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. 9,045,101

CORRECTED PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-20 OF U.S. PATENT NO. 9,045,101 UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. §§42.100 *et seq.*

Filed on behalf of Petitioners:

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

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Mercedes-Benz Group AG ("**Petitioner**") challenges Claims 1-20 of U.S. Patent No. 9,045,101 ("**'101**") (EX1001). The '101 claims nothing more than what was well-known in the art of motor vehicle safety systems. The '101 purports to invent a vehicle authentication and monitoring system permitting an authenticated driver to drive the vehicle within an operating profile and generate an alarm signal to govern mechanical operations of the vehicle remotely if the driver violates the operating profile. But this was not new at the time of the '101. Driver authentication, monitoring, generating an alarm signal, and remotely governing mechanical operations of a vehicle were well-known before this. For example, US6,225,890 ("**Murphy**") (EX1006), US2007/0168125 ("**Petrik**") (EX1009), and German Patent App. Publication No. DE10323723A1 ("**Schanz**") (EX1007,EX1008) each disclose driver authentication, monitoring, generating an alarm, and remotely governing operations of a vehicle.

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

A. Real Parties-in-Interest

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

B. Related Matters:

Assignee of record The Phelan Group, LLC ("**Patent Owner**") asserted the

’101 in the following proceedings:

- *The Phelan Grp., LLC v. Toyota Motor Corp.*, No. 2-23-cv-00093 (E.D. Tex.), filed March 7, 2023, voluntarily dismissed with prejudice.
- *The Phelan Grp., LLC v. Kia Corp.*, No. 2-23-cv-00094 (E.D. Tex.), filed March 7, 2023, voluntarily dismissed with prejudice.
- *The Phelan Grp., LLC v. Honda Motor Co.*, No. 2-23-cv-00606 (E.D. Tex.), filed December 15, 2023.
- *The Phelan Grp., LLC v. Mercedes-Benz Grp. AG*, No. 2-23-cv-00607 (E.D. Tex.), filed December 15, 2023.

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. If additional fees are due during the proceeding, the undersigned authorizes the Office to charge them to Deposit Account No.

50-1349.

IV. CERTIFICATION OF GROUNDS FOR STANDING

The undersigned and Petitioner certify that the ’101 is available for *inter partes* review, and that it is not barred or estopped from requesting this review.

V. PRECISE RELIEF REQUESTED

The relief requested is cancellation of the challenged claims, as follows:

Ground	References	Claims	Basis
1	Murphy	1-20	102/103
2	Murphy in view of Schanz	1-20	103
3	Murphy in view of Schanz in view of Benco	10	103
4	Petrik	1-20	102/103
5	Petrik in view of Schanz	1-20	103
6	Petrik in view of Schanz in view of Benco	10	103

VI. ’101 OVERVIEW

A. Background

The ’101 is directed toward “[a] driver authentication and safety system and method for monitoring and controlling vehicle usage by high-risk drivers.” (’101, Abstract.) An “authorized vehicle owner” (*e.g.*, “parent”) can create an “operating

profile," which is a "set of driving rules and conditions" for the "high-risk driver" (*e.g.*, "teen"). (*Id.*, 6:34-51.) Operating profile restrictions are enforced by a "driver authentication system" which includes a "master control unit" and a "slave control unit." (*Id.*, 2:19-36; 5:48-51; Fig. 6.)

Driver identification information and operating profile restrictions are loaded to the "master control unit" using a "driver identification and data logging device." (*Id.*, 2:19-36.) The driver is authenticated, and driving activity is monitored using a GPS providing "time of day, speed and location data associated with the vehicle." (*Id.*, 2:53-56.) If the driver violates an operating profile restriction, a "real time alarm signal" is generated. (*Id.*, 2:33-56.) "The alarm signal 445 can result in an actual audible alarm, or it can … communicate conditions to the driver, limit/disable radio functionality, govern mechanical operations (*e.g.*, lower/limit speed), remotely contact vehicle owners/fleet managers, and other electrical or mechanical functions[.]" (*Id.*, 6:65-7:5.)

B. Prosecution

The '101 was filed April 8, 2013 as a continuation of US8,417,415 ("**'415**") (EX1003), filed on July 1, 2009 and Provisional Application No. 61/077,568, filed on July 2, 2008. In a Non-Final Rejection, claims 1-20 were rejected over US2010/0004818 (publication of the '415). (EX1002, 99-104.) Patent Owner filed a terminal disclaimer, amended independent claims 1, 11, and 15 to add governing

mechanical operations remotely, and amended claim 10 to add "an iButton device; and a USB compatible device." (*Id.*, 78-86.) In a subsequent Non-Final Rejection, claims 1-9 and 11-20 were allowed and claim 10 was rejected as indefinite for claiming the trademark/trade name "iButton." (*Id.*, 59-63.) Patent Owner amended claim 10 to remove "an iButton device." (*Id.*, 49-52.) Following this, a Notice of Allowance issued. (*Id.*, 26-32.)

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 claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the '101. 37 C.F.R. § 42.100(b).

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

A POSITA at the time of the invention would have at least a bachelor's degree in electrical engineering, computer engineering, computer science, or similar disciplines, and at least two years of professional 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. Mehrdad Ehsani (EX1004, "Ehsani") ¶23.)[1] The more education one has, the less experience needed to attain an ordinary level of skill. *Id.* Similarly, more experience in the field may serve as a substitute for formal education. *Id.*

VIII. ANALYSIS OF GROUNDS FOR UNPATENTABILITY

A. Ground 1 – Murphy Anticipates or Renders Obvious Claims 1-20

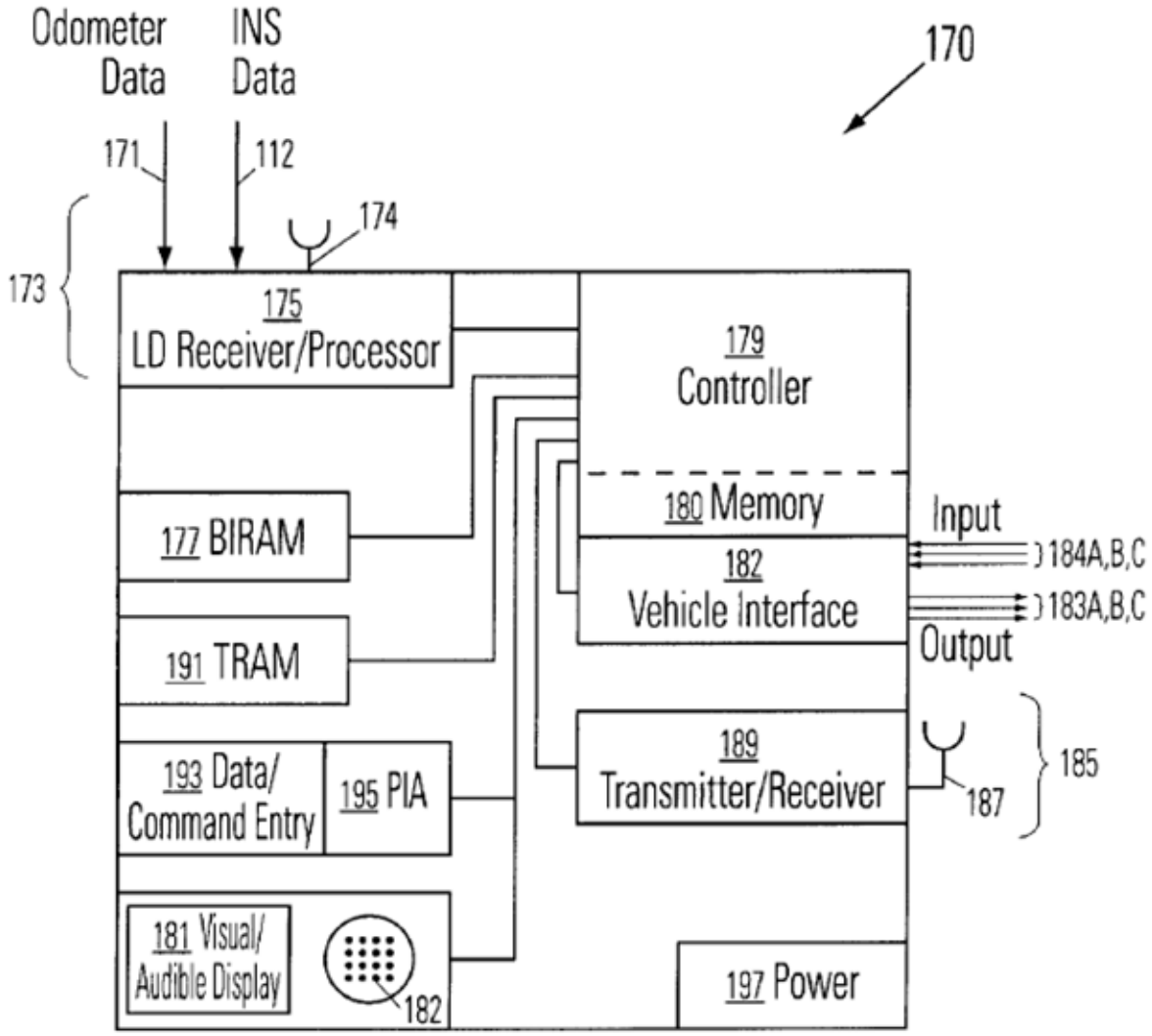
Murphy was filed March 20, 1998 and issued May 1, 2001. Murphy is prior art under at least pre-AIA § 102(b).

Murphy discloses a system that monitors a vehicle, authenticates a driver based on identity indicium (*e.g.*, fingerprint and/or information on a token or smart card) and restricts use within certain operating parameters (*e.g.*, time, location, and/or speed restrictions). (Murphy, Abstract, 2:20-34, 5:18-26.) If restrictions are violated, the system "takes at least one of 12 Control Actions" including disabling the vehicle or reducing speed with a "governor." (*Id.*, 5:29-60.)

Murphy discloses controller module 179 with associated memory module 180, biometric indicium receiving and analysis mechanism (BIRAM 177), token receiving and analysis mechanism (TRAM 191), Location Determination (LD) module 173 to receive location and speed information, vehicle interface 182 which includes a visual/audible display 181 and interface input and output terminals

[1] Dr. Ehsani is an expert in automotive control systems among other things.

184A,B,C and 183A,B,C, and communications module 185 to communicate with an information processing center. (Murphy, 13:27-14:54.)



(Murphy, Fig. 6.)

1. Independent Claim 1

Murphy anticipates or renders obvious claim 1. (Ehsani ¶¶39-48.)

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

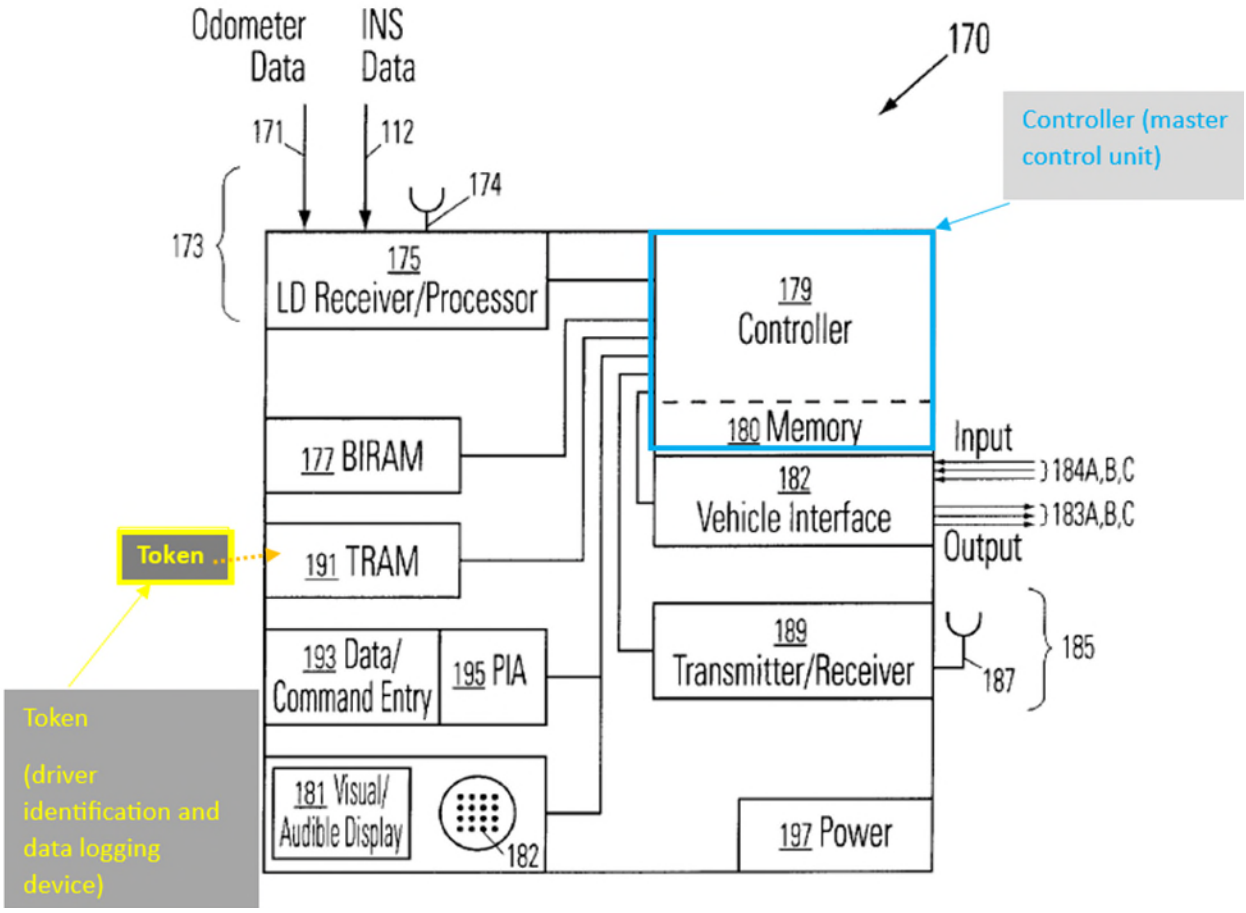
Murphy discloses a driver authentication and monitoring system. (Ehsani ¶39;

Murphy, Abstract; Figs. 6-7.) The system "authenticates" the driver by requiring the driver to provide one or more identity indicium like a "fingerprint" or "personal identification indicium contained on a token or card." (*Id.*) Once this "indicium is satisfactorily presented and analyzed, the system allows operation of the vehicle," and monitors vehicle operation including "operation time and/or mileage" and "location and speed." (*Id.*, Abstract, 11:60-67.) If the vehicle is not being operated as permitted, the system can take "control actions" including disabling the vehicle, reducing speed, or issuing an alarm. (*Id.*, Abstract, 2:20-34, 5:18-60.)

1[A]: ***a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device***

Murphy discloses or renders obvious Claim 1[A]. (Ehsani ¶¶40-44.)

Murphy's system includes a "master control unit" ("**MCU**") in the motor vehicle: "controller module 179." (Murphy, Fig. 6, 4:39-44, 5:13-24, 6:55-59, 15:66-16:11.) Controller module 179 identifies and authenticates a driver via "token receiving and analysis mechanism (TRAM") and "biometric indicium receiving and analysis mechanism (BIRAM)." (Murphy, Abstract, 4:39-44, 5:13-24, 6:55-59, 15:66-16:11, Figs. 2A-6.) The token's pre-programmed information permits the driver to operate the vehicle within an operating profile ("operating restrictions") loaded into controller 179. (Murphy, 6:59-7:14, 14:46-54; Ehsani ¶40.) Thus, the token is a "driver identification and data logging device":



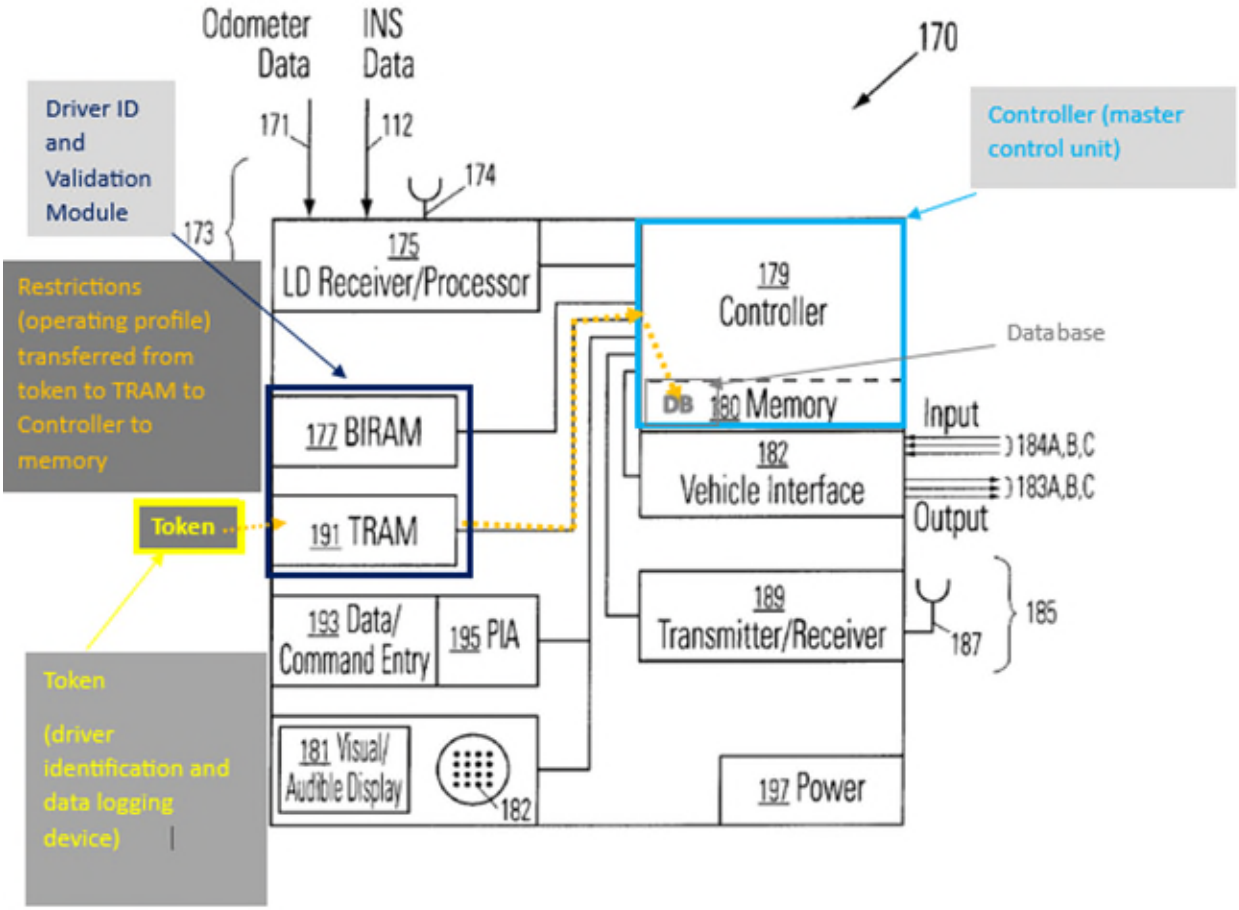
(Murphy, Fig. 6 (annotated).)

