is “coupled to” multiple “computers” associated with the vehicle. It is connected via its “interface [input/output] terminals” to various components—*e.g.*, “vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories”—and communicates instructions to these components and their “*microcomputers*” to “control[] or restrict[] operation,” such as “reduc[ing] the vehicle speed.” (*Id.*, Fig. 6, 13:53-14:17, Fig. 7, 15:32-54, 16:12-49; *see also* Ehsani, ¶¶59-63.)

It is also coupled to a “telecommunication module 185” (via the controller) and a “remote facility” (via the telecommunication module)—additional computers “associated with the motor vehicle.” (Murphy, 14:23-45, Fig. 6, 16:12-49.) The “remote facility” can “transmit signals that modify, add or delete vehicle operation restrictions” to the telecommunication module. (*Id.*) These “alter[ed] restrictions” are used by the in-vehicle system, including the vehicle interface module, to control driver operation. (*Id.*; *see also* Abstract, 12:16-27, Fig. 1, 16:50-17:63, 4:15-27.) *See*

infra Claims 2-3.⁸

1[D]: *[said slave control unit...] [i] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile thereby providing feedback to the master control unit about a usage of the vehicle, and [ii] wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit.*

Murphy renders obvious Claim 1[D]. (Ehsani, ¶¶64-77.)

First, Murphy’s vehicle interface module (*e.g.*, slave control unit) “cooperates” with “at least one computer” to control operation based on commands from the controller (*e.g.*, master control unit). Murphy’s “control system” can take different “Control Actions” if a driver violates her profile, including:

- (1)...disabl[ing] the vehicle...
- (2)...disabl[ing]... use of selected vehicle accessories...
- (3)...reduc[ing] the vehicle speed...
- (4)...forc[ing] the vehicle to operate only in selected lower gears...
- (5)...turn[ing] on at least one of the lights, exterior flashers and horn continuously or periodically...
- (6)...activat[ing] an on-board alarm...

⁸ The vehicle interface module is further “coupled to” a “visual and/or audible display [or feedback] module”—another “computer”—that provides vehicle operation information to the driver. (Murphy, Fig. 6, 13:61-14:17, Fig. 7, 15:47-50, 16:12-50, 5:55-60, 12:6-15, 10:29-40.)

(7)...transmit[ting] an alarm... to a selected facility... (8)...activat[ing] an air bag or other disabling device... (9)...allow[ing] the vehicle to operate for at most a selected cumulative time interval... (10)...allow[ing] the vehicle to operate only within one or more selected time intervals... (11)...allow[ing] the vehicle to operate for at most a selected cumulative vehicle mileage... and (12)...tak[ing] no action at that time but optionally log[g]ing the activity and allow[ing] the driver to operate the vehicle without restriction for a selected time interval.

(Murphy, 5:13-54; *see also* 17:30-63, 6:1-18.)

Murphy's controller "*determines* which Control Action(s), if any, should be imposed on vehicle use *and communicates this* information to a Control Action [or vehicle] interface module 215 *for implementation* by the vehicle engine, transmission, fuel supply, braking system... or other appropriate system." (*Id.*, 15:36-54, 13:66-14:17, Figs. 6-7.) When Murphy's vehicle interface module receives such a command from the controller, it cooperates with components connected to its "terminals" that are to be controlled, such as by communicating with the components and their "microcomputers" to "*control[] or restrict[]*" their operation. (*Id.*, 13:66-14:17, 2:20-53, 7:49-9:44, 10:45-11:27, 15:9-54, Figs. 2-3, 6-7, Cl. 1, Abstract; Ehsani, ¶¶65-77.)

Similarly, the vehicle interface module cooperates with other computers, like

the “telecommunication module” and “information processing facility,” to control operation based on commands from the controller. When a violation occurs, the telecommunication module transmits an “alarm signal” to the remote computer, which, in turn, sends commands back “to modify or add to the extant parameters for vehicle operation...” (*Id.*, 5:13-60, Cl. 1, 14:23-45; *see also* Abstract, 17:30-63.) The vehicle interface module then cooperates with the telecommunication module and remote computer to control the vehicle, such as by implementing any modified or new restrictions that the controller commands that were received by the telecommunication module from the remote computer. (*Id.*, 14:23-45; *see also* Cls. 7, 9, 12, 15, 18, Abstract, 12:16-27, 4:15-27.) *See infra* Ground 1, Claims 2-3.⁹

Second, regarding being “configured to monitor” operation and “generate” a signal if the driver violates her profile, thereby providing “feedback” about vehicle usage, Murphy’s controller (*e.g.*, master control unit) is configured to monitor “[i]nformation on the present vehicle location and/or vehicle speed and/or time

⁹ Murphy’s vehicle interface module also cooperates with the “visual and/or audible display [or feedback] module” (*e.g.*, computer) to control operation, including when the controller commands the display (or feedback) module to alert the driver she is violating her profile and, absent corrective action, the vehicle interface module disables the vehicle. (Ehsani, ¶¶65-77.)

and/or accumulated operating time and/or accumulated mileage” and “*compar[e]* *this... with* any vehicle operation *restrictions that may be imposed*” on an operator. (*Id.*, 13:53-61; *see also* 1:66-2:53, 7:49-9:44, 10:45-11:27, 13:28-43, 14:18-22, 15:9-16:11, 16:50-17:63, Figs. 2-3, 6-7, Cls. 1, 10, Abstract.) Further, the controller sends “signals” to other components to provide vehicle usage feedback. (*Id.*, 5:29-60, 10:29-40, 12:1-15, 13:61-65, 15:42-54, Figs. 6-7.)

It would have been obvious to a POSITA to modify Murphy to configure the vehicle interface module (instead of the controller) to “monitor” for violations and generate a “signal” to the controller if such a violation occurs, thereby providing feedback. (Ehsani, ¶¶74-77.) That is, it would have been obvious that certain functionality in Murphy’s controller could be implemented in its vehicle interface module. (*Id.*) This would not require additional hardware and would have been the simple substitution of one existing component (*e.g.*, controller) for another (*e.g.*, vehicle interface module) to perform the same functionality. (*Id.*) This substitution would have had predictable results: the system would determine whether the driver has violated her profile regardless of which component is used. (*Id.*)

Moreover, Murphy suggests the modification. (*Id.*) It uses its “input terminals” to monitor “components... whose activation may indicate that someone is preparing to drive the vehicle,” and if it determines such components have been activated, it provides this feedback to the controller, so the controller can “activate

a driver interrogation sequence.” (Murphy, 14:7-17, Fig. 6, Abstract, Fig. 3, 7:49-63.) Moreover, the “various limitations on vehicle operation” drivers can be stored in different modules. (Ehsani, ¶¶74-77.) Thus, a POSITA would have understood the vehicle interface module could similarly store or access such limitations and use them to determine whether a violation has occurred and provide such feedback to the controller. (*Id.*)

A POSITA would have been motivated to modify Murphy to configure the vehicle interface module to determine whether the driver has violated her profile and provide this information (*e.g.*, signals) to the controller. (*Id.*) The vehicle interface module is already connected via its “terminals” to components, such as the engine, transmission, fuel supply, power supply, and accessories, “for use in controlling or restricting” operation. (Murphy, 13:65-14:22.) Thus, by configuring the vehicle interface module to determine whether the driver is violating her profile, this could reduce the amount of information provided to the controller, as the vehicle interface module could provide information (*e.g.*, signals) about violations only when it determines one will occur. (Ehsani, ¶¶74-77.)

b) Claim 11

Murphy renders obvious Claim 11. (Ehsani, ¶¶78-94.)

11[pre]: A driver authentication and monitoring system, comprising:

If limiting, Murphy discloses Claim 11[pre]. (Ehsani, ¶79.) *See supra* Claim

1[pre].

11[A]: a master control unit in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver;

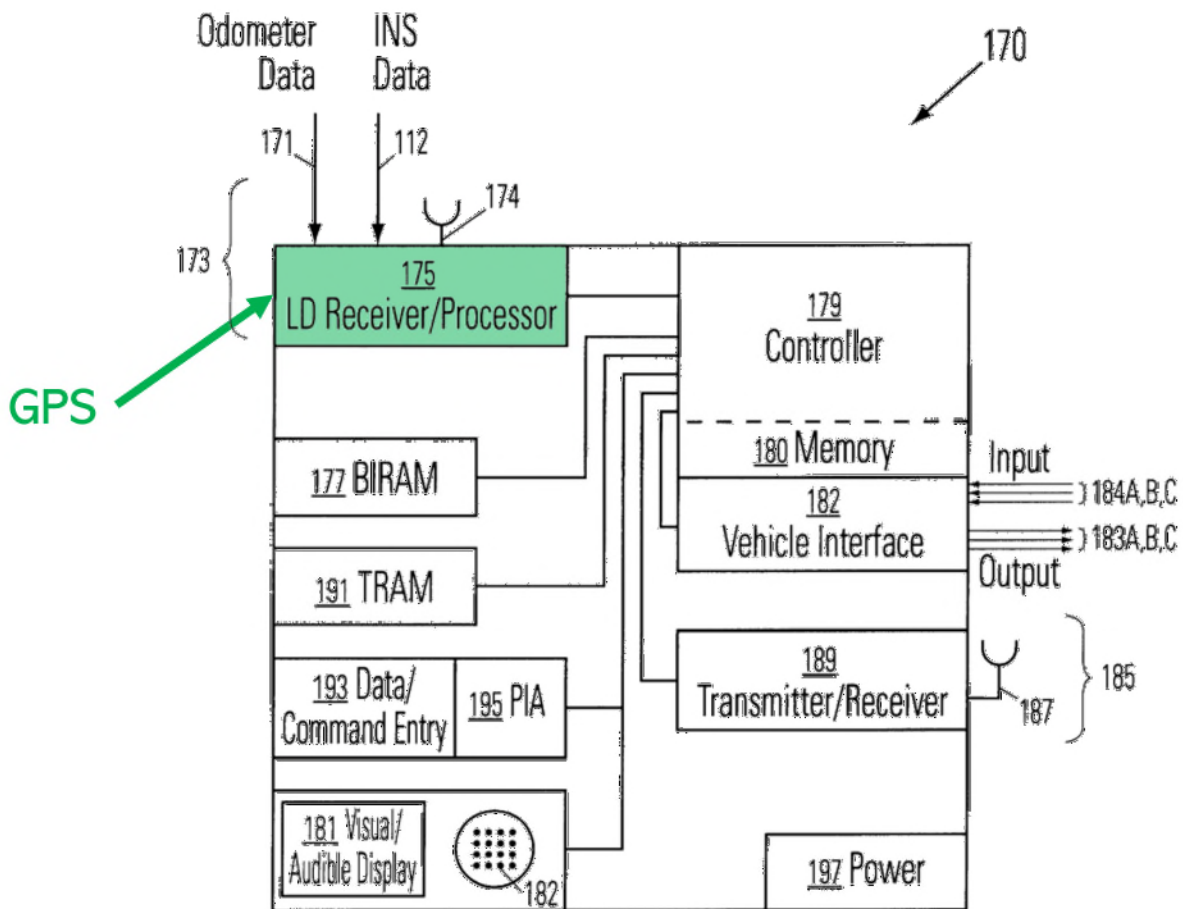
Murphy discloses Claim 11[A]. (Ehsani, ¶¶80-83.)

Murphy discloses a “master control unit” (*e.g.*, controller) for “authenticating at least one driver via [a] driver identification [interface].” *See supra* Claim 1[A]. Moreover, the controller “associate[s]” an “operating profile with the at least one driver.” *See supra* Claim 1[B].

11[B]: a GPS module providing at least location and speed information in association with movement of the motor vehicle;

Murphy discloses Claim 11[B]. (Ehsani, ¶¶84-85.)

Murphy includes a “location determination (LD) module” that “*determines the present location, present speed... of the vehicle...*” (Murphy, 3:48-64.) This information is “sent by the LD module 173 to the controller” for use in determining whether to take control actions:



(*Id.*, Fig. 6 (annotated), 13:28-65; *see also* Abstract, 14:23-45, Fig. 7, 15:32-54, 3:64-4:38, Fig. 5, 13:11-26, Cls. 1, 10, Fig. 2, 7:49-9:44.)

11[C]: a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module;

Murphy discloses Claim 11[C]. (Ehsani, ¶¶86-89.)

Murphy includes “an *operations log, including periodic recording of the present observation time, vehicle location and/or vehicle speed in a memory...*”

(Murphy, 12:1-5, Fig. 6, 13:53-15:65, 14:18-22.) This log allows location and speed

from the LD module to be stored for “subsequent review and analysis” (including when the driver violates her profile) and “copied from or removed from the system for subsequent analysis or storage.” (*Id.*, 15:42-54, Fig. 7, 5:52-54; *see also* 15:66-16:11.) Further, GPS “vehicle location and selected status parameters” can be stored in a remote “base station” for use in determining whether to take actions remotely (such as modifying or adding new restrictions). (*Id.*, 4:15-27, 1:66-2:24, 16:30-49.)

11[D]: *[i] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, [ii] said slave control unit in communication with said master control unit and...*

Murphy discloses Claim 11[D]. (Ehsani, ¶90.) *See supra* Claim 1[C].

11[E]: *[said slave control unit...] [i] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile thereby providing feedback to the master control unit about usage of the vehicle, and [ii] wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit;*

Murphy renders obvious Claim 11[E]. (Ehsani, ¶91.) *See supra* Claim 1[D].

11[F]: *wherein the master control unit permits the at least one driver to operate the vehicle within an operating profile if the master control unit receives at least one of a unique identification code to permit the at least one driver to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.*

Murphy discloses Claim 11[F]. (Ehsani, ¶¶92-94.)

Murphy’s system (*e.g.*, controller) “permits the at least one driver to operate the vehicle within an operating profile” after it receives a “unique identification

code.” *See supra* Claims 1[A]-1[B]. Moreover, once a driver is authenticated, the controller and system allows her to use the vehicle within her profile, unless restrictions therein are violated. *Id.* For example, if the driver violates her profile, or is “found to be unauthorized,” the system (*e.g.*, the controller with the vehicle interface module) can “disable[] the vehicle... through fuel cutoff, brake disablement or some other similar measure.” (Murphy, 5:17-67, 10:29-44, Abstract.) *See supra* Claim 1[D].

c) Claim 15

Murphy anticipates and renders obvious Claim 15. (Ehsani, ¶¶95-113.)

15[pre]: *A method of authenticating and monitoring drivers, comprising:*

If limiting, Murphy discloses Claim 15[pre]. (Ehsani, ¶96.) *See supra* Claim 1[pre].

15[A]: *providing a motor vehicle with a driver authentication and monitoring system;*

Murphy discloses a driver authentication and monitoring system in a vehicle. (Ehsani, ¶97.) *See supra* Claims 1[pre]-1[A].

15[B]: *programming the driver authentication and monitoring system with an operating profile associated with a high risk driver;*

Murphy discloses Claim 15[B]. (Ehsani, ¶¶98-101.)

Murphy includes operating profiles associated with high-risk drivers,

including restricted operators.¹⁰ *See* Ground 1, Claim 1[B]. For example, the system can “monitor operation of the vehicle by a teenager or other inexperienced driver, with restrictions imposed upon vehicle operation channel, total vehicle mileage, vehicle maximum speed and/or time interval of operation of the vehicle.” (Murphy, 11:60-67; *see also* 1:9-27, 1:66-2:16, 3:21-47, 16:49-17:62.)

Further, these profiles can be “programmed” into the system. (*Id.*, 15:66-16:11; *see also* Fig. 7, 5:52-54, Fig. 6, 13:35-41, 14:51-65.) *See also supra* Claim 11[C].¹¹ The profiles can be programmed into the system by: (1) an “authorized system administrator” who “modif[ies]” the “operating restriction tables” using a data entry device (Murphy, 7:40-48, 12:16-27, 13:44-52, Fig. 6); (2) presentation of a “token” with “pre-programmed information” on “restrictions” (*id.*, 6:55-7:14, 2:33-34, 14:46-54, Cl. 38); and (3) receipt of a “reprogramming signal” that “commands” the system to “modify, add, or delete vehicle operation restrictions” (*id.* 14:23-45, Abstract, 2:6-9). *See infra* Claims 2-3.

¹⁰ “Restricted operators” include “very young drivers” and “very old drivers.” (Murphy, 17:3-13, 3:20-47, 11:60-67.)

¹¹ Such data may also be stored in other associated modules, such as “the schedule module 211 and/or the vehicle activity log module 217.” (Murphy, 15:55-16:11.)

15[C]: authenticating the high risk driver and enable operation of the motor vehicle within limits of the operating profile by monitoring operation of the motor vehicle to determine if the high profile driver is violating the operating profile;

Murphy discloses and renders obvious Claim 15[C]. (Ehsani, ¶¶102-04.)

Murphy authenticates high-risk or high profile drivers and enables their operation of a vehicle within their respective profiles. (Ehsani, ¶103.) *See supra* Claim 1[A]-1[B]; *see also* Claim 15[B].

Further, Murphy monitors operation to determine if the driver violates her profile.¹² For example, Murphy’s controller will monitor “[i]nformation on the present vehicle location and/or vehicle speed and/or time and/or accumulated operating time and/or accumulated mileage” and “*compar[e] this... with* any vehicle operation *restrictions that may be imposed*” to determine if the driver is violating her profile. (Murphy, 13:53-61; *see also* 13:28-43, 14:18-22, Figs. 6-7, 15:9-16:11, 16:50-17:63, Cls. 1, 10, Abstract, 1:66-2:6, 2:20-53, Fig. 2, 7:49-9:44, Fig. 3, 10:45-11:27.) *See infra* Claim 15[D].

¹² Murphy also renders obvious “monitoring” vehicle operation to determine profile violations. *See supra* Claim 1[D].

15[D]: generating a signal if said high profile driver violates the operating profile while operating the motor vehicle; and

Murphy discloses Claim 15[D]. (Ehsani, ¶¶105-7.)

Murphy generates “signals” if the driver violates her operating profile.¹³ For example, if the controller determines the driver has violated her profile (*see supra* Claim 15[C]), it determines which “Control Action(s), if any, should be imposed on vehicle use and communicates this information” to the vehicle interface module for “implementation” via an “appropriate system.” (*Id.*, 15:36-54, 13:66-14:17, Figs. 6-7, 16:12-49.) Thus, the controller generates a signal to the vehicle interface module, which, in turn, generates a signal to the appropriate component. (*Id.*; *see also* Ehsani, ¶¶106-7.) The “Control Action(s)” include “an on-board alarm” signal and a “coded alarm signal” transmitted to “a selected facility.” (Murphy, 5:13-54, Abstract, 17:30-63.) *See infra* Claim 15[E]. Further, if there is a violation the controller can send signals to a “display [or feedback] module” and to the “operations [or vehicle activity] log,” causing, respectively, the display module to announce that a violation occurred and the operations log to record such violation. (Murphy, 5:29-60, 12:1-15, 15:42-54, 13:61-65, 10:29-40, Figs. 6-7.)

¹³ Murphy also renders obvious generating “signals” if the driver violates her profile. *See supra* Claim 1[D].

15[E]: governing mechanical operations of the vehicle remotely if the high profile driver violates the operating profile.

Murphy discloses Claim 15[E]. (Ehsani, ¶¶108-10.)

Murphy includes “an antenna 187 and associated receiver/transmitter [] that exchanges information signals with an information processing facility.” (Murphy, 14:23-45.) If the driver violates her profile, the system may “transmit[] an alarm... to a selected facility that is *spaced apart from the vehicle*.” (*Id.*, 5:13-54; *see also* 17:30-63, 6:1-18.) The remote facility can, in turn, send “commands” back to the system to “alter restrictions” of the driver’s profile. (*Id.*, 14:23-45, Cl. 1; *see also* Abstract, 2:6-9, 12:16-27, 17:30-63.) The system then cooperates with the remote facility to govern vehicle operation, such as by using new or modified driving restrictions received from the facility to control the driver’s vehicle usage. (*Id.*, 14:23-45; *see also* Cls. 7, 9, 12, 15, 18, Abstract, 12:16-27, 4:15-27; Ehsani, ¶¶108-10.) *See infra* Claims 2-3.

2. Dependent Claims

a) Claim 2

Murphy renders obvious Claim 2. (Ehsani, ¶¶111-16.)

Murphy includes a “database comprising a program module,”¹⁴ such as a “*database*” with “limitations on vehicle operation” (*e.g.*, operating parameters), including on “geographic regions,” “time intervals,” and “speed ranges.” (Murphy, 15:9-31.) “For each authorized driver whose name or other identifying characteristics are... in the database” information may be stored regarding: “(1) name or other identifier; (2) corresponding ident indicium...; (3) schedule applicable to driver; (4) actual range of vehicle locations; (5) actual range of vehicle speed; (6) actual times of vehicle operation; (7) present ‘state’ of the vehicle...; and (8) corresponding Control Actions applicable to various circumstances.” (*Id.*, 15:66-16:11; *see also* 5:12-6:17.) *See supra* Claim 1[D]. This “database” can be stored in the in-vehicle system, *e.g.*, in the memory of the controller or another module. (Murphy, 16:9-11; *see also* 13:35-41, 14:51-65, Fig. 7, 15:55-15:65, Figs. 6-7.)

Murphy’s database can be “programmed” remotely by an “authorized monitoring agency or person.” (*Id.*, 2:6-9, 7:40-48.) Specifically, Murphy “allows downloading from a *remote facility to modify or add* to the extant *parameters* for vehicle operation or for vehicle driver identification, where the parameters are

¹⁴ The ‘427 broadly describes “program modules” as including “routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types.” (‘427, 4:55-58.)

included in the operating code, stored data and the like.” (*Id.*, 14:40-45.) To do so, the system includes “telecommunication module 185... that exchanges information signals with an information processing facility... that is spaced apart” from the system. (*Id.*, 14:23-27, Fig. 6.) Murphy adds that using “[s]uitable telecommunication systems” (*e.g.*, networks), the remote facility can transmit “change or reprogramming signal[s]” that “modify, add or delete vehicle operation restrictions, for receipt by the apparatus [], and that allow downloading of commands that alter restrictions on present location, speed and/or present time, accumulated operating time and accumulated mileage items that determine the conditions under which a vehicle operation restriction is imposed.” (*Id.*, 14:27-40, Abstract; *see also* 12:16-27, Fig. 1, 16:12-17:63, 4:15-27, Cls. 7, 9, 12, 15, 18.) *See supra* Claim 15[B].

b) Claim 3

Murphy renders obvious Claim 3. (Ehsani, ¶¶117-26.)

Murphy allows for “*downloading from a remote facility* to modify or add to the extant *parameters for vehicle operation* or for vehicle *driver identification*.” (Murphy, 14:23-45; *see also* Fig. 6, 2:6-9; 7:40-48, Abstract, 12:16-27, Fig. 1, 16:12-17:63, 4:15-27, Cls. 7, 9, 12, 15, 18.) Thus, Murphy’s “driver identification interfaces” (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA) work with its “remote computer” (*e.g.*, remote facility) to “load” a driver’s profile into the controller.

First, the “remote facility” can transmit new “parameters for... *driver identification*” to the in-vehicle system, which the driver can use with the identification interface to authenticate herself and “load” her profile in the controller. (*Id.*, 13:28-15:54, Figs. 2, 6-7; *see also* Abstract, 7:40-8:53, 4:39-5:12, 6:55-7:14.) For example, if the system downloads a new “biometric indicium” like a new “facial image,” or a new “coded sequence of characters” for use with the data entry module, then the driver can enter these new parameters to authenticate herself using the system’s BIRAM and data entry module, respectively. (Ehsani, ¶¶118-22.) *See supra* Claim 1[A]. The driver’s profile is then loaded into the “controller” (*e.g.*, master control unit) once the driver is authenticated, and the driver is required to operate her vehicle in accordance with the loaded profile. (Murphy, 13:35-41, 14:51-65, 15:15-21, 15:66-16:11, 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62, Figs. 6-7.) Therefore, Murphy’s driver identification interfaces work in conjunction with the remote computer to load the driver’s “operating profile” in the controller. (Ehsani, ¶¶118-22.) *See also supra* Claim 1[B].