The TRAM receives and analyzes a presented token (Murphy, 6:55-7:14, 14:46-54), and the BIRAM receives a driver's biometric indicium. (*Id.*, 13:33-35.) The controller and associated modules receive information from the TRAM and BIRAM to determine the identity of the driver. (*Id.*, 13:35-40, 14:46-54.) Moreover, "[T]he control system either (i) identifies the driver, based on the ident indicium presented, or (ii) determines that the driver cannot be identified, because" *e.g.*, "the ident indicium presented is not in the control system database." (*Id.*, 7:49-63, Fig. 2A; *see also* 10:44-11:27, Fig. 3.)

1[B]: ***wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;***

Murphy discloses or renders obvious Claim 1[B]. (Ehsani ¶¶41-43.)

Murphy's controller 179 receives information regarding at least one driver via the TRAM and BIRAM, with the TRAM token including pre-programmed information permitting the driver to operate the vehicle within an "operating profile" (driver-specific "operating restrictions."). (Murphy, 6:59-7:14, 14:46-54; Ehsani ¶40.) The "token may have built into it a circuit or pre-programmed information in a storage medium that imposes restrictions on the vehicle and/or identifies the token holder." (Murphy, 6:59-62.) This information corresponds to the driver-specific operation profile. (Ehsani ¶40; Murphy, 6:62-7:14.) In addition, restrictions can be loaded or changed remotely via the (tele)communication module. (Murphy, 12:16-27.)



(Murphy, Fig. 6 (annotated).)

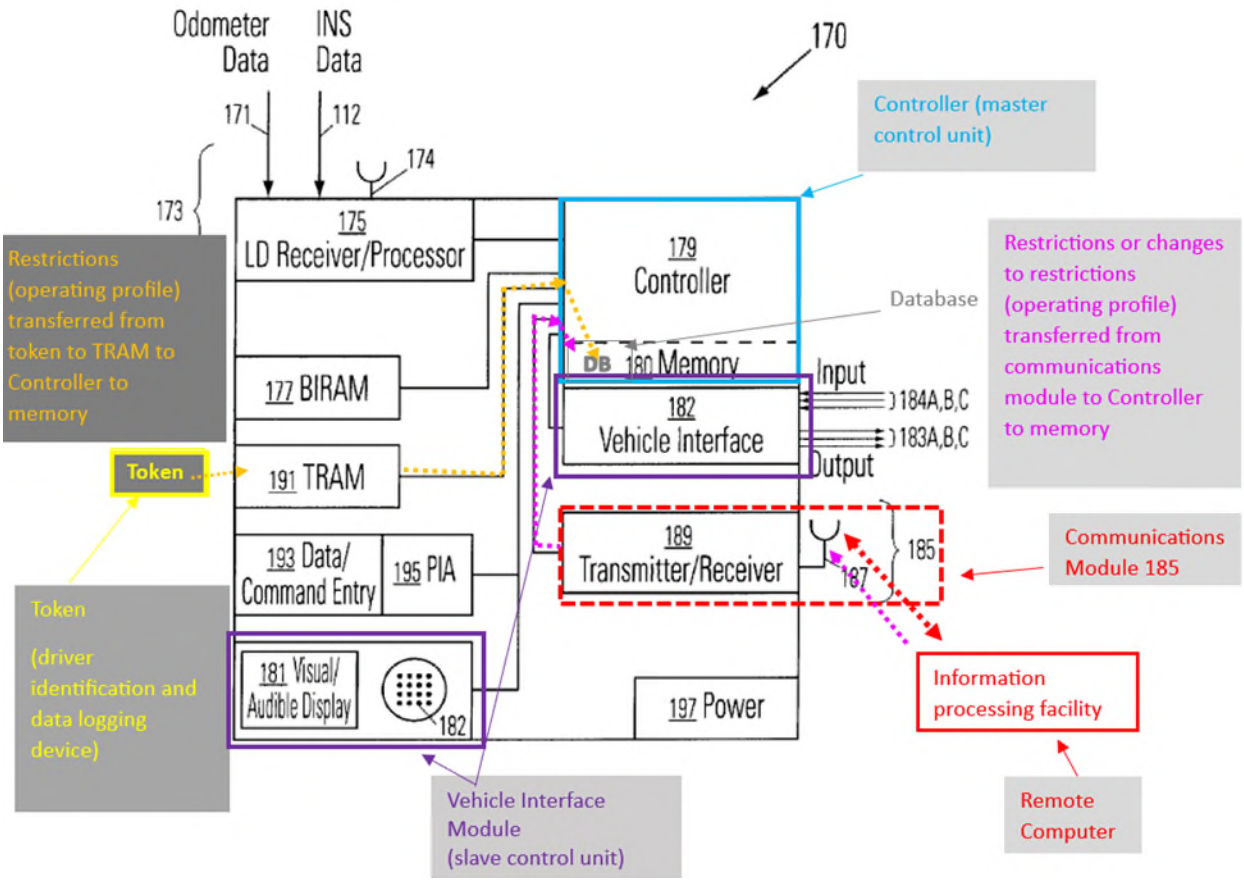
Murphy's controller further receives a "unique identification code" to permit a driver to operate the vehicle within the operating profile, as the token presented may be "specific for the person who presents the token." (*Id.*, 6:55-7:14, 2:20-34, 14:46-54; Ehsani ¶43.) The controller performs a comparison between stored identification indicia and the token to identify and authenticate the driver. (Murphy, 2:35-45, 5:13-17, Figs. 2A-3.) Additionally, the biometric sample must be unique to the driver, and comprises a unique identification code. (*Id.*; *see also* Murphy, 17:63-18:18.)

For authenticated drivers, Murphy allows operation of the vehicle, but only within the operating profile comprising time, location, and/or speed restrictions that can be assigned individually to each driver. (Murphy, Abstract, 5:18-26, 6:8-18, Figs. 2A–5.) For example, Murphy discloses "tak[ing] at least one of 12 Control Actions" when a driver has violated the operating profile restrictions. (*Id.*, 5:29-60, 15:37-42, Figs. 2A-5.)

1[C]: ***a slave control unit in a motor vehicle and in communication with said master control unit, said slave control unit configured to receive commands from said master control unit and to generate at least one of an alarm signal if said at least one driver violates said operating profile unique to said at least one driver thereby providing feedback about said vehicle usage and govern mechanical operations of said vehicle remotely thereby maintaining occupant safety.***

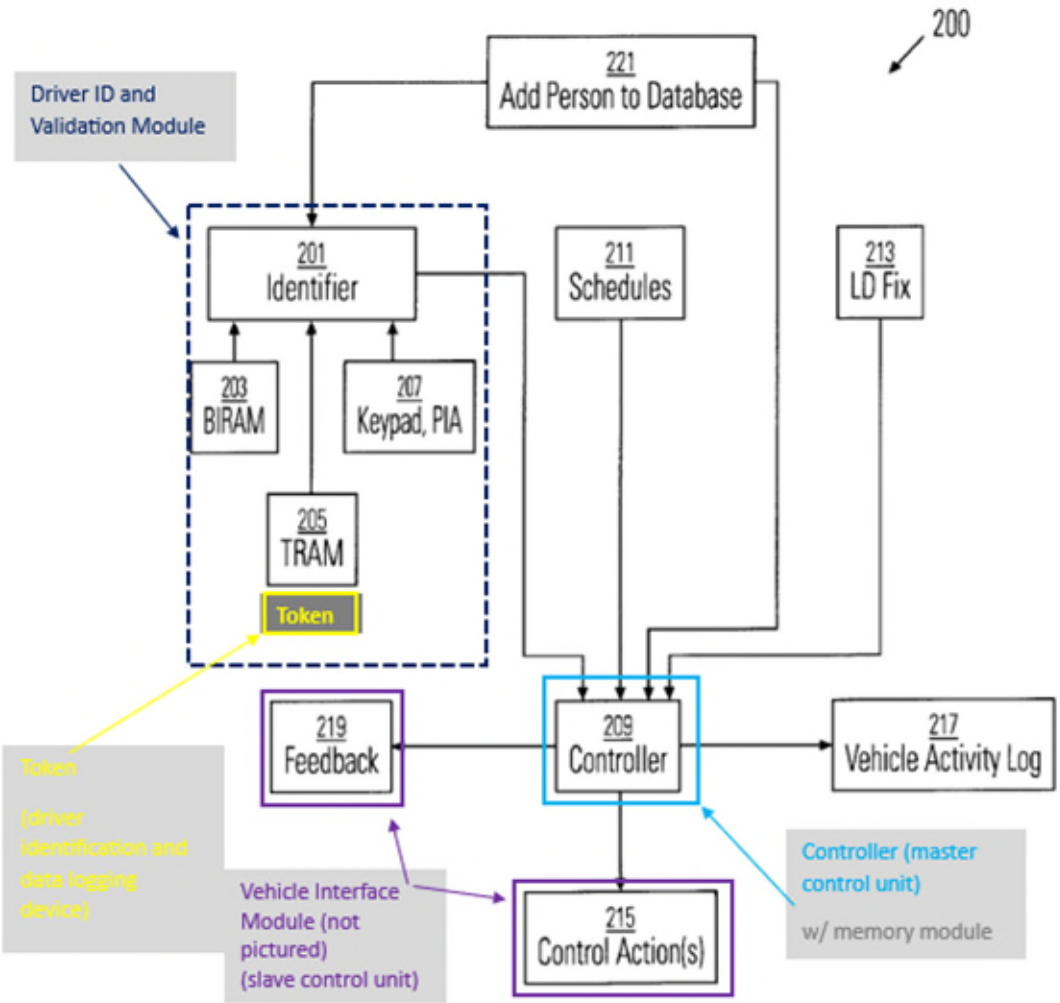
Murphy discloses or renders obvious Claim 1[B] ("**SCU limitations**"). (Ehsani ¶¶44-47.)

Murphy's system includes a vehicle interface module 182 and the Control Action(s) interface module 215, which are both a "slave control unit" ("**SCU**"). (Murphy, 13:66-14:4, 15:32-42, Figs. 6, 7.) Controller 179 (MCU) is in communication with the SCU as it is "connected to a vehicle interface module 182 that is in turn connected to at least one vehicle component … for use in controlling or restricting" vehicle operation. (Murphy, 13:66-14:4, 15:32-42, Figs. 6-7; Ehsani, ¶44.)



(Murphy, Fig. 6 (annotated).)

Further, the Control Action(s) interface module 215 is in communication with the MCU (controller module 209), as "controller module 209 determines which Control Action(s)" "should be imposed on vehicle use and communicates this information to a Control Actions interface module 215 for implementation by the [various systems] on the vehicle." (*Id.*, 14:37-42.) A POSITA would have understood the vehicle interface module 182 and Control Action(s) interface module 215 (collectively, "**Control Action Module**") are the same module because they relate to the same functionality in different figures/embodiments. (Ehsani, ¶44.)

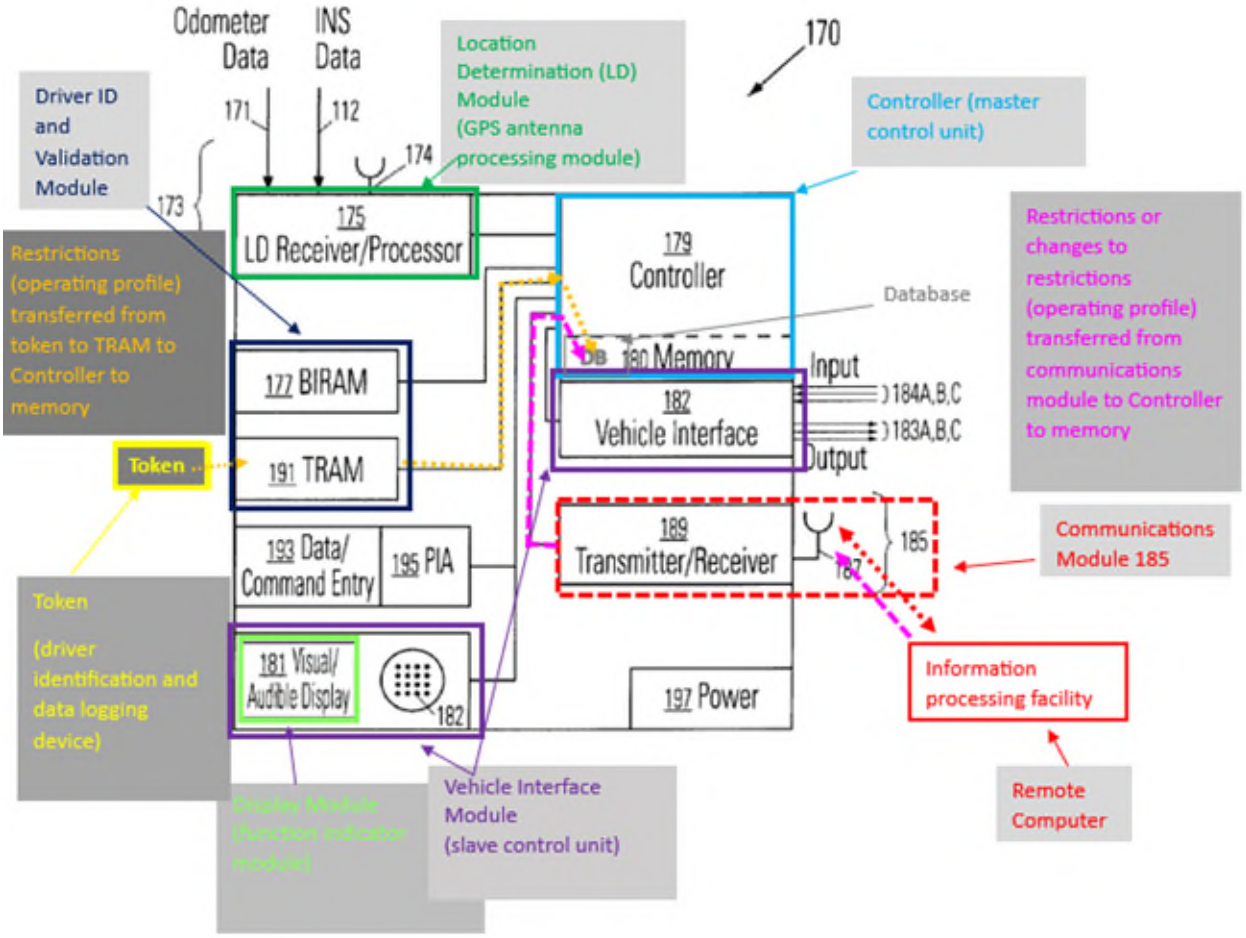


(Murphy, Fig. 7 (annotated).)

The Control Actions Module controls vehicle operation when the driver has violated the operating profile, including through 12 Control Actions. (*Id.*, 5:13-24, Figs. 2A-5.) These 12 Control Actions include generating signals that: "disables the vehicle," "reduces the vehicle speed … ***using a vehicle 'governor'***," turns on lights, flashes, or the horn, activates an audible/visual "on-board alarm," or "transmits an alarm" to a selected facility. (*Id.*, 5:29-54 (emphasis added).) Further, "the controller connects to a display system that audibly announces or visually displays" a violation

announcement and/or that the vehicle will be disabled. (*Id.*, 5:29-60, 10:36-38.)