Second, the “remote facility” can “*transmit signals* that modify, add or delete vehicle operation restrictions, for receipt by the [in-vehicle system], and that allow downloading of commands *that alter restrictions* on present location, speed and/or present time, accumulated operating time and accumulated mileage items *that determine the conditions under which a vehicle operation restriction is imposed.*”

(Murphy, 14:27-37.) Once “download[ed]” to Murphy’s system, these “alter[ed] restrictions” would be stored in the profiles of the drivers whose restrictions are being altered. (*Id.*, 15:66-16:11, 13:28-15:65, 16:50-17:62, Figs. 6-7; Ehsani, ¶¶123-26.) *See supra* Claim 1[B]. In conjunction with this, when a driver whose restrictions were altered authenticates herself using an “identification interface,” the controller (*e.g.*, master control unit) will use the “operating profile” with the “alter[ed] restrictions” that were “download[ed]” from the “remote facility.” (Murphy, 15:66-16:11, 13:28-15:65, 16:50-17:62, Figs. 6-7; Ehsani, ¶¶123-26.) Thus, in this way, too, Murphy’s driver identification interfaces work in conjunction with the remote computer to load the driver’s “operating profile” to the controller. (*Id.*)

c) Claim 4

Murphy renders obvious Claim 4. (Ehsani, ¶¶127-36.)

First, Murphy includes a “GPS module.” *See supra* Claim 11[B].

Second, Murphy includes a “memory module,” as it includes “controller 179 and *associated memory module 180*.” (Murphy, 13:35-41, 15:15-21, Figs. 6-7.) This memory and Murphy’s system include a “*database* of authorized vehicle operators.” (*Id.*, 15:15-21, 13:35-41, 14:51-65; *see also* 15:66-16:11, 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.) Murphy also includes “schedule module 211” (*e.g.*, memory) containing “limitations on vehicle operation and each authorized operator...” (*Id.*, 15:21-31, Fig. 7.) Murphy includes other memories as well, such

as in its token and operations log. (*Id.*, 6:55-7:14, 12:1-5; *see also* 16:30-49.)

Third, Murphy includes numerous “function indicator modules.”¹⁵ Murphy’s system, *e.g.*, its controller, can monitor functioning of the LD module, determine “if sufficient LD signals of acceptable quality are being received,” and, if not, take “Control Actions.” (*Id.*, 13:11-26, Fig. 5; *see also* 3:64-4:14, Fig. 6, 13:28-52.) Similarly, the system can include an “inertial navigation system [INS] device... or similar *location indicating device*” that monitors whether “LD information is lost or corrupted,” and, if so, can use its own “INS information” to “estimate the present location and/or speed and/or accumulated mileage.” (*Id.*, 4:28-38, 13:28-52.)

As further examples of “function indicator modules,” Murphy includes: (1) a “vehicle interface module” with “input terminals” monitoring the functioning of certain “components (doors, ignition, alarm system, vehicle cargo, accessories, etc.)” (*id.*, 13:66-14:17, Figs. 6-7, 15:37-54; *see also* Abstract, 13:28-15:8, Fig. 2, 7:49-63); (2) a “display system” monitoring vehicle operation and alerting the driver

¹⁵ The ’427 broadly describes “function indicator module” as a module that monitors “various functions in association with the vehicle... such [sic] for example, power, fault detection and monitoring, and other functions.” (’427, 8:11-14.) Moreover, the ’427 broadly describes “module” as a “physical hardware component and/or a software module.” (*Id.*, 8:4-16.)

“a violation has occurred and/or that the vehicle will become disabled” if action is not taken (*id.*, 10:29-40, 5:29-60; *see also* 12:6-15, 13:61-65, 15:47-50, Figs. 6-7); (3) a “vehicle odometer... or similar *distance indicating device*” supplementing LD or GPS information (*id.*, 13:44-48); (4) a BIRAM monitoring uses of “biometric indicium” that are not “legible/interrogatable,” so the system can take “control actions” after a “sequence of N consecutive” failed attempts (*id.*, 5:13-16, 6:19-39); and (5) a “governor” that monitors “vehicle speed” to “reduce[] the vehicle speed to a selected speed range” (*id.*, 5:29-60, 6:8-17, 17:30-63).

d) Claim 5

Murphy renders obvious Claim 5. (Ehsani, ¶¶137-40.)

In Murphy, drivers have different “operating profiles” loaded into the system’s “database” or “memory.” *See supra* Claim 1[B]. The memory the profiles are loaded into can be the memory (*e.g.*, memory module) of the controller. (Murphy, 13:35-41, 14:51-65, 15:15-21, 15:66-16:11, Figs. 6-7; *see also* 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.)¹⁶ Once a driver authenticates herself, her profile loaded in the memory is used to control vehicle operation. *See supra* Claim 1[B].

¹⁶ “Operating profiles” can also be loaded into the system from the token. (Murphy, 6:55-7:14, 14:46-54, Abstract, 2:33-35, Cl. 20; Ehsani, ¶¶137-40.)

In addition, Murphy can include a “schedule module 211” (*e.g.*, memory) with “limitations on vehicle operation for each authorized vehicle operator.” (Murphy, 15:9-54, 16:30-49, Fig. 7.) This information, along with “ident information” of “authorized drivers,” can be loaded into the “controller” (with its “memory unit”) to enable it to authenticate the driver and “determine[] which Control Action(s), if any, should be imposed on vehicle use.” (*Id.*)

e) Claim 6

Murphy renders obvious Claim 6. (Ehsani, ¶¶141-42.) *See supra* Claim 11[B].

f) Claims 8/13

Murphy renders obvious Claims 8/13. (Ehsani, ¶¶143-44.)

Murphy’s operating profiles include “*parameters for vehicle operation*, including restrictions on (a) “selected maximum speed” (*i.e.*, maximum allowable vehicle speed), (b) “selected geographic region” and “specific routes” (*i.e.*, allowable vehicle locations), and (c) “one or more selected time intervals during the day, or to selected days of the week” (*i.e.*, allowable hours of operation). (Murphy, 17:14-28, 14:40-45; *see also* Abstract, 5:12-54, 11:60-67, 2:46-53, 6:8-17, Fig. 2, 8:5-67, 12:16-35, 15:66-16:11.) *See supra* Claim 1[B].

g) Claims 9/14

Murphy renders obvious Claims 9 and 14. (Ehsani, ¶¶145-49.)

Murphy monitors whether a driver is operating the vehicle in accordance with

her profile, and, if she violates her profile, takes “control actions,” including generating “alarm signals.” *See supra* Claim 1[D]. For example, if the system determines the “present time” outside the driver’s “permitted time intervals” or “vehicle present location and/or speed” is not within the “permitted travel region or speed range,” it can (a) “**audibly announce[] or visually display[]** an announcement that a **violation has occurred...**” (*e.g.*, alert the driver); (b) “**transmit[] a selected alarm signal to a selected facility** that is spaced apart from the vehicle” (*e.g.*, alert authorized personnel at the remote facility); and (c) “activate[] an on-board alarm the [sic] is visually or audibly perceptible **to a person outside the vehicle**” (that is, alert others). (Murphy, 5:13-60, Cl. 1; *see also* Abstract, 17:30-63, Cl. 20, 2:6-9, 4:15-27, 12:8-12, Fig. 6, 13:60-65, 14:23-45, Fig. 7, 15:37-50, 16:11-49.)

It would have been obvious to a POSITA to modify Murphy to have the vehicle interface module (instead of the controller module) generate the “alarm signals” for the reasons above. *See supra* Claim 1[D]. (Ehsani, ¶¶145-49.) For example, a POSITA would have understood that, after determining there is a violation, the vehicle interface module could generate an “alarm signal”¹⁷ causing

¹⁷ The ’427 broadly describes the “alarm signal” as a signal that “**can result** in an actual audible alarm, or it can be used to control/govern operational aspects of the vehicle.” (’427, 7:21-29.)

the controller to issue an alarm that a violation has occurred, to transmit the alarm signal to authorized persons at the remote facility, or both. (Ehsani, ¶¶145-49.) Such would have been a simple substitution of one similar component for another. (*Id.*)

Moreover, Murphy suggests the modification, as its vehicle interface module already monitors vehicle operation and provides alerts (*e.g.*, if certain components are activated it can cause the system to alert the driver with a “driver interrogation sequence”), and a POSITA would have understood that the vehicle interface module could generate additional alerts based on the detection of conditions, *e.g.*, if the driver violates her profile. (*Id.*)

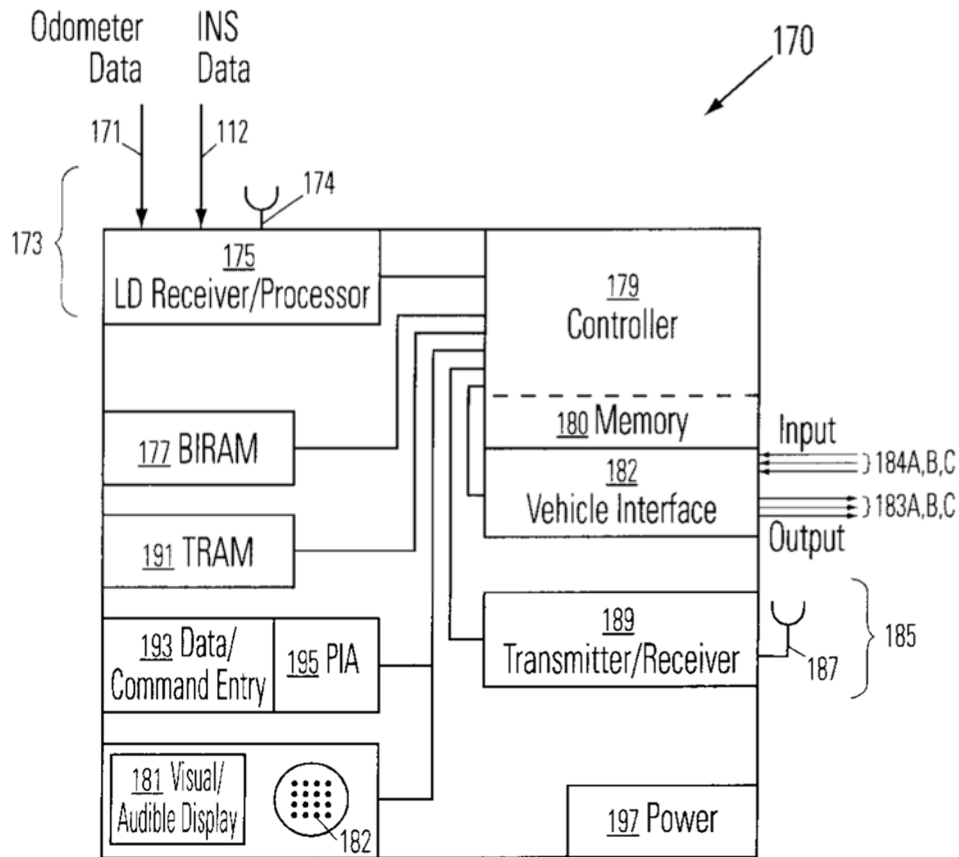
h) Claim 10

Murphy renders obvious Claim 10. (Ehsani, ¶¶150-54.)

Murphy’s driver identification interface can include a “token or *smart card*.” (referred to collectively as a ‘token’).” *See supra* Claim 1[A]. The token may be “specific for the *person* who *presents*” it, have “*built into it a circuit* or pre-programmed information in a storage medium that imposes selected restrictions on operation of the vehicle and/or that identifies the token holder,” and rely “upon digitized data stored in a flash *memory*, in a (re)programmable ROM or in similar information storage media.” (Murphy, 6:55-7:14; *see also* 2:33-34, 14:46-65, Cl. 38.) Further, the TRAM allows for “insertion *or* presentation” of the token. (*Id.*) Thus, the token is both a “portable handheld device” and a “radio frequency

identification device.” (Ehsani, ¶¶150-54.)

Murphy also discloses that its entire in-vehicle system, including the driver interface(s), can be a “portable handheld device.” Specifically, Murphy’s “apparatus 170”—including the “driver identification interfaces”—can be “a *stand-alone device* that communicates directly” with vehicle accessories:



(Murphy, 15:1-8, Fig. 6.)

i) Claim 16

Murphy anticipates or renders obvious Claim 16. (Ehsani, ¶¶155-56.) See

supra Claim 11[B].

j) Claims 17/18

Murphy anticipates or renders obvious Claims 17/18. (Ehsani, ¶¶157-58.)