Controller 209 is programmed with an operating profile (*e.g.*, time, location, and/or speed restrictions) and sends a Control Action, or command, to the Control Action Module when restrictions are violated. (Murphy, 5:18-60, 15:37-42.) The restrictions "can be changed remotely, using the communications module 30." (*Id.*, 12:16-20.)



(*Id.*, Figure 6 (annotated).)

Thus, the Control Action Module is an SCU that is in communication with

and configured to receive commands from the MCU (control module) to generate an alarm (Control Action, *e.g.*, disable or reduce vehicle speed or issue an alarm) if the driver violates the operating profile, thereby providing feedback about vehicle usage and governing mechanical operations of said vehicle remotely (either via the Control Actions Module or via changes to the restrictions via the communications module) thereby maintaining occupant safety. (Ehsani ¶¶44-47.)

2. Independent Claim 11

Murphy anticipates or renders obvious claim 11. (Ehsani ¶¶48-53.)

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

Murphy discloses a driver authentication and monitoring system. (Ehsani ¶40; *see* §VIII.A.1).

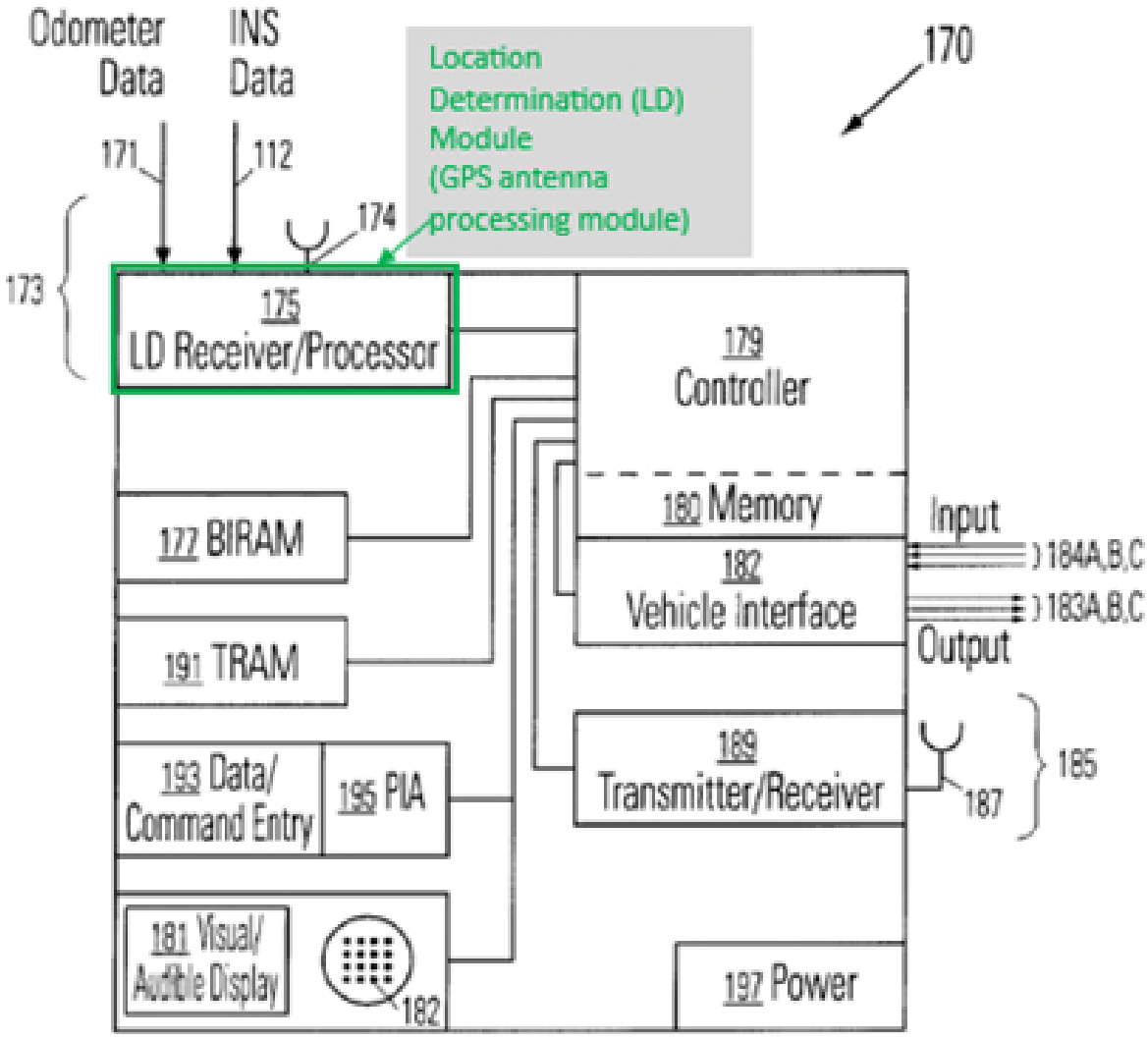
11[A]: ***a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and associating an operating profile with said at least one driver***

Murphy discloses or renders obvious Claim 11[A]. (Ehsani ¶49.) Murphy discloses a controller (MCU) that authenticates a driver via a token (driver identification). (*See* §VIII.A.1.) The controller associates a profile with the driver upon authentication, as each identified driver may be assigned an individual maximum speed, accumulated mileage, accumulated operation time, and/or time intervals for operation. (Murphy, 5:18-26, 6:8-7:14, 14:46-54; Ehsani ¶49.)

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

Murphy discloses Claim 11[B]. (Ehsani ¶50.)

Murphy discloses that "[i]nformation on the present vehicle location and/or vehicle speed" is sent "by the LD [(location determination)] module 173 to the controller module 179" for comparison with vehicle operation restrictions. (Murphy, 13:53-65.) The LD module can be implemented using "GPS" to determine location and speed. (*Id.*, Abstract, 3:48-56.)

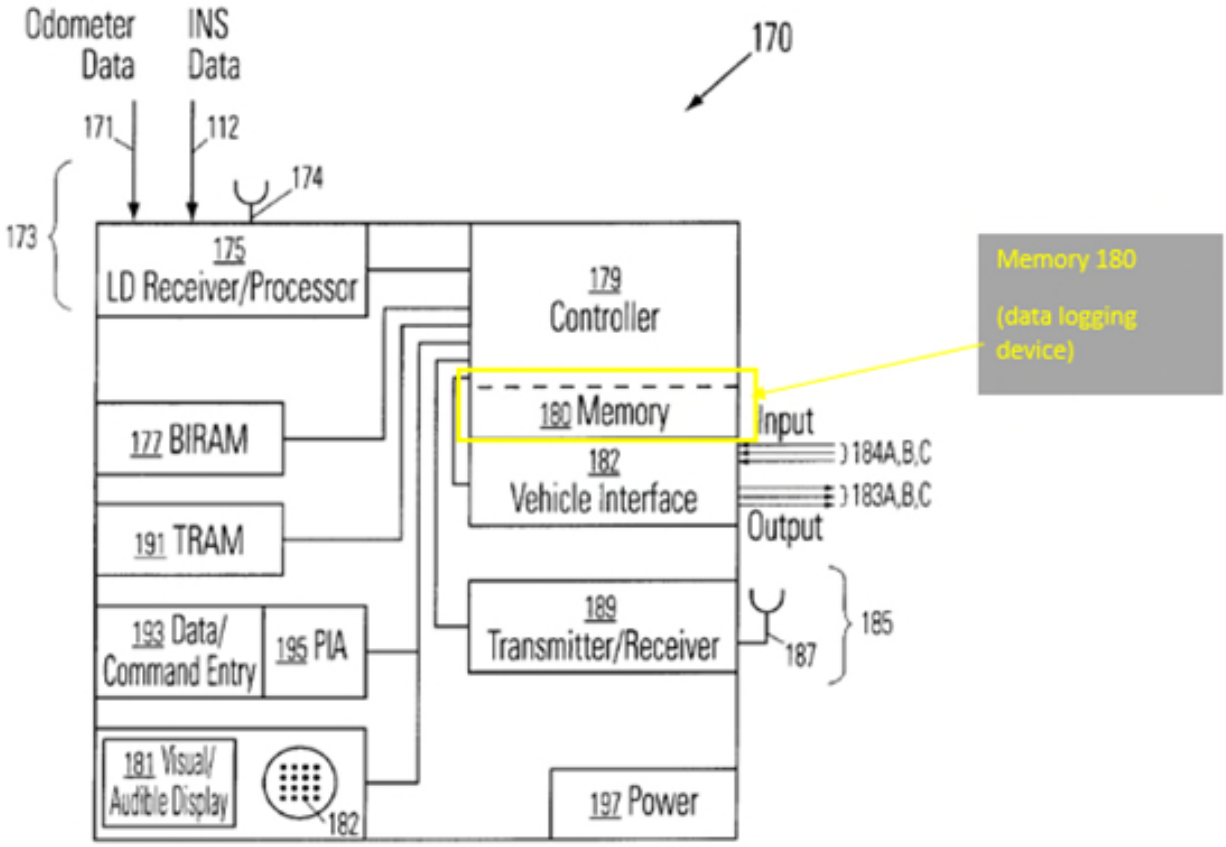


(Murphy, Fig. 6 (Annotated).)

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

Murphy discloses Claim 11[C]. (Ehsani ¶51.)

Murphy discloses "[i]nformation on the present vehicle location and/or vehicle speed" is sent "by the LD module 173 to the controller module 179." (Murphy, 13:53-65.) Murphy's "system can maintain its own operations log, including periodic recording of the present observation time, vehicle location and/or vehicle speed in a memory…." (Murphy, 12:1-3.) This information is recorded to the memory 180 (a data logging device) by LD module (GPS module). (Ehsani ¶51; Murphy, 15:32-16:11; §VIII.A.2.)



(Murphy, Fig. 6 (annotated).)

11[D]: ***a slave control unit in a motor vehicle and in communication with said master control unit, said slave control unit configured to receive commands from said master control unit and to generate an alarm signal if said at least one driver violates said operating profile unique to said at least one driver thereby providing feedback about said vehicle usage and govern mechanical operations of said vehicle remotely thereby maintaining occupant safety;***

Claim 11[D] is a narrowing of Claim 1[C], merely removing the phrase "at least one of." Murphy therefore discloses Claim 11[D] for the same reasons *supra*, §VIII.A.1. (Ehsani ¶52.).

11[E]: ***wherein master control unit permits said at least one driver to operate said vehicle within an operating profile if said master control unit receives at***

least one of a unique identification code to permit said at least one driver to operate said vehicle within an operating profile and said at least one driver has not violated said operating profile.

Murphy discloses or renders obvious Claim 11[E]. (Ehsani ¶53.) Murphy's controller (MCU) compares encoded driver-specific information received from the token and/or biometric sample (unique identification code) with stored identification indicia to identify and authenticate the driver. (*See* §VIII.A.1). Once authenticated, the controller allows the driver to operate within the operating profile described above when the driver has not violated those restrictions. (Murphy, 5:18-18; Ehsani ¶53.)

3. Independent Claim 15

Murphy anticipates or renders obvious claim 15. (Ehsani ¶¶54-59.)

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

Murphy discloses a method of authenticating and monitoring drivers. (Ehsani ¶54; §VIII.A.1).

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

Murphy discloses or renders obvious Claim 15[A]. (Ehsani ¶55.) Murphy provides a vehicle with a driver authentication and monitoring system, as it includes a vehicle with controller 179 connected to TRAM 191 and BIRAM 203 that identify and monitor drivers. *See supra,* §VIII.A.1 (Claim 1[A]).

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

Murphy discloses Claim 15[B]. (Ehsani ¶56.) Murphy discloses pre-programming information in the TRAM token, including operating restrictions, and loading the same into controller 179, thereby programming the driver authentication and monitoring system with an operating profile associated with a high risk driver. (*See* VIII.A.1). Moreover, Murphy specifies that the operating restrictions can be for a high risk driver, *i.e*, "teenager or other inexperienced driver." (Murphy, 11:60-67.)

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

Murphy discloses Claim 15[C]. (Ehsani ¶57.) Murphy's disclosure of the token presented to the TRAM constitutes authenticating said high risk driver and enabling operation within said operating profile. (*See* VIII.A.1). Murphy's disclosure of monitoring operation and sending a control action when a restriction is violated constitutes monitoring operation of said motor vehicle to determine if said high profile driver is violating said operating profile. (*Id.*)

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

Murphy discloses Claim 15[D]. (Ehsani ¶58.) Murphy discloses generating a Control Action alarm signal (*e.g.*, signal to disable or slow the vehicle, or to transmit alarm) if the high-risk driver violates driver-specific restrictions (operating profile). (*See* VIII.A.1).

15[E]: ***governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.***

Murphy discloses Claim 15[E]. (Ehsani ¶59.) Murphy discloses generating a Control Action to govern mechanical operation of the vehicle, including to disable or slow the vehicle (remotely at least when restrictions are changed via the communications module) when the driver violates restrictions (operating profile) thereby maintaining occupant safety. (*See* VIII.A.1).

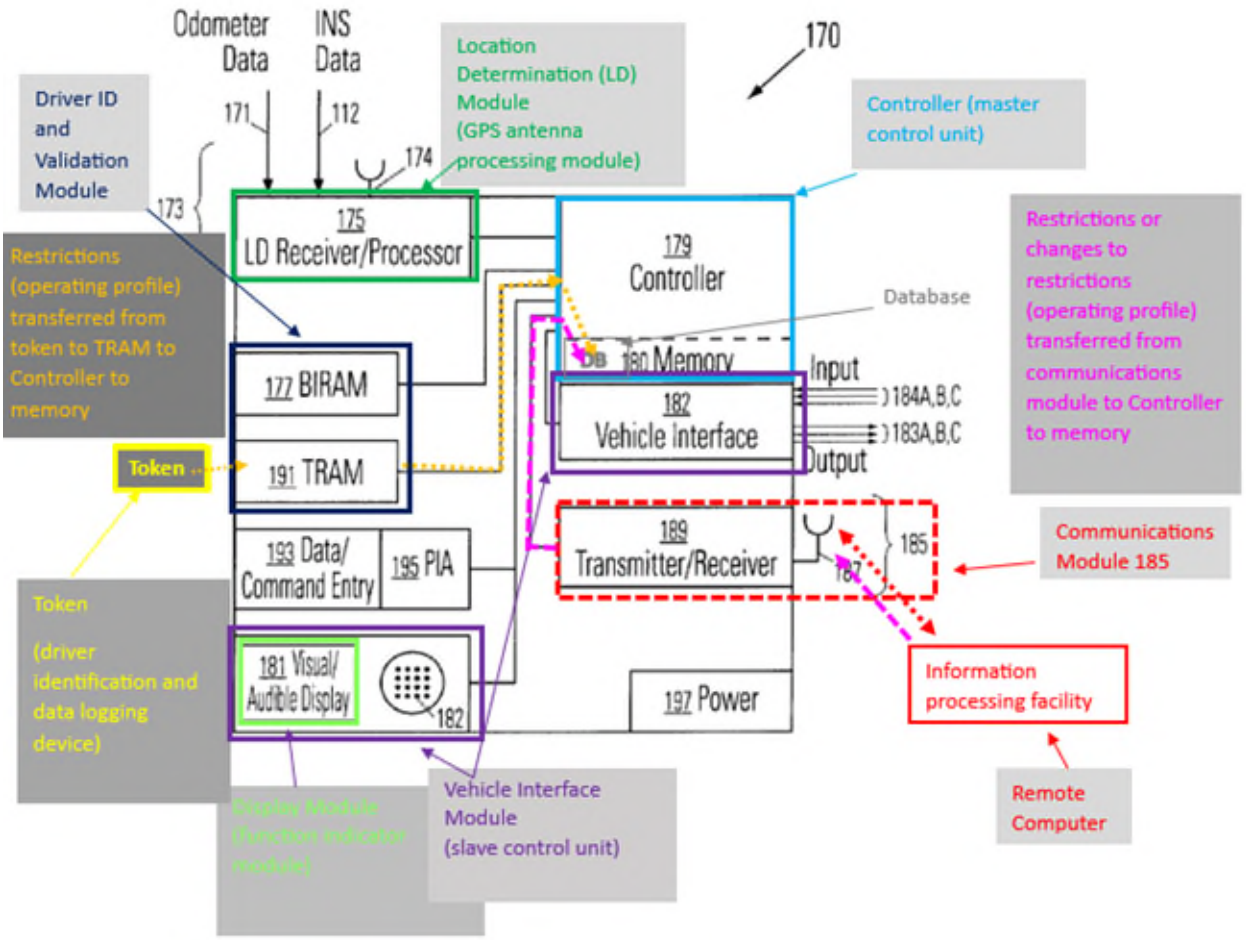
4. Claim 2

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, said program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, said program module accessed by said authorized user via a network utilizing a remote computer.***

Murphy anticipates or renders claim 2 obvious. (Ehsani ¶60.)

Murphy's system includes a database (in memory 180) with information for each authorized driver including various operating parameters. (Murphy, 15:15-21, 15:66-16:9.) These parameters "can be changed remotely" via the communications module. (*Id.*, 12:16-27; Fig. 6.) The telecommunication module is part of apparatus 170, and an information processing facility can transmit signals that modify operation restrictions, and that allow downloading of commands that alter restrictions on present location, speed and/or present time, accumulated operating time and accumulated milage items that determine when operation restrictions are imposed. (*Id.*, 14:27-35.) A POSITA would have understood the facility includes a

computer remote from the vehicle that transmits the information over a network. (Ehsani, ¶60.)