Murphy discloses generating an audible alarm to the driver via the “display [or feedback] module” and an alarm signal remotely to an authorized user at a “remote facility” via the “telecommunication module.” *See supra* Claims 9/14.

k) Claims 19/20

Murphy anticipates or renders obvious Claims 19/20. (Ehsani, ¶¶159-160.)

Murphy takes “Control Action(s)” in response to profile violations. *See supra* Claim 15[D]; *see also* Claims 1[D], 9/14. For example, the “controller” generates a signal (*e.g.*, alarm signal) to the vehicle interface module to alert it that the profile was violated and instruct it to take a “Control Action.” (Murphy, 15:36-54; *see also* 13:66-14:17, Figs. 6-7.) The vehicle interface module, in turn, generates a control signal to limit vehicle functionality, such as “disabl[ing] the vehicle” or “selected vehicle accessories.” (*Id.*, 5:13-54, 17:30-63.)

B. Ground 2 – Murphy-Adams Renders Obvious Claim 10

Adams, filed August 16, 2006, and published February 21, 2008, is prior art under pre-AIA §102(e). Adams discloses a “smart card” and “smart card reader” and that “smart cards” can be “contactless” and “communicate with their smart card readers” wirelessly using “*radio frequency identification (RFID)*.” (Adams, [0001],

[0022], [0027].)

It would have been obvious to a POSITA to apply this to Murphy to have its token be a “radio frequency identification device.” (Ehsani, ¶¶161-66.) Such would have been the simple combination of well-known prior art elements according to known methods to yield predictable results. (*Id.*) Both Murphy and Adams teach that smart cards were known and can communicate with an interface wirelessly. (Adams, [0001], [0022]-[0030]; Murphy, 6:55-59, Abstract, 14:46-54.) Adams simply adds an express recitation that this can be RFID. (Adams, [0027].)

Applying this to Murphy, Murphy would operate in the same fashion—authenticating drivers as it did before—only now its token would use the well-known RFID protocol to communicate with the TRAM. (Ehsani, ¶¶161-66.) A POSITA would have been motivated to use RFID in Murphy’s token as such would have provided an established protocol to enable wireless communications between the token and TRAM, without the need for a driver to insert her token. (*Id.*)

C. Ground 3 – Murphy-Wu Renders Obvious Claims 7/12

Wu, filed November 15, 2006, and published February 21, 2008, is prior art under pre-AIA §§102(a), (e). Wu discloses a vehicle control system having “a controller 20, a battery 40... an engine control module 60... a starter motor 80, a fuel pump 90, and an ignition circuit 100.” (Wu, [0020]-[0022], [0025]-[0027], Figs. 1-2.) Wu’s controller controls operations such as “starting” the vehicle and

(de)activating the ignition, as well as “accessories” like lights. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039].) These operations are done using a processor in the controller to send signals to “relays,” which (de)activate the components. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.)

Murphy in view of Wu renders obvious Claims 7/12. (Ehsani, ¶¶167-77.) Claims 7/12 merely add that the “slave control unit” includes certain well-known components—namely “a power regulator module; a starter relay module; a definable relay module; a slave microcontroller; and an alarm synthesizer.” Relatedly, the ’427 broadly describes the “slave control unit” as a collection of components across the vehicle that are connected and, *e.g.*, respond to commands, such as from the “master control unit.” (’427, Fig. 6, Abstract, 8:15-55; Ehsani, ¶¶170-71.)

Murphy discloses and renders obvious its slave control unit including a “slave microcontroller.” (Ehsani, ¶171.) For example, the vehicle interface module includes a “*microcomputer*” and “output terminals” connecting to the “microcomputers” of the components it controls. (Murphy, Fig. 6, 13:53-14:17, Fig. 7, 15:32-16:49.) Because these “microcomputers” are part of or connected to and take the actions instructed by the vehicle interface module, they are “slave microcontrollers.” (Ehsani, ¶171.)

Murphy discloses and renders obvious its slave control unit including an “alarm synthesizer.” (*Id.*, ¶172.) Murphy includes a “*loudspeaker* 182.” (Murphy,

Fig. 6, 12:8-12, Fig. 7, 15:37-50.) When the system (*e.g.*, interface module) determines a violation has occurred, it can cause the speaker to synthesize an “audibly perceptible presentation.” (*Id.*, 15:47-50, 5:13-60; *see also* Cl. 1, 17:30-63, 13:60-65; Ehsani, ¶172.) *See supra* Ground 1, Claims 9/14. Moreover, a POSITA would have understood the “output terminals” of the vehicle interface module, which are used to control myriad components, could likewise be connected to the “alarm synthesizer.” (Ehsani, ¶172.) Similarly, Wu discloses a synthesizer, including an “operational amplifier” and “resistor,” that can generate such audible alerts, and a POSITA would have understood this to be a common way to implement the alerts in Murphy. (Wu, [0030]; Ehsani, ¶172.)

Murphy in view Wu discloses and renders obvious its slave control unit including a “power regulator module.” (Ehsani, ¶¶173-75.) Murphy’s vehicle interface module is connected to a “power supply” and regulates power to components. (Murphy, 13:66-14:4, 14:66-15:8; Ehsani, ¶¶173-75.) Moreover, Wu discloses it was “standard” to include a power (or voltage) regulating device in modules, like Murphy’s, to regulate voltage to levels the system “requires.” (Wu, [0020], [0022], [0027]-[0028].) It would have been thus obvious to a POSITA to include a voltage regulator with the vehicle interface module, as this would merely be the use of a well-known component to perform its intended function. (Ehsani, ¶¶173-75.)

Murphy in view of Wu discloses and renders obvious its slave control unit including a “starter relay module.” (Ehsani, ¶176.) Murphy includes an “ignition circuit,” and if a driver is authenticated, the system can “enabl[e]” this “ignition circuit,” allowing the engine to be started. (Murphy, Abstract, 6:55-59, 8:10-14.) Wu discloses that when its controller receives a command to start the vehicle, its processor sends a signal to initiate a “starter relay,” which will engage a starter motor and cause the engine to start. (*Id.*, [0020]-[0021], [0025]-[0027], [0030]-[0031], [0039], Figs. 1-2.) A POSITA would have been motivated to include a “starter relay” as taught by Wu in Murphy to provide a well-known and commonly used mechanism for starting the engine. (Ehsani, ¶176.) Moreover, a POSITA would have understood the “output terminals” of the vehicle interface module, which are used to control myriad components, could be connected to the ignition circuit and starter relay and used to allow the vehicle to start, *e.g.*, if the driver is authenticated. (*Id.*)

Murphy in view of Wu discloses and renders obvious its slave control unit including a “definable relay module.” (Ehsani, ¶177.) Murphy’s vehicle interface module includes “output terminals” connected to other components that cause the activation of defined circuitry or functionality such as “turn[ing] on at least one of the lights, exterior flashers or horn.” (Murphy, 5:29-60, *see also* 13:66-14:17; Ehsani, ¶177.) In addition, Wu discloses that components such as the ignition system, lights, and accessories can be controlled by a processor sending a signal to

a “defined relay” for such components. (Wu, 0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.) A POSITA would have been motivated to use such definable “relays” in Murphy, as such would have merely been the implementation of known components for their intended purpose and would have allowed Murphy’s vehicle interface module to selectively (de)activate the ignition, lights, fuel injector, and other accessories. (Ehsani, ¶177.)

D. Ground 4 – Arshad Renders Obvious Claims 1, 4-6, and 10

Arshad renders obvious Claims 1, 4-6, and 10. (Ehsani, ¶¶178-215.) Arshad published October 9, 2003, and is prior art under pre-AIA §102(b).

1. Independent Claims

a) Claim 1

Arshad renders obvious Claim 1. (Ehsani, ¶¶181-202.)

1[pre]: A driver authentication and monitoring system, comprising:

To the extent limiting, Arshad discloses Claim 1[pre]. (Ehsani, ¶182.)

Arshad controls “access” to “[f]leet vehicles.” (Arshad, Abstract, [0005], [0008]-[0009], [0033].) In Arshad, a driver’s “transponder 20” transmits data to an in-vehicle control system to “uniquely *identify* the person carrying the transponder.” (*Id.*, [0033], [0019], [0012], Cl. 7.) After the driver is authenticated, “*monitoring* controller 38” monitors vehicle operation, “determines whether the operator is authorized” to take certain actions, and responds to unauthorized actions with “alert

(*Id.*, Figs. 1, 3 (annotated); [0020], [0024]-[0025], [0030]-[0033].) Transponder 20 communicates with antenna 58 of reader circuit 14 via “radio frequency” signals. (*Id.*, [0020]-[0025], [0029]-[0040].) Each transponder’s memory stores an “identification number” to “uniquely identify the person carrying” it. (*Id.*, [0033].)

To authenticate drivers, controller 38 issues “commands... to the control module” of reader circuit 14, including “to query for any transponder in range, and... to query for a specific transponder by its embedded identification number.” (*Id.*, [0031].) When a general query is issued, nearby transponders send “a response that includes their identification number.” (*Id.*, [0033].) Reader circuit 14 will then “single out and *identify* any transponder within range,” and the controller and reader circuit can communicate with identified transponders by sending “specific queries” including particular identification numbers, and any nearby transponder “internally checks to see if it has the identification number broadcast.” (*Id.*, [0032]-[0033].) If it does, it “responds with an affirmative message, and thereby establishes a communication session with controller 38.” (*Id.*)

Once reader circuit 14 “establishes the existence of a particular transponder” (*e.g.*, by authenticating through identification numbers), it communicates with the transponder to “download information” from the transponder’s memory “and thence to controller 38 for processing.” (*Id.*, [0033]-[0034].) *See infra* Claim 1[B].

1[B]: wherein the master control unit receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver and accessible by the master control unit;

Arshad discloses Claim 1[B]. (Ehsani, ¶¶187-90.)

In Arshad, drivers have different operating profiles, as each driver may have a “*different* degree[] of vehicle access.” (*Id.*, [0008]-[0012], [0020].) A driver’s transponder stores “*operational limits*,” such as “maximum speed,” “maximum load on the engine,” “total distance” of authorized travel, “geographical area” where the vehicle can operate, “allowed times and dates of operation,” “total time” of allowed operation, or “subsystems” the operator can use. (*Id.*, [0043]-[0044], [0057], [0026], [0074].) This operating profile, *i.e.*, degrees of access and operational limits, can be “downloaded” from the transponder to controller 38, which accesses the operating profile to determine whether the driver is “authorized” to use the vehicle or subsystem or is approaching or exceeding a limit. (*Id.*, [0031], [0034], [0043]-[0044], [0057], [0071]; *see also* [0011], [0019], [0040], [0059]-[0060], [0068], [0073]-[0074].)

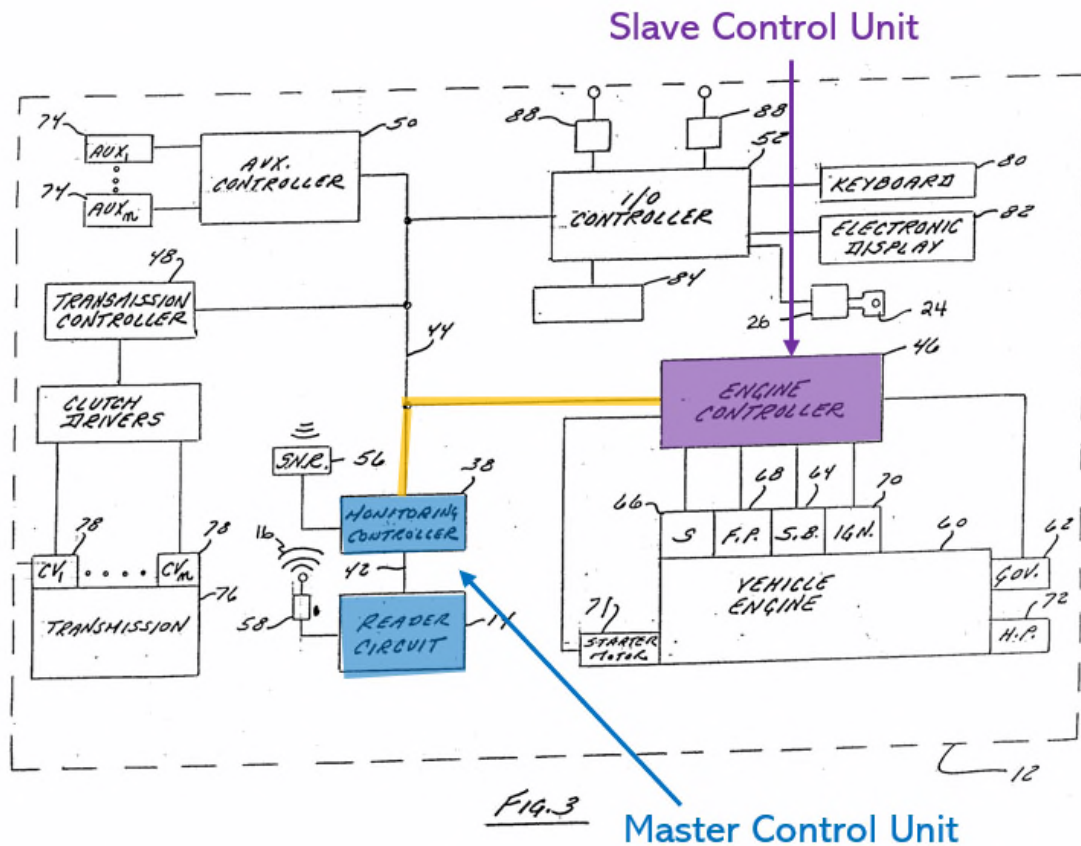
Further, controller 38 and reader circuit 14 receive a “unique identification code” that permits the driver to operate the vehicle within her profile. Each transponder stores an “*identification number*” to “*uniquely identify*” the driver carrying it, which is sent to reader circuit 14 to authenticate and establish communication sessions with particular transponders. (*Id.*, [0032]-[0034].)

Once a driver is authenticated using the transponder identification number, *see supra* Claim 1[A], controller 38 accesses the operational limits profile to permit vehicle operation within these limits. Specifically, controller 38 will not allow the vehicle to operate “until [it] has received the data stored in transponder 20 and determined whether the operator is authorized to operate specific vehicle systems.” (Arshad, [0040]; *see also* [0034].) Further, controller 38 “compares” data from other controllers and sensors with “data it received from the transponder” to determine whether the driver has “attempted to exceed any of the operational limits that were indicated by the transponder data.” (*Id.*, [0043]-[0045], [0040]-[0042], [0057]-[0063], [0071]-[0074].) If limits are exceeded, controller 38 takes appropriate actions such as shutting down or limiting vehicle subsystems or displaying a message indicating what limit has been exceeded. (*Id.*) *See supra* Claim 1[A].

1[C]: [i] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, [ii] said slave control unit in communication with said master control unit and...

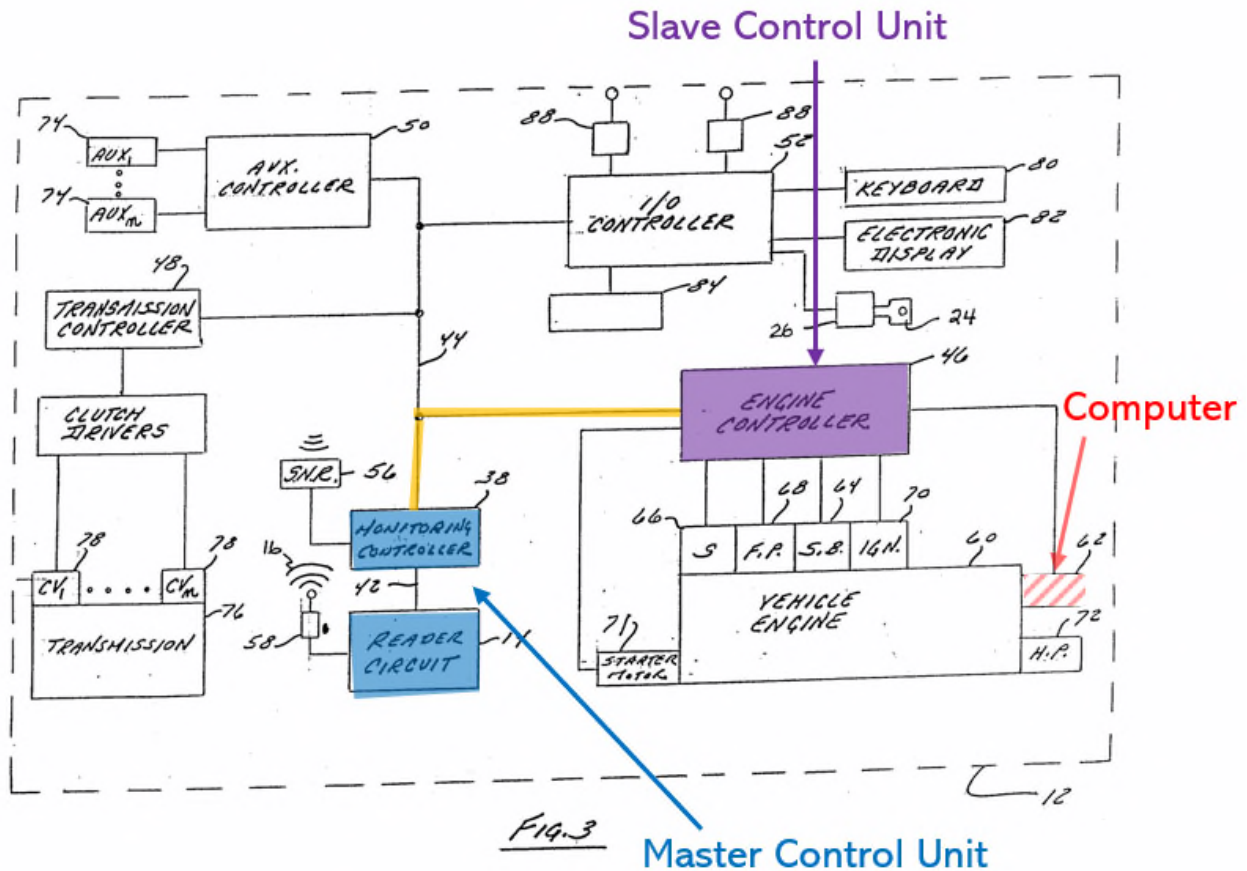
Arshad discloses Claim 1[C]. (Ehsani, ¶¶191-94.)

First, Arshad discloses a “slave control unit” installed in the vehicle and in communication with the “master control unit.” “Engine controller 46” (*e.g.*, slave control unit) is a “microprocessor-based controller” “coupled together with” monitoring controller 38 over “communication bus 44”:



(Arshad, Fig. 3 (annotated), [0028], [0041]-[0042].) Monitoring controller 38 “communicates with” engine controller 46 by sending and receiving data “packets” over the bus—for example, monitoring controller 38 transmits packets to engine controller 46 to shut down the fuel pump or ignition or limit vehicle or engine speed, and engine controller 46 transmits “packets on bus 44” indicative of engine operation to monitoring controller 38. (*Id.*, [0041], [0043]-[0044], [0065], [0072]-[0074].)

Second, engine controller 46 is coupled to multiple “computers” associated with the vehicle, such as “electronic” “governor 62”:



(Arshad, Fig. 3 (annotated).) Engine controller 46 sends signals to electronic governor 62 that “indicates a commanded fuel flow rate or power output,” which in turn generates and sends “an electronic signal” to fuel injectors or to open/close a “throttle valve.” (Arshad, [0046], Fig. 3.) Further, electronic governor 62 can “transmit a signal back to the engine controller 46” indicative of engine speed. (*Id.*) Thus, governor 62 is a “computer” because it is an electronic device that receives and processes information and can take different actions. (Ehsani, ¶¶192-94.)

Similarly, engine controller 46 is coupled to “transmission controller 48,” “auxiliary controller 50,” and “input/output controller 52” through bus 44. (Arshad,

Fig. 3, [0041], [0051]-[0054], [0063]-[0072].) Each has “microprocessor 90,” RAM, ROM, and “communication processor 96 configured to handle all communications over bus 44 with other controllers.” (*Id.*, [0075]-[0080], Fig. 4.) Thus, these other controllers comprise “computers” associated with the vehicle. (*Id.*; *see also* Ehsani, ¶¶192-94.)

1[D]: [said slave control unit...] [i] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile thereby providing feedback to the master control unit about usage of the vehicle, and [ii] wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit.

Arshad renders obvious Claim 1[D]. (Ehsani, ¶¶195-202.)

First, engine controller 46 (*e.g.*, slave control unit) is configured to monitor vehicle operation and generate signals to monitoring controller 38 (*e.g.*, master control unit), thereby providing feedback to it about vehicle usage. Engine controller 46 “is **configured to monitor**” operation, such as “elapsed engine hour[s],” “engine speed,” “engine load,” “oil pressure,” “oil temperature,” and “coolant temperature.” (Arshad, [0042]-[0043], [0046]-[0047], [0050], [0065], [0072], [0074].) It “**transmits**” such data (*e.g.*, signals) “on bus 44,” and “[c]ontroller 38 **receives** this information.” (*Id.*, [0072], [0042]-[0043], [0065].)

Regarding engine controller 46 generating a signal to monitoring controller 38 “if the at least one driver violates the operating profile, thereby providing

feedback to the master control unit about usage of the vehicle,” engine controller 46 receives operational limits from monitoring controller 38, with engine controller 46 then comparing engine operating conditions to the limits. (*Id.*, [0074].) If engine controller 46 determines a violation occurred based on the comparison of engine speed and load to the limits, it “can be configured to maintain these speed and load limits by itself, without input from controller 38.” (*Id.*) However, it would have been obvious to a POSITA that engine controller 46 could also, upon its comparison showing engine limits were violated, send a signal to the monitoring controller 38 regarding the violation, thereby providing such additional feedback about vehicle operation to monitoring controller 38. (*Id.*, [0065], [0069]- [0072], [0074].)

Arshad’s engine controller already provides engine operation information to monitoring controller 38 (and other controllers), and a POSITA would have understood engine controller 46 could likewise provide information regarding determined engine operation violations. (*Id.*; Ehsani, ¶¶196-200.) This would have simply been providing additional information (engine violations) that is similar to the information already provided (engine operating information) in the same manner by transmitting it over bus 44. (Arshad, [0064]-[0074].) In fact, engine operation violations are the type of data Arshad teaches monitoring controller 38 would consider, as Arshad discloses “[c]ontroller 38” constantly monitors data from other controllers, including data “indicative” of “events” or “error conditions experienced”

by the controllers. (*Id.*, [0042], [0069]-[0074].)

A POSITA would have been motivated to have engine controller 46 send data regarding violations of engine limits to monitoring controller 38, so that it can receive this feedback and take into account all vehicle operation information when issuing commands. (Ehsani, ¶¶196-200.) For example, where the operating time limit is exceeded, or where the driver forces the engine to exceed its operational load or RPM limits, engine controller 46 can alert monitoring controller 38 of this occurrence and then wait for a command on what action to take. (*Id.*, [0043]-[0045], [0072], [0074].) Having engine controller 46 send such a signal to monitoring controller 38 would also be consistent with Arshad’s approach of keeping all controllers in “constant communication with each other” (*id.*, [0064]), and allowing monitoring controller to determine the “priority” of the limit being exceeded before determining which actions the system should take. (*Id.*, [0043]-[0045].)