(Murphy, Fig. 6 (annotated).)

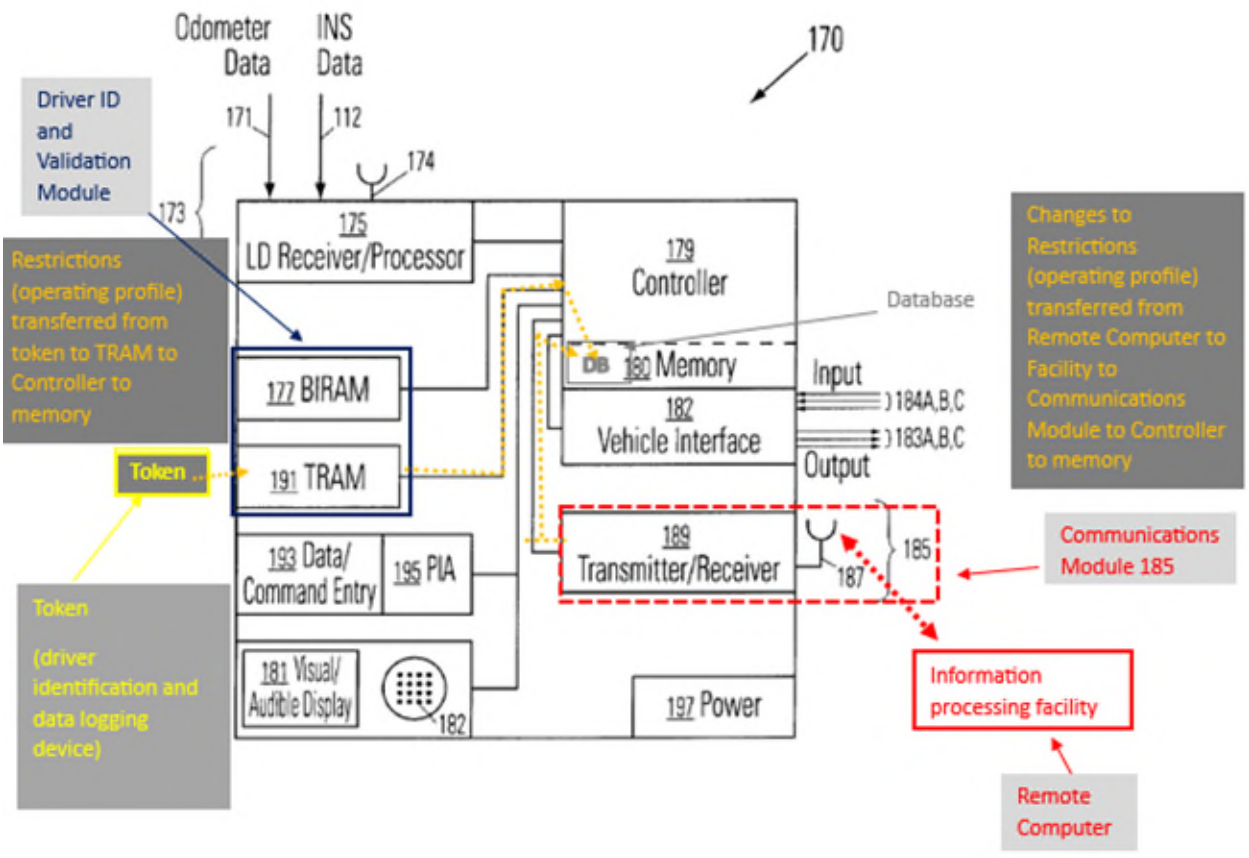
5. Claim 3

3: ***The driver authentication and monitoring system of claim 1, wherein said driver identification and data logging device in conjunction with a remote computer load said operating profile for said at least one driver.***

Murphy discloses or renders obvious Claim 3. (Ehsani ¶61.)

Murphy teaches that operating parameters can be loaded or changed remotely via the (tele)communication module. (Murphy, 12:16-27; Fig. 6; *see also* §VIII.A.2.)

Further, the token includes a circuit identifying the token holder and imposing restrictions on vehicle operation. (*Id.*, 6:55-7:14.) These parameters, which can be changed remotely via the communications module after being loaded from the token or previously transmitted through the communications module, may be stored in the database in memory 180. (*Id.*, 14:46-54, 15:66-16:11; *see* §VIII.A.1; Ehsani ¶61.) Thus, the token (driver identification and data logging device) loads the operating profile (restrictions from token and from the communication module) to the controller in conjunction with a remote computer. (*Id.*)



(Murphy, Fig. 6 (annotated).)

6. Claim 4

4: ***The driver authentication and monitoring system of claim 1, further comprising a driver identification and validation module; a GPS antenna processing module; a memory module; and a function indicator module.***

Murphy anticipates or renders claim 4 obvious. (Ehsani ¶¶62-65.)

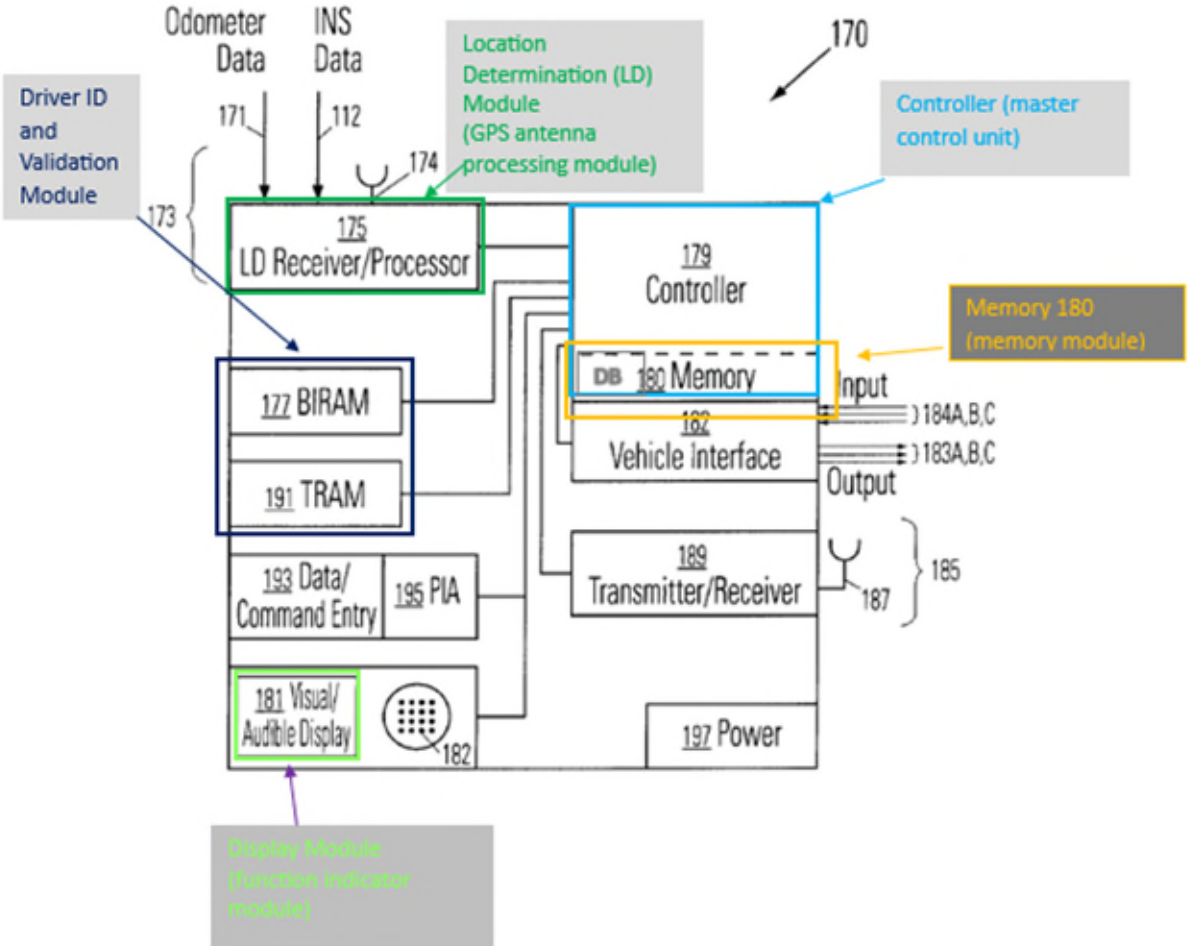
Murphy discloses a driver identification and validation module, as it includes an MCU (controller) with programming for authenticating a driver via a token. (*See* §VIII.A.1.) The system includes a software module that identifies and validates a driver based on indicium presented through the TRAM and/or BIRAM. (Ehsani ¶62.)

Murphy discloses a GPS module (LD module) that includes a GPS antenna module, as it incudes "an LD signal antenna" and "an LD signal receiver/processor." (Murphy, Abstract, 3:48-63; *see also* §VIII.A.2(11[B]).

Murphy discloses a memory module in the controller with a database of identities and matching indicia for drivers, and operating restrictions. (Murphy, 13:35-40, 15:15-21, 15:66-16:9.) Murphy further teaches vehicle restrictions can be stored in a schedule module (connected to the controller). (*Id.*, 15:21-31, 16:9-11; Ehsani ¶64.)

Murphy discloses a function indicator module, as the controller optionally "connects to a display system that audibly announces or visually displays an

announcement that a violation has occurred and/or that the vehicle will become disabled within a selected time interval." (Murphy, 5:55-60, 13:61-65.) This requires a module to, as stated in the '101 Patent, "monitor various functions in association with the vehicle" to generate the audible/visual alert. ('101, 7:53-56; Ehsani, ¶65; Murphy, 14:7-17 (input terminals 184A-C for monitoring vehicle components).)



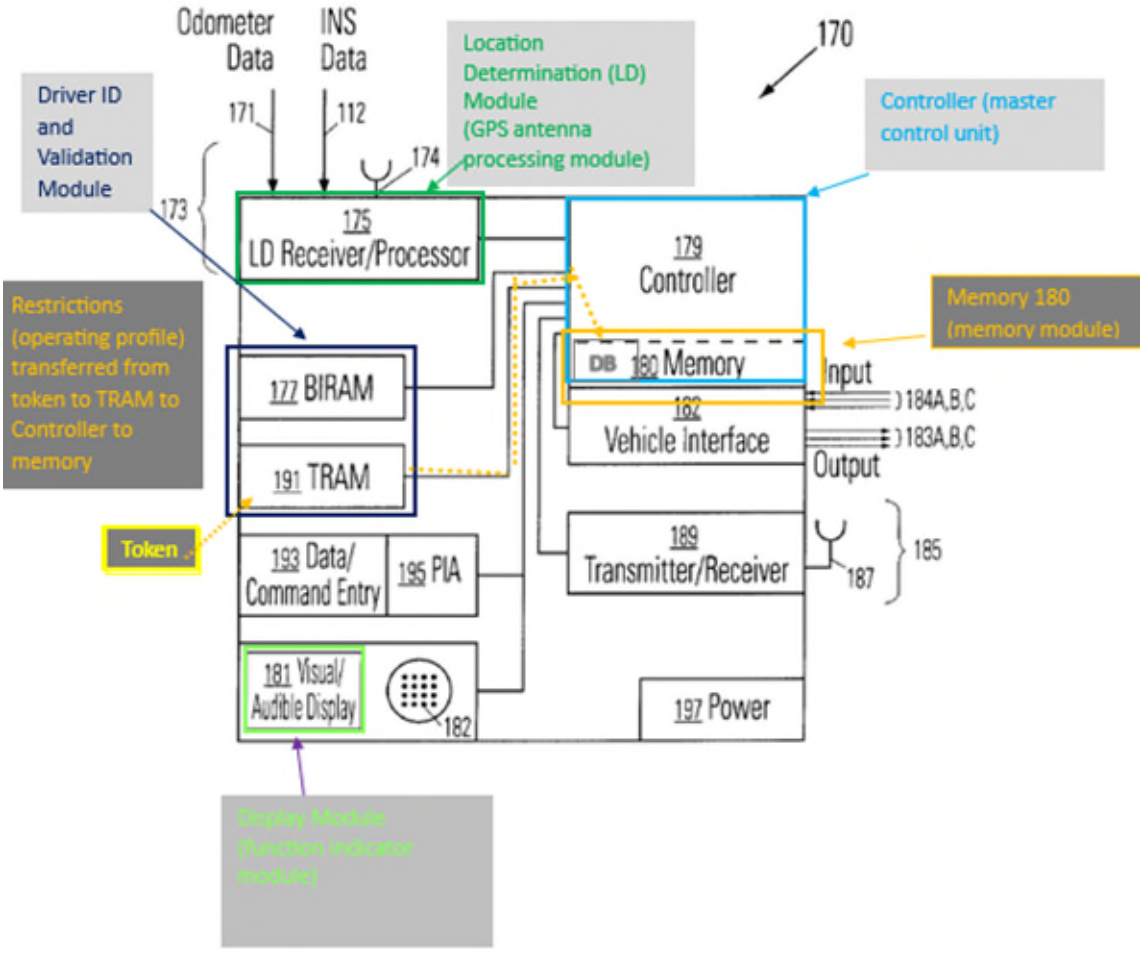
(Murphy Fig. 6 (annotated)

7. Claim 5

5: ***The driver authentication and monitoring system of claim 4, wherein said operating profile is loaded into said memory module for enabling operation of said vehicle when said at least one driver is authenticated.***

Murphy anticipates or renders claim 5 obvious. (Ehsani ¶66.)

The operating profile is loaded into Murphy's memory (*see* Claim 4, *supra*) upon authenticating a driver via BIRAM 177 or schedule module 211. (Murphy, 13:35-40, 15:15-21, 16:9-11; *See also* Ehsani ¶64.)



(Murphy, Fig. 6 (annotated).)

8. Claim 6

6: ***The driver authentication and monitoring system of claim 4, wherein said GPS antenna processing module provides location information in association with said vehicle.***

Murphy anticipates or renders claim 6 obvious. (Ehsani ¶67.) Murphy discloses a GPS antenna processing module (LD Module), which provides information on vehicle location. (Murphy, Abstract, 3:48-63, 13:53-65; *see* §VIII.A.6.)

9. Claims 7 and 12

7/12: ***The driver authentication and monitoring system of claim [1/11], wherein said slave control unit further comprises a power regulator module; a starter relay module; a definable relay module; a slave microcontroller[;/,] and an alarm synthesizer.***

Murphy renders obvious claims 7 and 12, which add only conventional, well-known components. (Ehsani ¶¶68-74.) As discussed for the SCU limitations, Murphy discloses a Control Action Module (SCU). Murphy also teaches that power supply 197 "supplies power to operate one or more of the components of the apparatus 170." (Murphy 14:66-67.) A POSITA would have been motivated to include a power regulator in the Control Action Module to regulate a power source for the vehicle to implement the Control Actions. (Ehsani ¶68; *see also* Murphy, 13:66-17:4.)

Murphy discloses or renders obvious a starter relay in the Control Action Module. (Ehsani ¶69.) Murphy teaches that "the vehicle may require insertion or

presentation of a token or smart card" "in order for the vehicle to be activated or 'started.'" (Murphy, 6:55-59, 8:10-14.) This is consistent with the starter relay 526 in the '101, which can be enabled by a starter engine signal from the MCU when the driver is authenticated. ('101, 8:7-10; Ehsani ¶60.) A POSITA would recognize that this function in Murphy requires a starter relay in the Control Action Module. (*Id.*)

Murphy discloses or renders obvious a definable relay module in the Control Action Module. (Ehsani ¶70.) The Control Action Module is connected to one or more vehicle components, and that the controller communicates vehicle operation to a vehicle activity log module. (Murphy, 13:67-14:17, 15:42-46.) A POSITA would have understood this to include that the Control Action Module receives information from vehicle components and relays that information to the controller, which in turn relays the information to the activity log module. (Ehsani, ¶70.) A POSITA would recognize this to require a definable relay module as claimed by the '101. (*Id.*; *see* '101, 7:59-61, 8:16-18, FIG 6 (definable relay 524 in the SCU receives information from Breathalyzer pin 542 to provide status regarding alcohol consumption).

Murphy renders obvious that the SCU comprises a slave microcontroller. (Ehsani ¶71.) Murphy's Control Action Module connects to various components to control vehicle operation. (Murphy, 13:66-14:4.) The Control Action Module optionally connects to interface input and output terminals and data can be provided according to serial data communications standards between microcomputers in a

vehicle. (*Id.*, 14:4-17.) A POSITA would have understood this to require the interface module to comprise a microcontroller, or alternatively, it would have been obvious to implement the Control Action Module with a microcontroller because it would involve merely selecting from one of a finite number of ways to implement the Control Action Module (*e.g.*, with a microcontroller or a microprocessor). (Ehsani ¶71.).

Murphy discloses or renders obvious that the SCU (Control Action Module) comprises an alarm synthesizer. (Ehsani ¶72.) As discussed for the SCU limitations, Murphy's controller (MCU) is connected to the Control Action Module which is in turn connected to vehicle component(s) (*e.g.* engine) for use in controlling vehicle operation. (Murphy, 13:66-14:4.) The Control Action Module receives a Control Action from the controller and generates an alarm (Control Action, *e.g.*, reduce vehicle speed using governor). (*Id.*, 15:37-42.) Additionally, Murphy's Control Action Module includes a "Visual/Audible Display 181" and/or a "feedback module 219" for visual or audible alerts to the driver. (*Id.*, 13:60-65,15:47-50, Figs. 6, 7.)

Alternatively, it would have been obvious to implement the feedback functionality into the Control Action Module to provide feedback in response to Control Action messages from the controller without requiring an additional message to the controller to be forwarded to the display. (Ehsani ¶72.)

Thus, Murphy renders obvious that the SCU comprises a power regulator

module, a starter relay module, a definable relay module, a slave microcontroller, and an alarm synthesizer.

10. Claims 8 and 13

8/13: ***The driver authentication and monitoring system of claim [1/11], wherein said [operating profile comprises] at least one operating parameter [comprises / including] at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.***

Murphy anticipates or renders claims 8 and 13 obvious. (Ehsani ¶75.) As discussed for the MCU and SCU limitations and claim 2, Murphy teaches that the system includes a database with information for each authorized driver, including a maximum allowable vehicle speed (inherent in the allowable speed range), locations, and hours of operation. (Murphy, 15:15-21, 15:66-16:9.)

11. Claims 9, 14, 17, 18

9/14: ***The driver authentication and monitoring system of claim [1/11] wherein said slave control unit generates an alarm signal for [remotely] alerting said authorized user when said at least one driver violates said operating profile.***

17/18: ***The method of authenticating and monitoring drivers in claim [15/16], wherein said step of generating an alarm signal includes providing an alarm remotely to an authorized user.***

Murphy anticipates or renders obvious claims 9, 14, 17, and 18. (Ehsani ¶76.) As discussed for the SCU limitations, Murphy discloses or renders obvious that the SCU (Control Action Module) is configured to generate an alarm signal (*e.g.*, Control Action to reduce speed using governor) if the driver violates the operating profile (*e.g.*, speed restriction). (Murphy, 5:18-60, 15:37-42.) One such Control

Action includes "transmit[ting] an alarm (optionally silent) to a selected facility that is spaced apart from the vehicle." (*Id.*, 5:43-45, 14:23-27.) A POSITA would have understood that the "selected facility" is limited to authorized users, or alternatively would have been motivated to limit access for privacy concerns. (Ehsani ¶76.)

12. Claim 10

10: ***The driver authentication and monitoring system of claim 1, wherein said driver identification and data logging device comprises one of: a radio frequency identification device; and a USB compatible device.***

Murphy anticipates or renders obvious claim 10. (Ehsani ¶77.) Murphy teaches that the vehicle may require "insertion or ***presentation*** of a token or smart card," and a POSITA would have understood that "presentation" implies the use of a radio frequency identification device ("**RFID**") which were commonly implemented in tokens or smart cards for automobiles before the '101. (*Id.* ¶77; Murphy, 6:55-59; Benco (EX1010) at [0002] – [0003].) Further, it would be trivial for a POSITA to implement the token using a RFID, as it would involve merely selecting from one of a finite number of known and commonly used techniques. (*Id.*, ¶77.)

13. Claim 16

16: ***The method of authenticating and monitoring drivers in claim 15, wherein said motor vehicle includes a GPS module and said monitoring operations of said motor vehicle further comprises obtaining GPS data including motor vehicle speed and location.***

Murphy discloses claim 16 for the reasons discussed in §VIII.A.2(11[B]).

14. Claims 19 and 20

19/20: ***The method of authenticating and monitoring drivers in claim [15/16], wherein said step of generating an alarm signal includes providing a control signal that limits functionality within said motor vehicle.***

Murphy anticipates or renders claim 19 and 20 obvious. (Ehsani ¶79.) As discussed for the SCU limitations, Murphy's Control Actions module generates alarm signals that provide a control signal to limit functionality within the motor vehicle, as the Control Actions include reducing vehicle speed using a governor (limiting functionality within the vehicle to cause the speed to be reduced to a selected range) and disabling accessories (thereby limiting their functionality within the vehicle). (Murphy, 5:28-60, 15:37-42.)

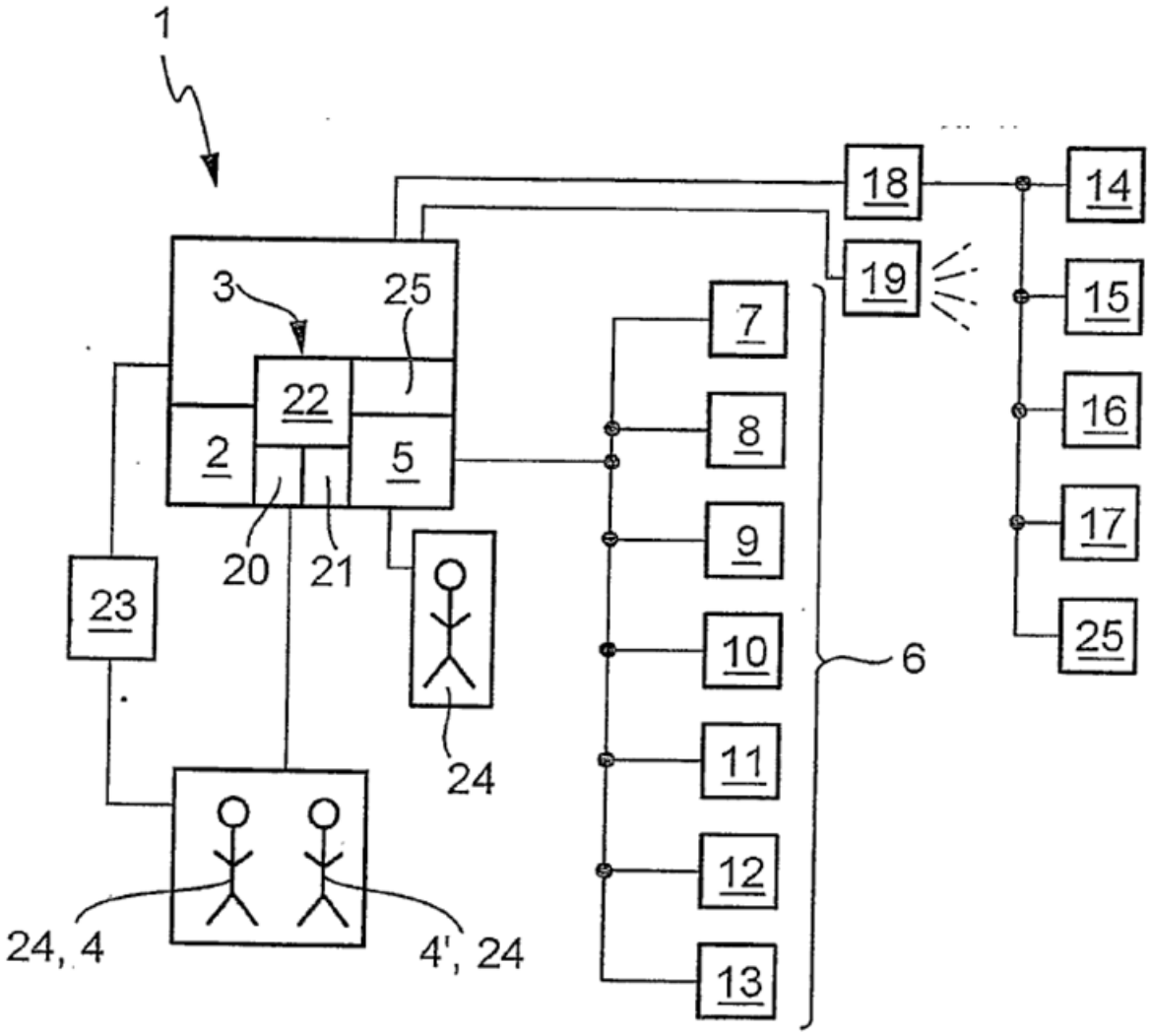
B. Ground 2 – Murphy-Schanz Render Obvious Claims 1-20

Murphy in view of Schanz renders claims 1-20 obvious. (Ehsani ¶¶69-96.)

Schanz was filed May 24, 2003, and published on December 9, 2004. Schanz is prior art under at least pre-AIA § 102(a) and (b).

Schanz discloses a vehicle control system (device 1) to adjust driving dynamic characteristics of a vehicle to the driving skills of a respective driver to increase driver safety. (Schanz, [0001]-[0006]; Fig. 1.) Like Murphy's controller, Schanz's "device 1" identifies and authenticates a driver and provides driver-specific parameters. (*Id.*, [0018], [0020].) As seen in Fig. 1, Schanz's "device 1" includes a "recognition device 3" that identifies a driver based on "person-specific

characteristics" using "a biometric recognition unit," "an acoustic recognition unit 21," and/or "a reading device" "for recognizing an identification code 22." (*Id.*, [0018].) Subcomponents of "device 1" "check[] whether special vehicle parameters 6 are stored for the respective driver." (*Id.*, [0020].) These parameters include restrictions like "maximum vehicle speed," "maximum distance 12 to the vehicle driving ahead," and "intervention parameter of a dynamic vehicle stabilization system." (*Id.*, [0019].) The "device 1" detects "exceeding of the set vehicle parameters 6" and responds with warnings or other interventions. (*Id.*, [0022], [0025].)



(Schanz, Fig. 1.)

1. Motivation to Combine

It would have been obvious to combine Murphy with Schanz, which disclose complimentary methods for driver authentication and monitoring. (Ehsani ¶¶83-87; Murphy, Abstract, 2:20-3:4, 5:13-6:17, 6:55-7:14; Schanz, Abstract, [0006] – [0010], [0017] – [0027].)

A POSITA would have looked to Schanz to improve Murphy given their

similarities and benefits. (Ehsani, ¶85.) The combined system would provide more flexibility for both the driver and the administrator (*e.g*. vehicle owner), enabling a driver to use a wireless token to start the vehicle (*see* Schanz, [0018]) and providing the administrator with additional options for driver-specific restrictions (*see* Schanz, [0020]) that when violated could allow for various alerts and vehicle control options (Murphy, 5:13-6:18). (Ehsani, ¶85.) For example, based on driver-specific parameters (*e.g*., speed limit) provided wirelessly from the token and/or from the administrator (*e.g*., parent), a vehicle can alert the driver and the remote administrator and control the vehicle (*e.g*., lower speed) to improve driver safety. (*Id*.)

A POSITA would have been motivated to combine the functionalities of Murphy and Schanz, including, *e.g*., using Schanz's identification code, driver-specific vehicle restrictions, and transmitting/receiving via radio signals with Murphy's token, controller, and Control Action Module, to improve vehicle occupant safety, as both Murphy and Schanz suggest, (*see* Murphy, 1:9-35, 11:60-67; Schanz, [0004], [0012]), while providing the flexibility for authentication and customizability that Schanz suggests, (*see* Schanz, [0017] – [0018], [0020]). (Ehsani ¶86.)

Combining Murphy and Schanz would have been nothing more than the simple combination of known elements to obtain predictable results and/or simple

substitution of known elements for others, which a POSITA would expect would be successful. (Ehsani ¶87.) For example, the combination of Schanz's identification code, driver-specific restrictions, and use of radio signals with Murphy's token would have yielded the predictable result of a system that allows the system to identify and authenticate a driver without mechanical interaction of the token and to notify the driver and administrator when restrictions are violated. (*Id.*) This would merely use known techniques for identification, authentication, and vehicle monitoring to improve Murphy to provide more granular vehicle safety controls. (*Id.*) A POSITA would have had a reasonable expectation of success in this combination because both disclose vehicle units (Murphy's controller and Control Action Module and Schanz's device 1) that serve analogous functions and operate in similar ways to improve driver safety. (*Id.*) A POSITA would have understood that features of Schanz's "device 1" can be easily applied to Murphy's controller and Control Action Module, and vice-versa, with a reasonable expectation of success in doing so. (*Id.*)

2. Independent Claims (1, 11, 15)

Murphy in view of Schanz renders claims 1, 11, and 15 obvious. (Ehsani ¶¶88-108.)

a. Preambles (1[P]/11[P]/15[P])

Murphy in view of Schanz discloses a driver authentication and monitoring

system and method. (Ehsani ¶89.) Murphy discloses a driver authentication and monitoring system and method. (*See* VIII.A.1,2,3). Similarly, Schanz discloses a driver authentication and monitoring system and method using a "recognition device (3)" to identify a driver, an "assignment device" to check "whether special vehicle parameters" (*e.g*. "maximum vehicle speed"), "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Ehsani ¶89; Schanz, Abstract, [0019]-[0020], [0024]-[0025].)

b. Master Control Unit (1[A]/11[A],[E]/15[A-C])

Murphy in view of Schanz renders obvious the MCU limitations. (Ehsani ¶¶90-92, 98, 102, 104-106.) As discussed in Ground 1, Murphy discloses a controller (MCU) which uses a token (driver identification and data logging device), associates an operating profile with the driver, and permits vehicle operation within the operating profile. (*See* §VIII.A.1,2,3, Murphy, 5:55-7:14; Ehsani ¶90.)

Further, it would have been obvious to integrate Schanz's vehicle parameters (*see* §VIII.B.1) into Murphy's token and controller. Like Murphy's controller, Schanz's "device 1" detects "exceeding of the set vehicle parameters 6" and responds with warnings or other interventions. (*Id*., [0022], [0025].) A POSITA would have been motivated to modify Murphy's token to include Schanz's vehicle parameters and Murphy's controller to include Schanz's interventions for violations of the vehicle parameters, as Schanz's "device 1" and Murphy's controller serve

analogous functions, operate in similar ways, and serve similar goals of improving driver safety. (*See* §VIII.B.1; Ehsani ¶91.) This system would have operated in the same manner such that an authenticated driver could operate the vehicle so long as the driver-specific vehicle parameter restrictions have not been violated. (*Id.*)

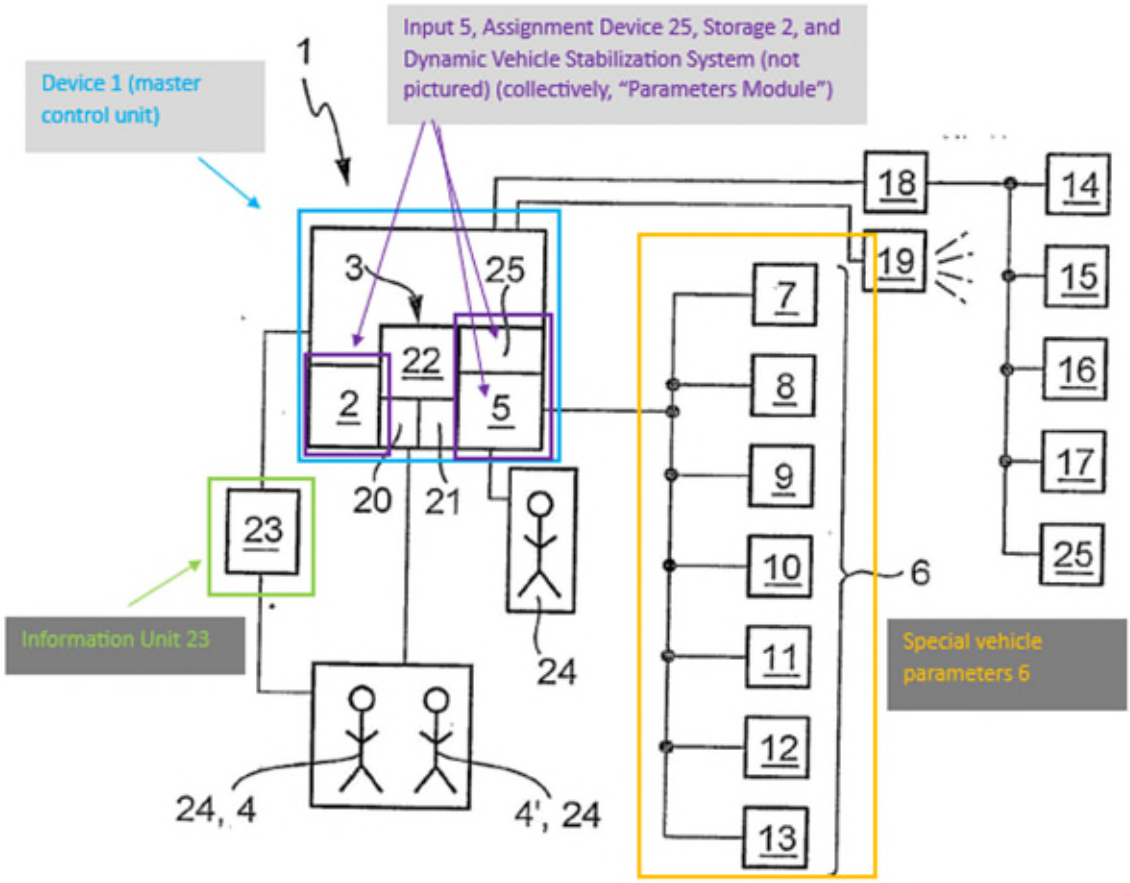
Further, Schanz discloses receiving a unique identification code in that "recognition device 3" within "device 1" may include "a reading device…for recognizing an identification code 22." (Schanz, [0018].) A POSITA would have recognized the advantage of integrating Schanz's identification code functionality in Murphy's controller to receive and recognize a driver-specific identification code. (Ehsani ¶92.) A POSITA would have been motivated to implement this combination to achieve Murphy's goal of identifying and authenticating the individual driver based on the token. (*Id.*; Murphy, 6:55-7:14.) A POSITA would have had a reasonable expectation of success in this combination for the reasons discussed in §VIII.B.1. Further, the modified system would have operated in the same manner such that information read from the token (including Schanz's identification code) is used to authenticate the token-holder. (Ehsani ¶92.)

c. Slave Control Unit (1[B]/11[D]/15[D-E])

Murphy in view of Schanz renders obvious the SCU limitations. (Ehsani ¶¶93-96, 101, 105.) As discussed in Ground 1, Murphy's controller (MCU) connects to a Control Action Module (SCU). (*See* VIII.A.1,2,3, Murphy, 13:66-14:4, 14:37-42,

Fig. 6, 7.) Alternatively, it would have been obvious to a POSITA to implement both the functionalities of Schanz's input 5, assignment device 25, storage device 2, and dynamic vehicle stabilization system (collectively, "**Parameters Module**") and Schanz's information unit into Murphy's Control Action Module. (Ehsani ¶93.)