Second, engine controller 46 cooperates with at least one “computer” to control vehicle operation based on commands received from monitoring controller 38 (*e.g.*, master control unit). (Ehsani, ¶¶201-02.) For example, in response to information from engine controller 46 that an engine limit was exceeded, monitoring controller 38 can transmit a packet instructing engine controller 46 to “shut down the fuel pump, the ignition system, or to limit the speed of the vehicle or the engine,” as well as “transmit a packet to I/O controller 52 commanding it to display a message

indicating what limit has been exceeded.” (Arshad, [0044]-[0045], [0058]-[0063], [0071]-[0074].) In response to such commands, engine controller 46 cooperates with “computers” to control vehicle operation, such as by “sending a signal” to electronic governor 62, which then instructs the “fuel injectors” to regulate “fuel flow rate or power output” to “limit the speed of the vehicle,” “stop[]” the engine, or limit the engine’s RPM and load. (*Id.*, [0044]-[0046], [0074]; Ehsani, ¶¶201-02.)¹⁸

Similarly, engine controller 46 cooperates with I/O controller 52 (another computer) to control vehicle operation based on commands from monitoring controller 38. (*Id.*, [0044]-[0045], [0072].) When operational limits are exceeded, monitoring controller 38 transmits “packets” (*e.g.*, commands) to engine controller 46 and other controllers to take certain actions. (*Id.*, [0044]-[0046], [0058]-[0063], [0071]-[0074]; Ehsani, ¶¶201-02.) For example, based on information from engine controller 46, monitoring controller 38 can instruct I/O controller to display a message indicating a limit is about to be exceeded so the driver can take action, and if the driver does not make a correction, monitoring controller 38 can instruct engine controller 46 to limit engine speed and load or even shut down. (Arshad, [0044]-[0045], [0071]-[0074]; Ehsani, ¶¶201-02.)

¹⁸ The governor may alternatively “open or close” a “throttle valve.” (Arshad, [0046].)

2. Dependent Claims

a) Claim 4

Arshad renders obvious Claim 4. (Ehsani, ¶¶203-08.)

Arshad includes “satellite navigation receiver 56” connected to monitoring controller 38:

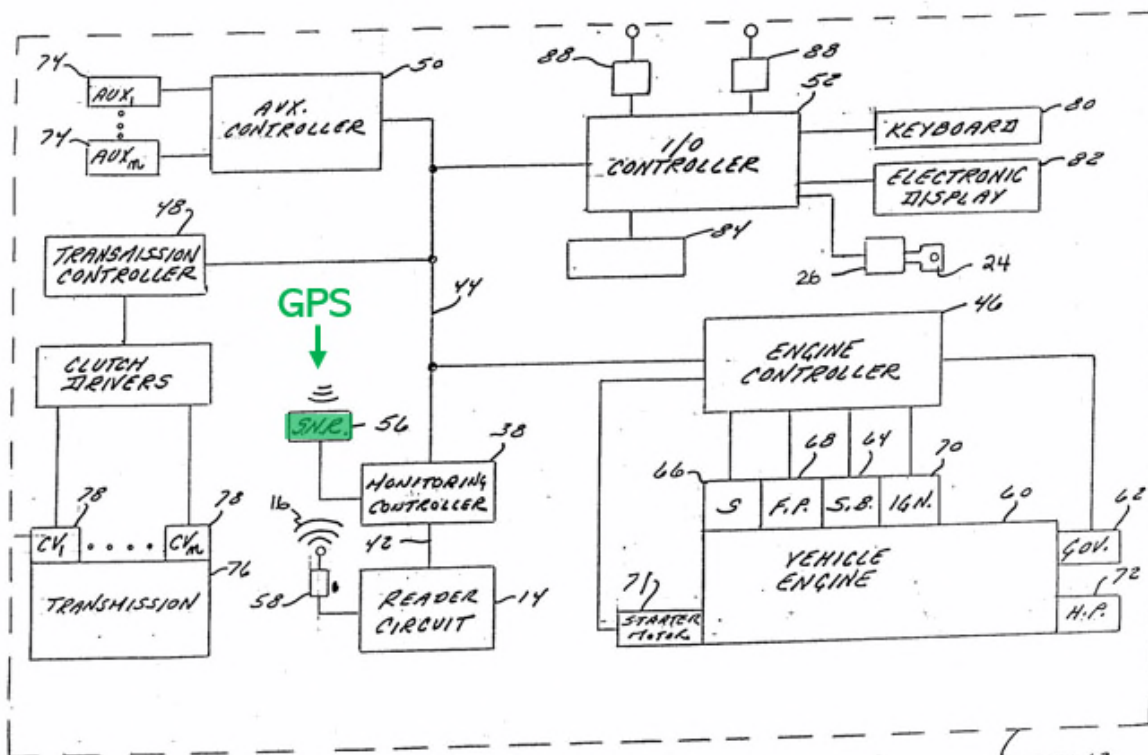


FIG. 3

(Arshad, Fig. 3 (annotated), [0029].) The satellite navigation receiver is a GPS receiver because it “is configured to receive radio transmissions from satellites and to convert them into data indicative of the vehicle’s current location such as latitude and longitude.” (*Id.*, [0029], [0073]; Ehsani, ¶¶204-08.)

Arshad includes “memory modules,” as each controller has **RAM memory 92** and **ROM memory 94** and “transponder 20” has “internal digital **memory.**” (Arshad, [0023]-[0027], [0075]-[0079], Figs. 2-4.)

Arshad includes numerous “function indicator modules.” Engine controller 46 is coupled to “sensors 66 that... generate signals **indicative** of oil pressure (oil pressure sensor), oil temperature (oil temperature sensor), coolant water temperature (coolant temperature sensor), engine speed (sensor 64) and engine load.” (*Id.*, [0047], [0050], [0065], Figs. 2-4.) Arshad also includes “display 82” which can “**indicate[]**” “**alarm conditions**” that the controllers determine exist based on sensor information, such as “oil pressure too low” or “approach[ing] the authorized engine RPM.” (*Id.*, [0056], [0074].) Further, Arshad’s controllers 38, 46, 48, 50, and 52 monitor vehicle operation and determine “**fault or error conditions,**” such as “low fuel” or “electrical output too low,” which are recorded in the transponder’s memory. (*Id.*, [0027].)

Additionally, Arshad’s controllers 38, 46, 48, 50, and 52 and sensors (*e.g.*, function indicator modules) further monitor functions including geographic location (*id.*, [0029], [0042], [0058]), engine operation time (*id.*, [0065], [0072]), and use of auxiliary components (such as hydraulic systems) (*id.*, [0051], [0060]-[0062], [0071].)

b) Claim 5

Arshad renders obvious Claim 5. (Ehsani, ¶¶209-11.)

First, Arshad’s operating profile, *e.g.*, driver “operational limits,” include “numeric or digital values that are remotely downloaded into the transponder” and stored in its memory. (Arshad, [0026]-0027], Fig. 2, [0023].)

Second, the transponder loads these “operational limits” into monitoring controller 38 when the driver is authenticated, thereby enabling controlled operation of the vehicle. (*Id.*, [0031], [0034], [0040]-[0043].) For example, monitoring controller 38 includes “RAM *memory 92*” to store “working variables” used by it, including the operational limits. (Arshad, [0075], [0078]-[0079]; Ehsani, ¶¶210-11.) *See supra* Claims 1[A]-[B], 4.

c) Claim 6

Arshad renders obvious Claim 6. (Ehsani, ¶212.) *See supra* Claim 4.

d) Claim 10

Arshad renders obvious Claim 10. (Ehsani, ¶¶213-15.)

Arshad’s identification interface includes a “radio (RF) transponder 20” (“preferably one of Texas Instruments RFID products”) that transmits “radio signals” which are then “receiv[ed]” by reader circuit 14’s “antenna 58.” (Arshad, Abstract, [0019], [0022]-[0025], [0030]-[0034].) *See supra* Claim 1[A]-[B].

Arshad’s “transponder 20” is also a “portable handheld device.” (Ehsani,

¶¶214-15.) It includes a microcontroller, integrated circuit package, antenna, capacitors, and memory and can be “molded into a thin credit card-sized sheath” and “easily carried” or incorporated into the ignition key. (*Id.*, [0020]-[0023], Figs. 1-2].)

E. Ground 5 – Arshad-Petrik Renders Obvious Claims 2-4 8-9, 11, and 13-20

Arshad in view of Petrik renders obvious Claims 2-3, 9, 11, and 13-20. (Ehsani, ¶¶216-69.) Petrik was filed August 9, 2005, published July 19, 2007, and is prior art under pre-AIA §§102(a), (e).

1. Independent Claims

a) Claim 11

Arshad in view of Petrik renders obvious Claim 11. (Ehsani, ¶¶220-34.)

11[pre]: *A driver authentication and monitoring system, comprising:*

If limiting, Arshad discloses Claim 11[pre]. (Ehsani, ¶221.) *See* Ground 4, Claim 1[pre].

11[A]: *a master control unit in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver;*

Arshad discloses Claim 11[A]. (Ehsani, ¶¶222-23.)

Arshad discloses a “master control unit” (*e.g.*, reader circuit 14 and monitoring controller 38) for “authenticating at least one driver via [a] driver identification [interface].” *See* Ground 4, Claim 1[A]. The reader circuit and

monitoring controller “associate[]” an “operating profile with the at least one driver.” *See* Ground 4, Claim 1[B].

11[B]: a GPS module providing at least location and speed information in association with movement of the motor vehicle; and

Arshad in view of Petrik renders Claim 11[B] obvious. (Ehsani, ¶¶224-28.)

Arshad discloses a “satellite navigation receiver 56” (*e.g.*, “GPS module”) which provides monitoring controller 38 with “data indicative of the vehicle’s current location.” (Arshad, [0029], [0073], Fig. 3.) *See* Ground 4, Claim 4.

In addition, it would have been obvious for such GPS module to provide speed information as well. (Ehsani, ¶¶225-28.) For example, Petrik, in the same field, discloses a “GPS based” system with an “in-vehicle monitoring unit” for authenticating drivers, monitoring vehicle operation, and taking actions such as issuing alerts and slowing or stopping a vehicle if the driver deviates from her operational limits. (Petrik, [0016]-[0026], [0030], Fig. 1.)

Petrik uses a “GPS receiver module” to provide location *and* speed information and “keeps a constant log of the date, time, location, distance travelled and speed of the vehicle both in the units’ memory and in the smart card.” (*Id.*, [0001], [0025]-[0026], [0009], [0040].) GPS speed and location information is used by the in-vehicle unit to prevent the exceeding of speed limits and to determine if a driver has deviated from an allowed route. (*Id.*, [0025]-[0028], [0030]; Ehsani,

¶¶225-28.)

A POSITA would have been motivated to use GPS in Arshad to determine both location and speed, as taught by Petrik, to have an accurate source of location, speed, and time information that could not be manipulated by the driver and that could be stored in vehicle operation logs. (Petrik, [0001], [0009], [0012], [0025]-[0028].) A POSITA would have had a reasonable expectation of success using a GPS module to provide both speed and location, as this would simply be use of a known component for its intended function. (Ehsani, ¶¶225-28.) Moreover, a POSITA would have understood that using GPS speed and location would provide the information necessary to determine if a driver has violated speed or geographic operational limits. (*Id.*)

11[C]: a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module; and

Arshad in view of Petrik renders obvious Claim 11[C]. (Ehsani, ¶¶229-31.)

Arshad’s “microcontroller 30” within transponder 20 can “receive[] data from the vehicle” and “store[] this data in its internal memory”—thus disclosing a “data logging device recording vehicle operation data” (*e.g.*, distance travelled, time vehicle started/stopped). (Arshad, [0025]-[0027].) *See* Ground 4, Claim 11[C].

Moreover, Petrik teaches “automatically and irrefutably logging via GPS, ...vehicle location, vehicle speeds, speeding offences, distance covered etc. and

recording these on a secure smart card as well as in the vehicle units' memory.” (Petrik, [0009], [0012], [0018], [0025]-[0029].) It would have been obvious to a POSITA to modify Arshad to record GPS location *and* speed information in transponder 20, as well as in controller 38's memory. (Ehsani, ¶¶230-31.) A POSITA would have understood this would, as taught by Petrik, provide a log of operational and infraction data that could not be manipulated by the driver. *See supra* Claim 11[B].

11[D]: *[i] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, [ii] said slave control unit in communication with said master control unit and...*

Arshad discloses Claim 11[D]. (Ehsani, ¶232.) *See* Ground 4, Claim 1[C].

11[E]: *[said slave control unit ...] [i] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile thereby providing feedback to the master control unit about usage of the vehicle, and [ii] wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit;*

Arshad discloses Claim 11[E]. (Ehsani, ¶233.) *See* Ground 4, Claim 1[D].