Like Murphy's Control Action Module, Schanz's Parameters Module is connected to and receives commands from device 1 (MCU) to "adjust[]" "driving dynamic characteristics" to enforce driver-specific "vehicle parameters 6," *e.g.*, "maximum vehicle speed." (Schanz, [0019]-[0020]; *see also* §VIII.B.1.) For example, "device 1" can "adjust[]," or control, a "dynamic vehicle stabilization system" to cause it to "actively intervene in driving operation of a beginner 'earlier' ... to alert the beginner to critical driving situations." (*Id*., [0022].) In addition, Schanz discloses an "information unit 23" which "emits suitable optical and/or acoustic warning signals when the set vehicle parameters 6 are exceeded." (Schanz, [0025].) Schanz depicts "information unit 23" as external to but connected to "device 1." (Schanz, Fig. 1.) This indicates that "device 1" communicates with "information unit 23," *e.g.*, to cause it to generate an alarm when "device 1" detects violation of a "vehicle parameter." (Ehsani ¶94.)



(Schanz, Fig. 1 (annotated).)

The combined Murphy-Schanz system integrating Schanz's Parameters Module and information unit with Murphy's Control Action Module would have a SCU for governing vehicle operations remotely and generating an audible alarm. For the reasons discussed in VIII.B.1, a POSITA would have been motivated to combine these features from Schanz with Murphy's Control Action Module, as Schanz's Parameters Module and Murphy's Control Action Module serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety by generating an alert when vehicle parameters are violated. (Ehsani ¶95.) Further,

the modification would have operated in the same manner such that the modified Control Action Module sends an alarm signal in response to commands from the MCU when an operating restriction is violated to control the vehicle and present an alarm. (*Id.*)

Furthermore, the ’101 specification illustrates the “SCU as a collection of components, and does not require connections or communication between these components.” (’101, Fig. 6, 7:57-8:2; *see also* EX1012, 185-186.) Therefore, both the Parameters Module and the “information unit 23” can be integrated as a collection of components in the Control Action Module to collectively form the SCU, even if the two systems do not otherwise connect with or communicate with one another. (Ehsani ¶96.)

d. GPS (11[B])

Murphy in view of Schanz discloses Claim 11[B]. (Ehsani ¶99.) Murphy discloses an LD module that can be implemented using GPS to determine present location and present speed. (*See* VIII.A.1; Murphy, Abstract, 3:48-56.)

e. Data Logging Device (11[C])

Murphy in view of Schanz discloses Claim 11[C]. (Ehsani ¶100.) Murphy discloses a data logging device (memory 180 of controller 179) that records speed and location information received from LD module (GPS module). (*See* VIII.A.1; Murphy, 13:53-65, 12:1-3.)

3. Claim 5

Murphy in view of Schanz renders claim 5 obvious. (Ehsani ¶¶109-110.) As discussed in Ground 1, Murphy discloses a memory module that stores the driver indicia and operating restrictions (operating profile). (*See* VIII.A.7.) Alternatively, a POSITA would have been motivated to modify Murphy's system to incorporate Schanz's "storage unit 2" for storing the "vehicle parameters 6," which can include "special vehicle parameters 6" "stored for the respective driver 4" (operating profile). (Ehsani ¶110; Schanz, [0017], [0020].) If parameters are stored for the identified driver, they are used to "adjust[]" the "driving dynamic characteristics of the vehicle." (*Id*., [0020].) Therefore the "parameters" (operating profile) stored in "storage device 2" (memory module) are activated (loaded) for controlling operation of the vehicle when the driver is authenticated. A POSITA would have been motivated to combine Schanz's vehicle parameters with Murphy's analogous controller as discussed in VIII.B.1 to operate similarly with similar goals of improving driver safety when the parameters have not been violated. (*See also* Ehsani ¶ 110.) Further, the combined system would operate in the same manner such that an authenticated driver could operate the vehicle within the operating profile. (*Id.*)

4. Claims 8 and 13

Murphy in view of Schanz renders claims 8 and 13 obvious. (Ehsani ¶¶111-

112.) As discussed in Ground 1, Murphy's system includes a database with information for each authorized driver, including a maximum allowable vehicle speed, allowable locations, and allowable hours of operation. (*See* VIII.A.10; Murphy, 15:15-21, 15:66-16:9.)

Alternatively, it would have been obvious to combine Schanz's vehicle parameters into Murphy's token and controller. Schanz discloses that the definable "vehicle parameters 6" (resulting in an operating profile when defined for a driver) include "a maximum vehicle speed 9." (Schanz, [0019].) Schanz further teaches that the "vehicle parameters 6" can include "special vehicle parameters 6" that "are stored for the respective driver" (as part of operating profile per driver) "so that the driving dynamic characteristics of the vehicle can be adjusted in relation to the driving skills of the respective driver." (*Id.*, [0020].) A POSITA would have been motivated to combine Schanz's vehicle parameters with Murphy's analogous controller as discussed in VIII.B.1 to operate similarly with similar goals of providing additional driving restriction options. (*See also* Ehsani ¶ 110.)

5. Claims 9, 14, 17, 18

Murphy in view of Schanz renders claims 9, 14, 17, and 18 obvious. (Ehsani ¶¶113-114.) Murphy discloses or renders obvious that the SCU (Control Action Module) generates an alarm for remotely alerting an authorized user when the driver violates the operating profile. (*See* VIII.A.11; Murphy at 5:18-60, 15:37-42.)

6. Claim 10

Murphy in view of Schanz renders claim 10 obvious. (Ehsani ¶115.) As discussed in Ground 1, Murphy discloses or renders obvious that the driver identification and data logging device comprises an RFID. (*See* VIII.A.12.) Alternatively, a POSITA would have been motivated by Schanz to modify Murphy's token to use a radio signal device implementation such as RFID, as was commonly used in automobiles. (*Id.*; Benco, [0002]-[0004].) Schanz teaches a unit for sending and/or receiving "infrared or radio signals." (Schanz, [0018].) Both Murphy and Schanz are directed towards driver authentication and vehicle monitoring and control. (Murphy, Abstract, 2:20-3:4, 5:13-6:17, 6:55-7:14; Schanz, [0006], [0019].) A POSITA would have understood the benefits of implementing Murphy's token using a unit capable of transmitting and receiving data signals for use in identifying the driver. (Ehsani ¶115.) A POSITA would accordingly have been motivated to apply Schanz's transmission/receiving teachings to Murphy, and would have had a reasonable expectation of success as the system would have operated in the same manner with the TRAM reading information from the token upon presentation to the TRAM to authenticate the driver. (*Id.*)

7. Claims 19 and 20

Murphy in view of Schanz renders claim 19 and 20 obvious. (Ehsani ¶117.) As discussed for the SCU limitations, Murphy teaches that the Control Action

Module (SCU) can implement Control Actions, including to disable the vehicle, reduce the speed using a governor, or disable accessories. (Murphy, 5:18-60, 15:37-42.) Alternatively, it would have been obvious to a POSITA to combine the teachings of Murphy's Control Actions with Schanz's teaching of actively intervening in driving operations to alert the driver. (Ehsani ¶95.) Schanz's "dynamic vehicle stabilization system" "actively intervene[s] in driving operation …in order to ***alert*** the beginner to critical driving situations." (Schanz, [0022] (emphasis added).) A POSITA would accordingly have been motivated to apply Schanz's teachings of actively intervening in operations to Murphy's Control Action Module, and would have reasonably expected to succeed in doing so given the references' teachings. (*Id.*)

8. Claims 2-4, 6-7, 12, 16

Murphy in view of Schanz renders obvious claims 2-4, 6-7, 12, and 16. (*See* §§VIII.B.1 (motivation to combine), VIII.A.4-6,8-9,13 (Ground 1).)

C. <u>Ground 3</u> – Murphy-Schanz-Benco Renders Obvious Claim 10

Benco was filed December 8, 2006, and published on June 12, 2008. Benco is prior art under at least pre-AIA § 102(a) and (b).

Benco teaches an apparatus for improving security with a keyless ignition system. (Benco, [0004].)

Alternatively, it would have further been obvious to a POSITA to implement

Murphy's token with RFID in view of Benco. As discussed in Ground 1, Murphy teaches "insertion or ***presentation*** of a token or smart card." (*See* VIII.A.12; Murphy, 6:55-59.) Benco teaches that many vehicles used a keyless ignition system using "a coded Radio Frequency Identification (RFID) chip." (Benco, [0002]-[0003].) A POSITA would have been motivated to combine Murphy or (Murphy in view of Schanz) with Benco to provide convenience to drivers with a remote keyless ignition system by implementing Murphy's token with RFID. (Ehsani ¶¶119-125.) It would have been trivial to implement, as RFID was commonly used for remote keyless ignition systems within the automotive industry. (*Id.*, ¶125; Benco, [0003].)

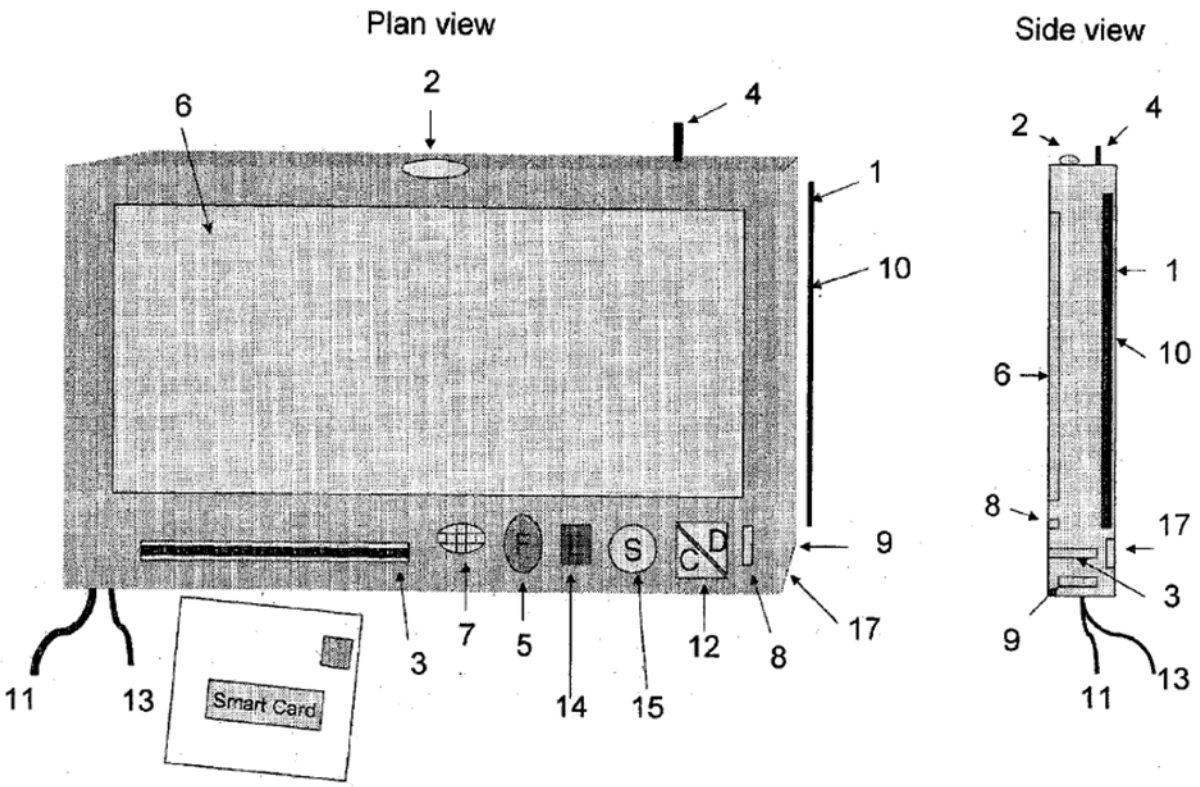
D. Ground 4 – Petrik Discloses or Renders Obvious Claims 1-20

Petrik was filed August 9, 2005, and published on July 19, 2007. Petrik is prior art under at least pre-AIA § 102(a) and (b).

Petrik discloses an in-vehicle monitoring unit incorporating GPS monitoring, management, and cruise control. (Petrik, Abstract.) The in-vehicle unit uses a "fingerprint reader" and a "smart card reader/writer" to "confirm [a driver's] identity," which "automatically logs [the driver] in as the current driver and enables engine ignition." (*Id.*, [0025].) "The engine will not start if … an invalid driver card and fingerprint combination is presented." (*Id.*) The unit logs GPS, operational parameters, vehicle location, speeds, and other information in the smart card and the

in-vehicle unit's memory. (*Id.*, [0009].) "Intended vehicle route plans" are loaded to "the unit and with a remote Transport Management Command Centre via SATELITE/GPRS/GSM/BLUETOOTH prior to the start of each journey." (*Id.*, [0011].) The unit warns of speed zone changes and interacts with the engine management system to slow down or speed up the vehicle. (*Id.*, [0025].) The vehicle can also be stopped remotely via a "disable" command to the unit to lock up the engine management unit. (*Id.*, [0030].)

Petrik's in-vehicle unit includes a microcomputer 1, a GPS module 2, a smart card reader writer 3, a SATELITE/GPRS/GSM/BLUETOOTH module 4, a fingerprint module 5, a display 6, a beeper 7, a USB connector 8, a power connector 11, and an engine management system connector 14. (Petrik, [0069], Fig. 1.)



(Petrik, Fig. 1.)

1. Independent Claim 1

Petrik anticipates or renders obvious claim 1. (Ehsani ¶¶129-137.)

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

Petrik discloses a driver authentication and monitoring system. (Ehsani ¶130; Petrik, Abstract, [0025].)

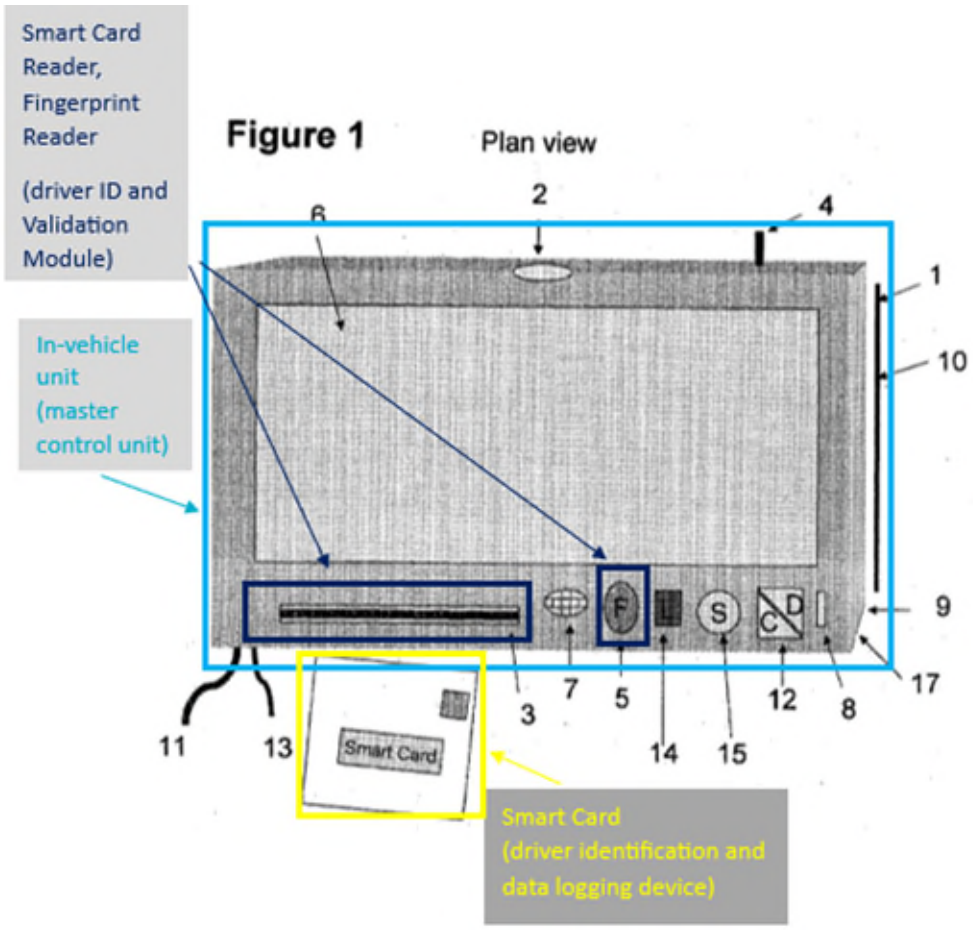
1[A]: ***a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device***

Petrik discloses or renders obvious claim 1[A]. (Ehsani ¶¶131-134.)

Petrik discloses an in-vehicle monitoring unit (MCU) with 16 components, where "1 is the microcomputer[,]" "3 is the smart card reader writer" and "5 is the

fingerprint module." (Petrik, [0069], Fig. 1("form one").) "Drivers are issued with their logbook smart cards with their fingerprint template recorded in the card." (*Id.*, [0022].) The in-vehicle unit uses the "smart card reader/writer" and "the fingerprint reader" "to confirm [a driver's] identity" using the smart card and associated fingerprint combination. (*Id.*, [0025].) The smart card is a driver identification and logging device. (Ehsani ¶131.)

In response to a smart card and fingerprint combination, the in-vehicle unit logs in the authenticated user "as the current driver and enables engine ignition[,]" but the "engine will not start if … an invalid ... combination is presented." (*Id.*) Thus, Petrik discloses a master unit in a motor vehicle (in-vehicle unit) for authenticating at least one driver via a driver identification and data logging device (smart card). (Ehsani ¶132.)



(Petrik, Fig. 1 (annotated).)

During authentication, an operating profile is loaded into the in-vehicle unit. (Petrik, [0025].) An authenticated driver can operate the vehicle within the operating profile, including at least the route plan, speed limits, and rest parameters. (*Id.*) The system provides "automated intelligent speed adaptation" and using "geographically based speed location tables" can "beep[] to warn the driver of the zone change and ... interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (*Id.*) Further, the GPS-based cruise control "can be programmed never to allow the

vehicle to exceed a set absolute maximum speed" and even though a "driver can always override the system by using the break, or the accelerator," the driver can only accelerate "to the set absolute maximum speed only." (*Id.*, [0025] – [0026].) The in-vehicle unit is also programmed to "warn[] the driver every time he is due to take a rest break." (*Id.*, [0028].) These parameters are part of an operating profile. (Ehsani ¶134.) The system monitors vehicle operation to determine if the driver is violating the operating profile. (*Id.*)

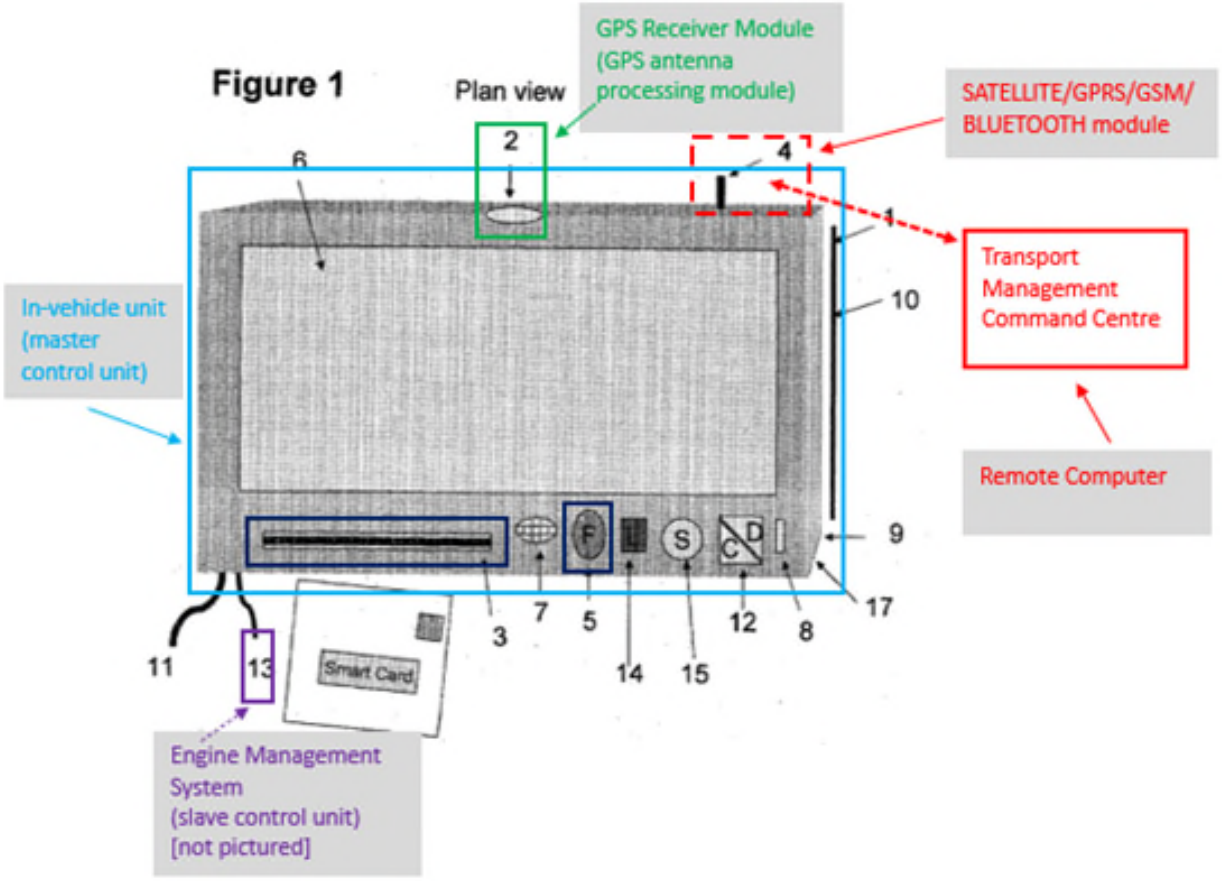
1[B]: ***wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;***

Petrik discloses or renders obvious claim 1[B]. (Ehsani ¶133.) A POSITA would have understood that confirmation of a driver's identity using both the smart card and fingerprint would include the in-vehicle unit (MCU) receiving information comprising/equivalent to "a unique identification code" from both the smart card and fingerprint. (*Id.*)

1[C]: ***a slave control unit in a motor vehicle and in communication with said master control unit, said slave control unit configured to receive commands from said master control unit and to generate at least one of an alarm signal if said at least one driver violates said operating profile unique to said at least one driver thereby providing feedback about said vehicle usage and govern mechanical operations of said vehicle remotely thereby maintaining occupant safety.***

Petrik discloses or renders obvious claim 1[B]. (Ehsani ¶¶135-137.) The in-vehicle unit (MCU) connects to engine management system (SCU; not shown in Fig. 1) using 13 "the engine management system connector." (Petrik, [0069], Fig. 1.)

"[T]he unit is connected to the engine management system which is programmed to take instructions from it." (*Id.*, [0020].) The in-vehicle unit (MCU) can interact with the engine management system (SCU). (*Id.*, [0025].) Thus, Petrik discloses a SCU in communications with said MCU.



(Petrik, Fig. 1 (annotated).)

The Petrik in-vehicle GPS unit "interacts with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits …" (Petrik, [0025]; '101 at 6:65-7:5 ("alarm signal" includes slowing vehicle).) The engine management system also controls the vehicle in response to

commands from the remote Transport Management Command Centre, and a "vehicle can be stopped by sending a 'disable' command to the unit via the SATELITE/GPRS/GSM to lock up the engine management unit." (Petrik, [0030].) Thus, Petrik discloses an SCU (engine management system) configured to receive commands from said MCU (in-vehicle unit) and generate an alarm signal (*e.g.*, disable, slow down) if the driver violates said operating profile unique to the driver (operating parameters including route plan and speed limits) thereby providing feedback about said vehicle usage and govern mechanical operations (*e.g.*, slow down or disable) remotely (via SATELITE/GPRS/GSM) thereby maintaining occupant safety. (Ehsani ¶136.)

Alternatively, Petrik renders obvious that its SCU (engine management system) generates an alarm signal (*e.g.*, beep) if the driver violates his/her operating profile (*e.g.*, exceeding speed limit). Petrik discloses beeping to warn the driver as it approaches a new speed zone, and if allowed, interacts with the engine management system to slow or accelerate the vehicle. (Petrik, [0025].) A POSITA would recognize that there are a limited number of ways to implement the beep signal, and recognize that an obvious design choice would be to have the in-vehicle unit send the new zone's speed limit to the engine management system to in turn send a signal to the beeper (alarm signal) in addition to sending a slowdown command when the vehicle's speed exceeds the new speed limit. (Ehsani ¶137.) A

POSITA would have been motivated to make this design choice and would have had a reasonable expectation of success because the engine management system is directly involved in maintaining speed and would be in the best position to send a signal to the beeper when the speed is different from the new zone. (*Id.*)

2. Independent Claim 11

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

Petrik discloses a driver authentication and monitoring system. (Ehsani ¶138; Petrik, Abstract, [0025].) (*See supra*, §VIII.D.1).

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

Petrik discloses or renders obvious Claim 11[A]. (Ehsani ¶139.)

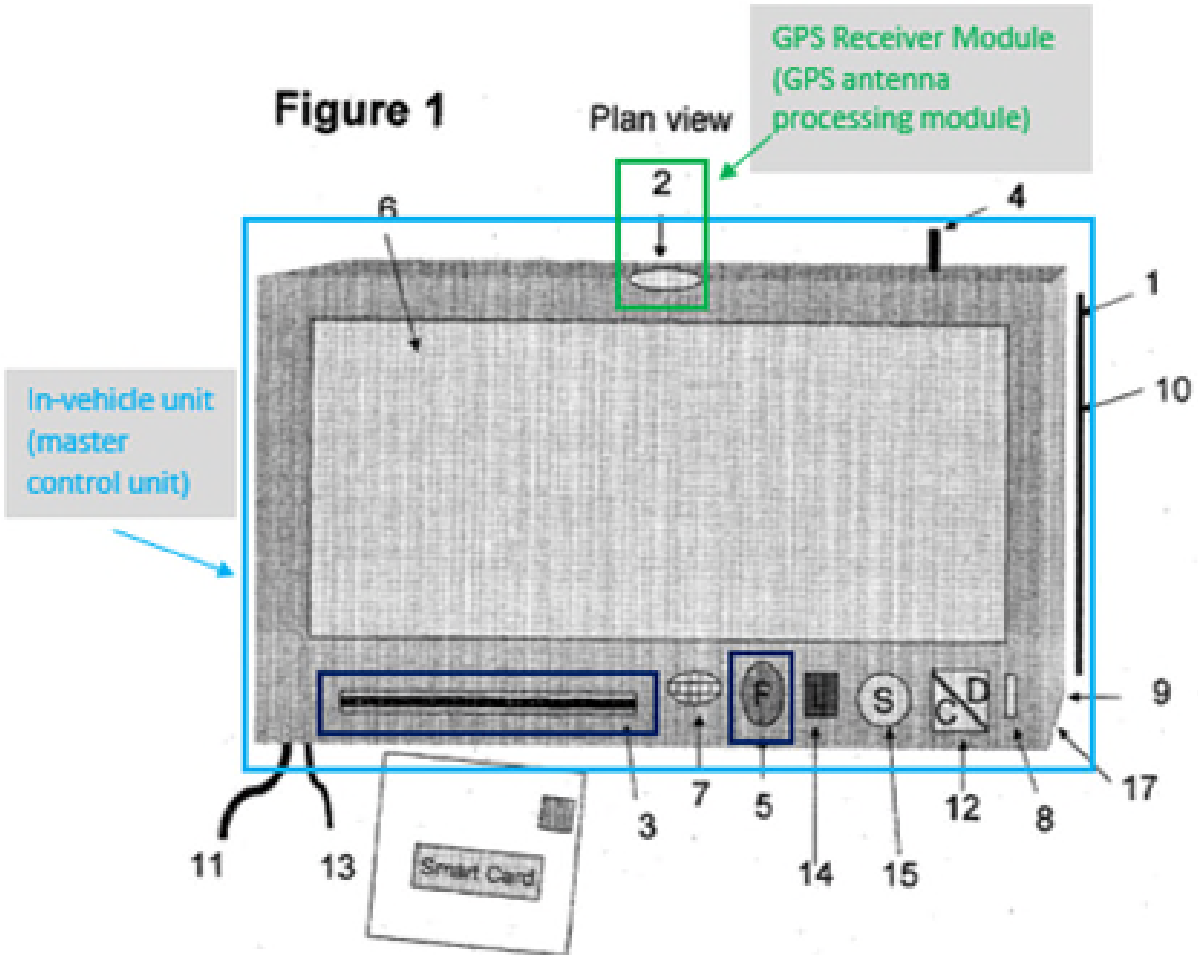
Petrik discloses a MCU (in-vehicle unit) for authenticating a driver via a driver identification (smart card). (*See supra*, §VIII.D.1). Claim 11[A] additionally requires "associating an operating profile with said at least one driver." Petrik's in-vehicle unit associates the loaded profile with the driver upon authentication. (Petrik, [0025] – [0026]; Ehsani ¶139.)

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

Petrik discloses Claim 11[B]. (Ehsani ¶140.)

Petrik discloses a GPS module that "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." (Petrik, [0025], Fig. 1 (GPS Receiver Module 2).)



(Petrik, Fig. 1 (annotated).)

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

Petrik discloses Claim 11[C]. (Ehsani ¶141.)

Petrik teaches "a method and system of automatically … 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].) Further, the "monitoring unit…correlates each vehicle and driver related operational parameter and records the results in its' memory as well as on the smart card." (Petrik, [0018].) A POSITA would thus have understood that the smart card and monitoring unit's memory are each a data logging device. (Ehsani ¶141.)

11[D]: ***a slave control unit in a motor vehicle and in communication with said master control unit, said slave control unit configured to receive commands from said master control unit and to generate an alarm signal if said at least one driver violates said operating profile unique to said at least one driver thereby providing feedback about said vehicle usage and govern mechanical operations of said vehicle remotely thereby maintaining occupant safety;***

Petrik discloses or renders obvious Claim 11[D]. (Ehsani ¶142.)

Claim 11[D] is substantially the same as Claim 1[C], and Petrik therefore discloses Claim 11[D] for the same reasons given above with respect to Claim 1[C], *supra* §VIII.D.1.

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

Petrik discloses or renders obvious Claim 11[E]. (Ehsani ¶¶143-144.)

Petrik discloses the in-vehicle unit (MCU) permits a driver to operate the vehicle within the operating profile (including route plan, speed limits, and rest parameters) in response to receiving a unique identification code (information comprising/equivalent to a unique identification code from both the smart card

reader/writer and fingerprint reader) so long as the driver has not violated the operating profile. (*See* §VIII.D.1). If a driver diverts from the route plan, the unit notifies the Centre and the vehicle can be stopped by sending a "disable" command, thus preventing the driver from operating the vehicle when the route plan is violated. (Petrik, [0030]; Ehsani ¶144.)

3. Independent Claim 15

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

Petrik discloses a driver authentication and monitoring system and method. (Ehsani ¶145; Petrik, Abstract, [0025].) (*See* §VIII.D.1).

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

Petrik discloses or renders obvious Claim 15[A]. (Ehsani ¶146.)

Petrik's in-vehicle controller constitutes providing a motor vehicle with a driver authentication and monitoring system. (*See* §VIII.D.1).

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

Petrik discloses Claim 15[B]. (Ehsani ¶147.)

Petrik's disclosure of loading an operating profile including route plan and speed limits constitutes programming said driver authentication and monitoring system with an operating profile associated with a high risk driver. (*See* §VIII.D.1).

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

Petrik discloses Claim 15[C]. (Ehsani ¶148.)

Petrik's smart card and fingerprint confirming identity constitutes authenticating said high risk driver and enabling operation. (*See* §VIII.D.1).

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

Petrik discloses Claim 15[D]. (Ehsani ¶149.) Petrik discloses generating an alarm (*e.g.*, slow down or disable engine, optical/acoustic warning) when the driver violates the operating profile (including exceeding speed limit). (*See* §VIII.D.1).

15[E]: ***governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.***

Petrik discloses Claim 15[E]. (Ehsani ¶150.) Petrik discloses governing of said vehicle remotely (slow down or disable engine) when the driver violates the operating profile (including exceeding speed limit). (*See* §VIII.D.1).

4. Claim 2

Petrik anticipates or renders claim 2 obvious. (Ehsani ¶¶151-152.)

Petrik's system includes a remote, networked "Transport Management Command Centre with an up to date database of road conditions" in communication with the in-vehicle unit. (Petrik, [0010], cl. 49.) "Prior to each departure, dispatch automatically 'files' the intended vehicle route plan and cargo details with the national Transport Management Command Centre and in the in-vehicle unit via the SATELITE/GPRS/GSM." (*Id.*, [0024]; *see also id.*, cls. 49, 51 (internet on-line facility and database).) A "vehicle route plan" includes operating parameters (*e.g.*,

speed limits) associated with the vehicle. (Ehsani ¶151-52.) Thus, Petrik discloses a database comprising a program module (software that allows filing of route plan) including at least one operating parameter associated with the vehicle (driver route plan), said program module remotely accessible (via the SATELITE/GPRS/GSM) by an authorized user (dispatch) to program an operating profile with respect to at least one driver (at least route plan). (*Id*.)