11[F]: *wherein the master control unit permits the at least one driver to operate the vehicle within an operating profile if the master control unit receives at least one of a unique identification code to permit the at least one driver to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.*

Arshad discloses Claim 11[F]. (Ehsani, ¶234.) *See* Ground 4, Claims 1[B]-1[D].

b) Claim 15

Arshad in view of Petrik renders obvious Claim 15. (Ehsani, ¶¶235-50.)

15[pre]: *A method of authenticating and monitoring drivers, comprising:*

If limiting, Arshad discloses Claim 15[pre]. (Ehsani, ¶236.) *See* Ground 4, Claim 1[pre].

15[A]: *providing a motor vehicle with a driver authentication and monitoring system;*

Arshad discloses a driver authentication and monitoring system in a vehicle. (Ehsani, ¶237.) *See* Ground 4, Claims 1[pre]-1[A].

15[B]: *programming the driver authentication and monitoring system with an operating profile associated with a high risk driver;*

Arshad discloses and renders obvious Claim 15[B]. (Ehsani, ¶¶238-40.)

Arshad's system can be programmed with an operating profile associated with a high-risk driver.¹⁹ *See* Ground 4, Claim 1[B]. Arshad's "operational limits" are programmed into the transponder, as they are "*remotely downloaded into* the transponder" and maintained in its memory. (Arshad, [0026], [0043], [0057]-[0059].) *See* Ground 4, Claim 1[B]. Further, the operational limits are programmed

¹⁹ The '427 states high-risk drivers may be fleet or rental drivers. ('427, 2:34-38.)

Arshad can be used with drivers of "fleet[]" vehicles, including rental vehicles. (Arshad, [0005]-[0009], [0033], [0045].)

into monitoring controller 38, as they are downloaded from the transponder's memory to controller 38 "for processing." (*Id.*, [0034], [0043], [0057], [0071]-[0073]; *see also* [0074] (operational limits may be downloaded to engine controller 46).) Moreover, these limits are maintained by "data logging devices," namely the memories in transponder 20, monitoring controller 38, and other controllers. (*Id.*, [0034], [0043], [0057], [0074]-[0080].)

15[C]: *authenticating the high risk driver and enable operation of the motor vehicle within limits of the operating profile by monitoring operation of the motor vehicle to determine if the high profile driver is violating the operating profile;*

Arshad discloses Claim 15[C]. (Ehsani, ¶¶241-43.)

Arshad authenticates high-risk or high profile drivers and enables their operation of a vehicle within respective operating profiles. (Ehsani, ¶242.) *See* Ground 4, Claims 1[A]-[B].

Further, Arshad "monitors" vehicle operation to determine if the driver violates her profile. *See* Ground 4, Claims 1[C]-[D]. For example, monitoring controller 38 compares data received from controllers and sensors with operational limit data received from the transponder "to determine whether the operator has attempted to exceed any of the operational limits" and if the limits are exceeded. (*Id.*, [0042]-[0044], [0058]-[0059], [0065], [0071]-[0074].)

15[D]: *generating a signal if said high risk driver violates the operating profile while operating the motor vehicle; and*

Arshad discloses and renders obvious Claim 15[D]. (Ehsani, ¶¶244-45.)

Arshad generates a signal if the high-risk driver violates her profile. For example, if operational limits are approached or exceeded, monitoring controller 38 generates a signal to other controllers “directing” them to take action. (Arshad, [0028], [0043]-[0046], [0057]-[0063], [0071]-[0074].) Monitoring controller 38 can signal engine controller 46 to slow or stop the engine, and signal I/O controller 52 to generate an “audio alarm” or visual “alphanumeric message.” (*Id.*, [0044]-[0045], [0057]-[0059], [0061]-[0063], [0071]-[0074].) *See* Ground 4, Claims 1[C]-[D].

15[E]: *governing mechanical operations of the vehicle remotely if the high profile driver violates the operating profile.*

Arshad in view of Petrik renders obvious Claim 15[E]. (Ehsani, ¶¶246-49.)

Petrik’s in-vehicle unit communicates with a “base station” and a “Command Centre” through SATELLITE/GPRS/GSM two-way communications. (Petrik, [0016]-[0018], [0030], [0069], Fig. 1, Cls. 48-51.) The in-vehicle unit and remote Command Centre monitor vehicle operation, including whether the driver is adhering to an allowed “route plan.” (*Id.*, [0030], [0010].) If the driver is not adhering to such plan, or is out of control or hostile, a signal can be sent from the in-vehicle unit to the remote Command Centre, and the Command Centre can send the in-vehicle unit a “disable” command. (*Id.*) This Command Centre “disable”

command controls operation of the vehicle remotely, as it causes the engine management system to “lock up” and stop the vehicle. (Ehsani, ¶¶247-49.)

It would have been obvious to modify Arshad to include a Command Centre in communication with Arshad’s “control system 12” to allow for remote vehicle control, as taught by Petrik. (*Id.*) A POSITA would have been motivated to modify Arshad’s control system 12 to include providing for remote commands to control vehicle operation, as taught by Petrik, to increase safety and give real-time instructions based on information at the command facility. (Petrik, [0030], Cls. 48-53, 58-60.)

A POSITA would have had a reasonable expectation of success in implementing such remote commands to, for example, disable the engine, in Arshad. (Ehsani, ¶¶247-49.) Arshad’s engine controller 46 can slow or stop the engine based on commands received from monitoring controller 38 (Arshad, [0044]-[0045], [0074]), and Petrik merely adds that a command sent from an in-vehicle controller (like Arshad’s monitoring controller 38) to an engine controller (like Arshad’s engine controller 46) can originate from a remote facility. (Petrik, [0030], Cls. 58-60.) This would have merely added a known component—a two-way communications module like Petrik’s SATELITE/GPRS/GSM module—for its intended purpose.

Arshad’s system was ready for such modification, as it includes multiple

controllers communicating over a bus, and adding the two-way communication module would simply be the addition of another controller on this same bus. (Ehsani, ¶¶247-49.) Thus, Arshad would continue operating as expected, but with an additional safety backup to allow a remote facility to take control of the vehicle if the driver continuously violates limits or is out of control. (*Id.*)

2. Dependent Claims

a) Claim 2

Arshad in view of Petrik renders obvious Claim 2. (Ehsani, ¶¶250-254.)

Arshad's program module, comprising "numeric or digital values" indicative of operational limits, can be "remotely downloaded into the transponder." (Arshad, [0026].) These limits reflect "different degrees of access" authorized by fleet management. (*Id.*, [0008]-[0013].)

Petrik, like Arshad, discloses a fleet management system that authenticates drivers and allows vehicle operation only within drivers' parameters, such as speed limits, geographic route plans, and time limits. *See supra* Claim 11[B]. Petrik includes a "Command Centre with an up to date database of road conditions" and other parameters associated with a vehicle, such as "accidents, road closures, detours, adverse weather," "geographic speed zones," "state border crossings," and "driver hours of service records." (Petrik, [0010]-[0011], [0024], [0030], Cl. 49.) An authorized dispatcher at a dispatch has access to the Command Centre database via

a SATELITE/GPRS/GSM link and can use the database to program the driver's operating profile. (*Id.*, [0024], [0030], Cls. 49-51; Ehsani, ¶¶251-54.)

It would have been obvious to a POSITA to modify Arshad to provide access to a remote database of information relevant to driver and vehicle parameters, as taught by Petrik. (Ehsani, ¶¶251-54.) A POSITA would have understood this could be done, for example, by providing authorized fleet managers computer access to the remote database over a network communication link. (Petrik, [0010], [0018], [0024], [0030], Cls. 48-51.) This would have allowed fleet managers to access the database and review the information therein when programming the “numeric or digital values” indicative of operational limits, before they are downloaded remotely to the transponder. (Arshad, [0026]; Petrik, [0010], [0018], [0024], [0030], Cls. 48-51; Arshad, [0026]; Ehsani, ¶¶251-54.)

Arshad was ready for improvement in this regard, and a POSITA would have had a reasonable expectation of success because this would have involved simply using known networked computers and communication interfaces for their intended functions. (Ehsani, ¶¶251-54.) Moreover, this would have facilitated Arshad's goals of managing fleets of vehicles and authorizing different degrees of vehicle operation. (Arshad, [0008]-[0013]; Ehsani, ¶¶251-54.)

b) Claim 3

Arshad in view of Petrik renders obvious Claim 3. (Ehsani, ¶¶255-56.)

Arshad's driver identification interface (*e.g.*, transponder 20 and reader antenna 58) loads driver operational limits to the master control unit (*e.g.*, reader circuit and monitoring controller 38). *See* Ground 4, Claim 1[A]-[B].

Moreover, Arshad in view of Petrik renders obvious loading the operational limits using the transponder and a remote computer. *See* Ground 5, Claim 2. As discussed, a POSITA would have understood an authorized user at a remote computer could access a central database, program a profile, and then "remotely download" operating limit values to the transponder. *Id.*

c) Claim 4

Arshad in view of Petrik renders obvious Claim 4. (Ehsani, ¶¶257-58.)

Arshad discloses a satellite navigation module, memory module, and function indicator module. *See* Ground 4, Claim 4. Moreover, Petrik discloses a GPS module, and it would have been obvious to include such a GPS module in Arshad. *See supra* Claim 11[B].

d) Claims 8/13

Arshad in view of Petrik renders obvious Claims 8 and 13. (Ehsani, ¶¶259-60.)

Arshad's "operating limits" include (i) "maximum speed" (*i.e.*, maximum allowable vehicle speed), (ii) "geographical area in which the vehicle" can operate and "total distance of authorized travel" (*i.e.*, allowable vehicle locations), and (iii)

“allowed times and dates of operation,” “number of hours of authorized use,” and “predetermined number of hours” the engine can be operated (*i.e.*, allowable hours of operation). (Arshad, [0011]-[0013], [0026], [0043]-[0045], [0057], [0059], [0072]-[0074].) *See* Ground 4, Claim 1[B].

e) Claims 9/14

Arshad in view of Petrik renders obvious Claims 9/14. (Ehsani, ¶¶261-65.)

Arshad monitors whether a driver is operating the vehicle in accordance with her operating profile, and, if she violates her profile, the system can “display a message” that provides an alert “indicating what limit has been exceeded.” *See* Ground 4, Claim 1[D]. Further, Petrik discloses an “in-vehicle monitoring unit” that generates an alarm signal which “notifies” *authorized personnel at a remote facility* (*e.g.*, “Transportation Management Command Centre”), via a “SATELLITE/GPRS/GSM” link, when a driver violates her profile, such as by “divert[ing] inappropriately from the ‘filed’ route plan.” (Petrik, [0030], Cls. 58-60.)

It would have been obvious to a POSITA to modify Arshad to have its system (*e.g.*, engine controller 46) generate and send “alarm signals” to remote authorized personnel via a communications link, as taught by Petrik. *See* Ground 5, Claim 15[E]. (Ehsani, ¶¶263-65.) A POSITA would have understood in view of Petrik that, after determining there is a violation, Arshad’s engine controller could generate an “alarm signal” causing system to transmit an alert to authorized persons at a remote

facility. (*Id.*) The inclusion of such a communications link to alert remote personnel would have been the mere addition of basic, well-known components that could be used with the system already existing in Arshad. (*Id.*)

A POSITA would have understood that such profile-violation alerts in Arshad could likewise be transmitted to authorized personnel at a remote facility, as taught by Petrik. (*Id.*) A POSITA would have also been motivated (and it would have been obvious to try) to have engine controller 46 generate such alerts, since it is already monitoring operation of vehicle components and can determine whether a profile violation has occurred. (*Id.*) By having Arshad’s engine controller and system send such an alert to authorized personnel at a remote facility, Arshad would be able to better “manage access to vehicles used in fleets” (a stated purpose of it), as remote personnel would be able to monitor driver operation in real-time and better ensure that drivers comply with profiles. (*Id.*)

f) Claim 16

Arshad in view of Petrik renders obvious Claim 16. (Ehsani, ¶266.) *See supra* Claim 11[B].

g) Claims 17/18

Arshad in view of Petrik renders obvious Claims 17/18. (Ehsani, ¶¶267-68.)

Arshad generates an audible alarm by energizing an annunciator to generate a “sound to get the operator’s attention.” (Arshad, [0063], [0071]-[0072].)

Further, Arshad in view of Petrik renders obvious providing an alarm signal remotely to an authorized user. *See supra* Claims 9/14.

h) Claims 19/20

Arshad in view of Petrik renders obvious Claims 19/20. (Ehsani, ¶¶273-74.)

Arshad takes numerous actions in response to profile violations, including generating a control signal that limits vehicle functionality by slowing or stopping the vehicle. *See supra* Claim 15[D]; *see also* Ground 4, Claim 1[D].

Arshad further discloses “transmit[ing] a packet that shuts down a particular vehicle subsystem” if a driver violates her profile. (Arshad, [0044]-[045], [0057], [0060]-[0063], [0071]; *see also* [0011]-[0013], [0026], [0040], [0051], [0067].)

F. Ground 6 – Arshad (Alone or as Modified by Petrik) in View of Wu Renders Obvious Claims 7/12

Arshad (alone or as modified by Petrik) in view of Wu renders obvious Claims 7/12. (Ehsani, ¶¶271-76) Each of the well-known components recited in Claims 7/12 is disclosed or would have been obvious based on Arshad or, at minimum, Arshad in view of Wu. (*Id.*)

Arshad’s slave control unit includes a “power regulator module.” (Ehsani, ¶272.) Engine controller 46 includes a “driver circuit 102” that “controls the application of power” to “actuators” such as the “fuel pump, governor and ignition system.” (Arshad, [0077]; *see also* [0044], [0048]-[0049], [0064].) Moreover,

because it is an electronic component and controls electronic components, a POSITA would have understood engine controller 46 to have a “power regulator” to ensure receipt of a stable supply of the required voltage, including as taught by Wu. (Wu, [0020], [0022], [0027]-[0028]; Ehsani, ¶272.)

Arshad’s slave control unit includes a “starter relay module.” (Ehsani, ¶273.) Engine controller 46 “is coupled to the engine starting motor 71 to turn the starting motor on or off under computer control.” (Arshad, [0049]-[0050].) Such a coupling includes a starter relay to energize the starting motor. (Ehsani, ¶273.) Wu discloses that “starter relays” are commonly used to energize starter motors. (Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2), and a POSITA would have included such relay in Arshad to provide a well-known, commonly-used mechanism for activating the starting motor. (Ehsani, ¶135.)

Arshad’s slave control unit includes a “definable relay module.” (Ehsani, ¶274.) Engine controller 46 is “coupled to ignition system 70 of the engine” and can “energize or de-energize the ignition under computer control.” (Arshad, [0049]-[0050]; *see also* [0044].) Such coupling would involve a relay module to (de)activate the ignition system. (Ehsani, ¶274.) Moreover, Wu discloses that ignition systems can be (de)energized using an ignition circuit enabling means comprising a processor (like in Arshad’s engine controller) and a relay. (Wu, [0020]-[0021], [0025], [0031], [0039], Figs. 1-2.) A POSITA would have been motivated to use

such a processor and ignition relay, as taught by Wu, to implement the computerized control of the ignition system with Arshad's engine controller. (Ehsani, ¶274.) This would have merely been the implementation of known components (*e.g.*, ignition relay) in a similar system for their intended purpose to achieve the same results (*e.g.*, (de)energizing the ignition). (*Id.*)

Arshad's slave control unit includes a "slave microcontroller." (Ehsani, ¶275.) Arshad's engine controller 46 and other controllers are "microprocessor-based controller[s]," each including a microprocessor, RAM, ROM, sensor circuit, driver circuits, and communication processor. (Arshad, [0028], [0075]-[0080], Fig. 4.)

Arshad renders obvious that its slave control unit includes an "alarm synthesizer." (Ehsani, ¶276.) Arshad's I/O controller can "energize annunciator 84" to "generate a sound to get the operator's attention" when operational limits are exceeded. (Arshad, [0054], [0063], [0071]-[0072].) A POSITA would be motivated to provide the annunciator with engine controller 46, such that engine controller 46 could activate the annunciator to issue an audible alarm, upon engine controller 46 determining allowed engine operational hours have been or will be exceeded. (Ehsani, ¶276.) Engine controller 46 includes driver circuitry like the I/O controller does, and it would have been obvious to use this driver circuitry to operate an annunciator immediately when engine controller 46 determines an operational limit is or will be exceeded. (Arshad, [0072], [0074]; Ehsani, ¶276.) Similarly, Wu

discloses generating such audible alerts with a synthesizer, including an “operational amplifier” and “resistor,” and a POSITA would have readily understood this to be a common and simple way to implement the audible alerts in Arshad. (Wu, [0030]; Ehsani, ¶276.)

IX. DISCRETIONARY CONSIDERATIONS UNDER 314(A) AND 325(D) STRONGLY FAVOR INSTITUTION.

The Board should institute review because Petitioner has been diligent and the circumstances around the parallel district court case (which involves seven patents with over 130 claims) do not warrant denial under §314(a). *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 11-21 (Dec. 1, 2020) (precedential) (citations omitted). The case was recently transferred to NDGA, and the Georgia court has not set a trial date, issued a schedule, or even set an initial conference date. Even before the transfer, the case was in its early stages in EDTX. Little fact discovery had taken place (including no depositions), and *Markman* proceedings had not commenced.

Similarly, analysis under the framework from *Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH* demonstrates that denial under §325(d) is not appropriate. IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (precedential). The grounds in this Petition are not the same or substantially the same as art and arguments raised during prosecution. The “new, noncumulative prior art

asserted in the Petition” strongly favors IPR. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (P.T.A.B. Oct. 16, 2019) (§§II.B and II.C precedential). Should PO attempt to analogize any previously considered art or arguments to those here, Petitioner reserves the right to respond.

The Board should institute review because the merits are strong and the circumstances here do not warrant discretionary denial. Should Patent Owner raise discretionary denial theories, Petitioner reserves the right to respond before institution. *See* March 26, 2025, USPTO Memorandum titled “Interim Processes for PTAB Workload Management.”

X. CONCLUSION

For the reasons above, *inter partes* review and cancellation of Claims 1-20 of U11,472,427 are requested.

Date: April 25, 2025

/s/ Celine J. Crowson

Celine J. Jimenez Crowson (Reg. No. 40,357)

Joseph J. Raffetto (Reg. No. 66,218)

Scott Hughes (Reg. No. 68,385)

HOGAN LOVELLS US LLP

555 13th Street N.W.

Washington, D.C. 20004

Telephone: 202.637.5600

Facsimile: 202.637.5710

TABLE OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 11,472,427 (“ 427 Patent ”)
1002	File History for the ’427 Patent
1003	Reserved
1004	Declaration of Dr. Mark Ehsani
1005	Curriculum Vitae of Dr. Mark Ehsani
1006	U.S. Patent No. 6,225,890 (“ Murphy ”)
1007	U.S. Patent Application Publication No. 2003/0189482 A1 (“ Arshad ”)
1008	U.S. Patent Application Publication No. 2007/0168125 A1 (“ Petrik ”)
1009	U.S. Patent Application Publication No. 2008/0046739 (“ Adams ”)
1010	U.S. Patent Application Publication No. 2008/0114501 (“ Wu ”)

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing Petition for *Inter Partes* Review contains 13,896 words, excluding those portions identified in 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

/s/ Celine J. Crowson
Celine J. Crowson, Lead Counsel
(Reg. No. 40,357)

CERTIFICATION OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, the foregoing Petition for *Inter Partes* Review and exhibits thereto were served on April 25, 2025, by Overnight Courier at the following address of record and addresses known to Petitioner as likely to effect service and the address of record for the '427 Patent:

64064 - Ortiz & Lopez, PLLC P.O. BOX 4484 Albuquerque, NM 87196 United States	Ortiz & Lopez, PLLC 6605 Uptown Blvd. NE 260 Albuquerque, NM 87196 United States
--	---

/s/ Jason A. Bradley
Jason A. Bradley
Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004-1109

Appendix A

Claim	Limitations
Independent Claim 1	[pre] A driver authentication and monitoring system, comprising:
	[A] a master control unit operating in a motor vehicle for authenticating at least one driver via a driver identification interface,
	[B] wherein the master control unit receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver and accessible by the master control unit; and
	[C] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, said slave control unit in communication with said master control unit and
	[D] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile thereby providing feedback to the master control unit about usage of the vehicle, and wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit.
Claim 2	The driver authentication and monitoring system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.
Claim 3	The driver authentication and monitoring system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the master control unit for the at least one driver.

Claim 4	The driver authentication and monitoring system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.
Claim 5	The driver authentication and monitoring system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.
Claim 6	The driver authentication and monitoring system of claim 4, wherein the GPS module provides location information to at least the master control unit in association with a physical location of the vehicle.
Claim 7	The driver authentication and monitoring system of claim 1, wherein the slave control unit further comprises a power regulator module; a starter relay module; a definable relay module; a slave microcontroller; and an alarm synthesizer.
Claim 8	The driver authentication and monitoring system of claim 2, wherein the at least one operating parameter comprises at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.
Claim 9	The driver authentication and monitoring system of claim 1, wherein the slave control unit generates an alarm signal for alerting said authorized user when the at least one driver violates the operating profile.
Claim 10	The driver authentication and monitoring system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.
	[pre] A driver authentication and monitoring system, comprising:

<p>Independent Claim 11</p>	<p>[A] a master control unit in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver;</p> <p>[B] a GPS module providing at least location and speed information in association with movement of said motor vehicle;</p> <p>[C] a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module; and</p> <p>[D] a slave control unit installed in the motor vehicle and coupled to at least one computer associated with the motor vehicle, said slave control unit in communication with said master control unit and</p> <p>[E] configured to monitor operation of the motor vehicle and generate a signal to the master control unit if the at least one driver violates the operating profile, thereby providing feedback to the master control unit about usage of the vehicle, and wherein the slave control unit cooperates with the at least one computer to control operation of the vehicle based on commands received from the master control unit;</p> <p>[F] wherein the master control unit permits the at least one driver to operate the vehicle within an operating profile if the master control unit receives at least one of a unique identification code to permit the at least one driver to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.</p>
<p>Claim 12</p>	<p>The driver authentication and monitoring system of claim 11, wherein the slave control unit further comprises a power regulator module; a starter relay module; a definable relay module; a slave microcontroller; and an alarm synthesizer.</p>
<p>Claim 13</p>	<p>The driver authentication and monitoring system of claim 11, wherein the operating profile comprises at least one operating parameter including at least one of: a maximum allowable vehicle</p>

	speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.
Claim 14	The driver authentication and monitoring system of claim 11, wherein the slave control unit generates an alarm signal for remotely alerting the authorized user when the at least one driver violates said operating profile.
Independent Claim 15	[pre] A method of authenticating and monitoring drivers, comprising:
	[A] providing a motor vehicle with a driver authentication and monitoring system;
	[B] programming the driver authentication and monitoring system with an operating profile associated with a high risk driver;
	[C] authenticating the high risk driver and enable operation of the motor vehicle within limits of the operating profile by monitoring operation of the motor vehicle to determine if the high profile driver is violating the operating profile;
	[D] generating a signal if said high profile driver violates the operating profile while operating the motor vehicle; and
	[E] governing mechanical operations of the vehicle remotely if the high profile driver violates the operating profile.
Claim 16	The method of authenticating and monitoring drivers in claim 15, wherein the motor vehicle includes a GPS module and the monitoring operation of the motor vehicle further comprises obtaining GPS data including motor vehicle speed and location.
Claim 17	The method of authenticating and monitoring drivers in claim 15, wherein the step of generating a signal includes providing an

	audible alarm to the driver and a signal remotely to an authorized user.
Claim 18	The method of authenticating and monitoring drivers in claim 16, wherein the step of generating a signal includes providing an alarm remotely to an authorized user.
Claim 19	The method of authenticating and monitoring drivers in claim 15, wherein the step of generating an alarm signal includes providing a control signal that limits functionality within the motor vehicle.
Claim 20	The method of authenticating and monitoring drivers in claim 16, wherein the step of generating a signal includes providing a control signal that limits functionality of the motor vehicle.