5. Claim 3

Petrik discloses or renders obvious Claim 3. (Ehsani ¶153.)

As discussed for 1[C], the smart card is the driver identification and logging device. When a driver is authenticated, the system logs him in and enables engine ignition. (*Id.*, [0025].) A POSITA would recognize that loading the operating profile (at least the route plan) is performed in conjunction with the driver identification and data logging device (smart card) and a remote computer necessary to transmit the route plan to the in-vehicle unit via the SATELITE/GPRS/GSM. (Ehsani ¶153.)

6. Claim 4

Petrik anticipates or renders claim 4 obvious. (Ehsani ¶¶154-157.)

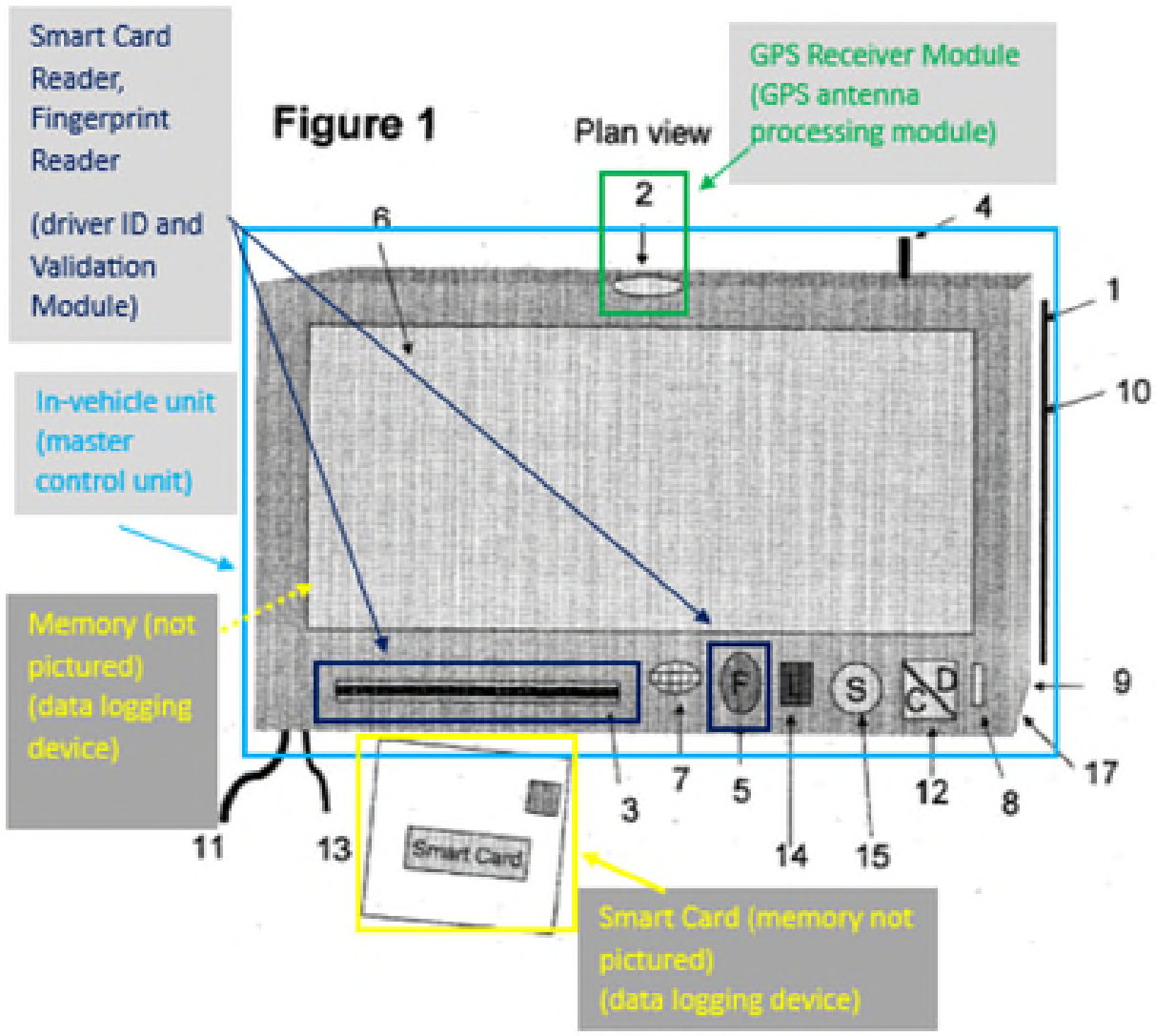
As discussed for the MCU limitations, Petrik discloses a MCU (in-vehicle unit) for authenticating at least one driver via a driver identification and data logging device (smart card). The in-vehicle unit enables the engine if the driver is authenticated. (Petrik, [0025].) For authentication, the in-vehicle unit necessarily has

a software module that identifies and validates a driver based on the smart card and fingerprint. (Ehsani ¶154.)

Petrik discloses a GPS antenna processing module. The in-vehicle unit has "a GPS receiver module" that necessarily comprises a GPS antenna processing module. (Ehsani ¶155; Petrik, [0016]; *see also* Fig. 1)

Petrik discloses a memory module, both in the in-vehicle unit and the smart card. Petrik teaches that the in-vehicle unit "is supplied with an upgradable software program[,]" "stores previous 2 minutes of data logged by engine management system[,]" and "correlates each vehicle and driver related operational parameter and records the results in its memory as well as on the smart card." (Petrik, [0018].)

Petrik discloses a function indicator module in beeper 7. (Petrik, [0016], Fig. 1; Ehsani ¶157.) The in-vehicle unit beeps to warn the driver of a speed zone change and interacts with the engine management system to slow or accelerate the vehicle. (Petrik, [0025].) A POSITA would recognize the beep as a response to a restriction being violated (*e.g.*, speed higher than limit in new zone requiring engine management to slow it down). (Ehsani ¶157.) A POSITA would recognize this to require a function indicator module that comprises the intelligent speed adaptation and geographically based speed zone location tables to monitor the function of vehicle speed and relay an indication to the beeper when the limit is exceeded. (*Id.*)



(Petrik, Fig. 1 (annotated).)

7. Claim 5

Petrik anticipates or renders claim 5 obvious. (Ehsani ¶158.) As discussed VIII.D.6 (claim 4), Petrik discloses a memory module, both in the in-vehicle unit and the smart card, in which the route plans are "filed.". (Petrik, [0011].) A POSITA would have understood that the operating profile, including route plans, are stored

within the in-vehicle unit and smart card memory modules. (Ehsani ¶158; *see also* Petrik, [0018] (operating parameters recorded within unit and smart card memory).)

8. Claims 6 and 16

Petrik anticipates or renders claims 6 and 16 obvious. (Ehsani ¶119.) As discussed in VIII.D.6 (claim 4), Petrik discloses a GPS Receiver Module 4—a GPS antenna processing module—which "keeps a constant log of the date, time, ***location***, distance travelled and speed of the vehicle …." (Petrik, [0016], [0025], Fig. 1 (GPS Receiver Module 2); Ehsani ¶¶159, 171.)

9. Claims 7 and 12

Petrik renders claims 7 and 12 obvious. (Ehsani ¶¶160-166.) As discussed for the SCU limitations, Petrik discloses an engine management system (SCU). Petrik teaches power connector 11 and power/cigarette lighter connector in the in-vehicle unit. (Petrik, [0016], [0040].) A POSITA would have understood either one to imply a power regulator or equivalent to regulate a power source to allow Petrik's engine management system to control vehicle operations. (Ehsani ¶160.) A POSITA would be motivated to implement a power regulator in the engine management system, as it would be necessary for operation of the corresponding powertrain ECU for the engine management system to slow down the vehicle. (*Id.*; *see also* Petrik, [0025].)

Petrik discloses or renders obvious a starter relay in the engine management system. (Ehsani ¶161.) When the driver is authenticated, the system "logs him in as

the current driver and enables engine ignition." (Petrik, [0025].) This is consistent with the starter relay 526 in the '101. (§VIII.A.9; '101, 8:7-10; Ehsani ¶161.) A POSITA would recognize that this function requires a starter relay in the engine management system. (*Id.*)

Petrik discloses or renders obvious a definable relay module in the engine management system. (Ehsani ¶162.) Petrik teaches that the engine management system (SCU) transmits the last 2 minutes of data logged to the Transport Management Command Centre. (Petrik, [0032].) A POSITA would recognize this to require a definable relay module as claimed by the '101 that receives information and passes that information along to the transceiver for transmittal to the Command Centre. (Ehsani ¶162.) A POSITA would recognize that the definable relay 524 in the '101 would be used to receive information relating to the driver's alcohol consumption and to pass that information to another part of the system, just as Petrik's engine management system receives information that it logs and passes along to another part of the system to transmit to the Transport Management Command Centre. (Ehsani ¶162 *see* §VIII.A.9; '101, 7:59-61, 8:16-18, FIG 6.)

Alternatively, Petrik teaches that the engine management system prevents the vehicle from starting if authentication fails. (Petrik, [0025].) A "BLUETOOTH enabled hand held unit can be used locally … to 'disable' the engine management unit and stop the vehicle regardless of the drivers' actions." (*Id.*, [0031].) A POSITA

would recognize that this requires a definable relay to pass information from one system component to another. (Ehsani ¶163.) A POSITA would be motivated to implement such a definable relay within the engine management system to pass information between the engine and the in-vehicle unit. (*Id.*)

Petrik discloses or renders obvious that the SCU comprises a slave microcontroller. (Ehsani ¶164.) The engine management system includes an engine management computer. (Petrik, claims 64, 68, 70, 89, 98, 100.) A POSITA would have understood this to require the engine management system to comprise a microcontroller, or alternatively, it would have been obvious to implement the engine management system with a microcontroller because it would involve merely selecting from one of a finite number of ways to implement the engine management system (either a microcontroller or a microprocessor, or both). (Ehsani ¶164.)

Petrik discloses or renders obvious that the SCU comprises an alarm synthesizer. (Ehsani ¶165.) As discussed for the SCU limitations, Petrik's engine management system (SCU) controls the vehicle to stay within a zone's speed limit and that the engine management system can control the vehicle in response to remote commands to stop the vehicle in response to a hostile driver or out of control vehicle. (Petrik, [0025], [0030]; '101 at 6:65-7:5 ("alarm signal" includes slowing down vehicle).) Additionally, Petrik teaches generating a beep if a driver exceeds a speed limit on the route plan. (Petrik, [0025].) Thus, Petrik discloses or renders obvious

that the SCU (engine management system) is configured to generate at least one of an alarm signal (*e.g.*, signal to lock up the engine management system or generate a beep). A POSITA would further recognize that this requires the engine management system to have an alarm synthesizer to synthesize such an alarm signal. (Ehsani ¶165.)

Thus, Petrik renders obvious that the SCU comprises a power regulator module, a starter relay module, a definable relay module, a slave microcontroller, and an alarm synthesizer.

10. Claims 8 and 13

Petrik anticipates or renders claims 8 and 13 obvious. (Ehsani ¶168.) Petrik discloses that the GPS cruise control "can be programmed never to allow the vehicle to exceed a set absolute maximum speed" and that the driver can only accelerate "to the set absolute maximum speed only." (*Id.*, [0025] – [0026].) Thus, Petrik renders obvious that the at least one operating parameter comprises at least a maximum allowable vehicle speed. (Ehsani ¶168.)

11. Claims 9, 14, 17, 18

Petrik anticipates or renders claims 9, 14, 17, and 18 obvious. (Ehsani ¶169.) As discussed for the SCU limitations, Petrik's SCU (engine management system) generates an alarm signal (*e.g.*, disable command) if the driver violates the operating. Petrik further teaches that "[i]f a driver diverts inappropriately from the 'filed' route

plan the unit notifies the Centre." (Petrik, [0030].) Thus, an alarm signal is generated by the engine management system (SCU) when the driver violates the operating profile, and the signal is used to notify the Centre (authorized user).

12. Claim 10

Petrik renders claim 10 obvious. (Ehsani ¶170.) As discussed for the MCU limitations, the smart card is the driver identification and logging device. Smart cards were known to incorporate RFID technology for automatic identification for vehicles, meeting this limitation. (*See*, VIII.A.12 (Ground 1, claim 10); Ehsani ¶170.)

13. Claims 19 and 20

Petrik anticipates or renders claim 19 and 20 obvious. (Ehsani ¶172.) Petrik teaches that the in-vehicle unit can interact with the engine management system to slow down the vehicle to stay within speed limits and can also receive a remote command to lock up or disable the engine management system to stop a hostile driver or out of control vehicle. (Petrik, [0025]; *see* §VIII.D.1.) This would necessarily require sending a control signal to the engine to slow down or disable to engine. (Ehsani ¶172.)

E. Ground 5 – Petrik-Schanz Render Obvious Claims 1-20

Petrik in view of Schanz renders claims 1-20 obvious. (Ehsani ¶¶173-207.)

1. Motivation to Combine

It would have been obvious to combine Petrik with Schanz, which disclose

complimentary methods for driver authentication and monitoring. (Ehsani ¶132.); Petrik, Abstract, [0001] – [0015], [0025] – [0026]; Schanz, Abstract, [0006] – [0010], [0017] – [0027].) Like Petrik's in-vehicle unit, Schanz's "device 1" identifies and authenticates a driver and provides driver-specific parameters. (Schanz, [0018], [0020]; *See* §VIII.B.1 (Ground 2, motivation to combine).)

A POSITA would have looked to Schanz to improve Petrik given their similarities and benefits. (Ehsani, ¶175.) The combined system would provide more flexibility for both the driver and the administrator, allowing a driver to present a smart card wirelessly to start the vehicle (*see* Schanz, [0018]) and providing the administrator with more options for driver-specific restrictions (*see* Schanz, [0020]) that when violated could allow for various alerts and vehicle control options (Petrik, [0025], [0030]). (Ehsani, ¶175.) For example, based on driver-specific parameters (*e.g.*, driver-specific speed limit) provided wirelessly from the smart card and/or from administrator (*e.g.*, parent), a vehicle can alert the driver and the remote administrator and control the vehicle (*e.g.*, lower speed) to improve driver safety. (*Id.*)

A POSITA would have been motivated to combine the functionalities of Petrik and Schanz (including, *e.g.*, using Schanz's identification code, additional driver-specific vehicle restrictions, and transmitting/receiving via radio signals with Petrik's smart card, in-vehicle unit, and engine management system to improve

vehicle occupant safety, as both Petrik and Schanz suggest, (*see* Petrik, [0003], Schanz, [0004], [0012]), while providing the flexibility for authentication and customizability that Schanz suggests, (*see* Schanz, [0017] – [0018], [0020]). (Ehsani ¶176.)

Combining Petrik and Schanz would have been merely a simple combination of known elements to obtain predictable results. (Ehsani ¶177.) For example, the combination of Schanz's identification code, additional driver-specific restrictions, and use of radio signals with Petrik's smart card would have yielded the predictable result of a system that allows identification and authentication of a driver without mechanical interaction of the smart card and to notify the driver and administrator when those restrictions are violated. (*Id.*) This would have been nothing more than the use of known techniques for identification, authentication, and vehicle monitoring to improve Petrik to provide more granular vehicle safety controls. (*Id.*) A POSITA would have had a reasonable expectation of success in combining them because both disclose vehicle units (Petrik's in-vehicle unit and Schanz's device 1) that serve analogous functions and operate in similar ways to improve driver safety. (*Id.*.) A POSITA would have understood that features of Schanz's "device 1" can be easily applied to Petrik's in-vehicle unit, and vice-versa. (*Id.*.)

2. Independent Claims (1, 11, 15)

Petrik in view of Schanz renders claims 1, 11, and 15 obvious. (Ehsani ¶¶178-

200.)

a. Preambles (1[P]/11[P]/15[P])

Petrik in view of Schanz discloses a driver authentication and monitoring system and method. (Ehsani ¶¶179, 187, 193.) As discussed in VIII.D.1, VIII.D.2, VIII.D.3 and VIII.B.2, Petrik and Schanz both disclose the preambles.

b. Master Control Unit (1[A],1[B]/11[A],[E]/15[A-C])

Petrik in view of Schanz renders obvious the MCU limitations. (Ehsani ¶¶180-182, 188, 192, 194-196.) Petrik discloses an in-vehicle unit (MCU) which uses a smart card (driver identification and data logging device) "to confirm [a driver's] identity." (*Id.*; *see* Petrik, [0025]; VIII.D.1, VIII.D.2, VIII.D.3.) Petrik's MCU associates an identified driver with an operating profile and permits operation within that profile. (Petrik, [0025]-[0028].)

Alternatively, it would have been obvious to integrate Schanz's vehicle parameters into Petrik's smart card and in-vehicle unit. Subcomponents of Schanz's "device 1" "check[] whether special vehicle parameters 6 are stored for the respective driver." (*Id.*, [0020]; *see also* §VIII.B.1.) The "device 1" detects exceeding the vehicle parameters and responds with warnings or other interventions. (*Id.*, [0022], [0025].) For the reasons discussed in VIII.E.1, a POSITA would have been motivated to modify Petrik's smart card to include Schanz's vehicle parameters and Petrik's in-vehicle unit to include Schanz's interventions for violations of the

vehicle parameters, as Schanz's "device 1" and Petrik's in-vehicle unit serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. (Ehsani ¶181.)

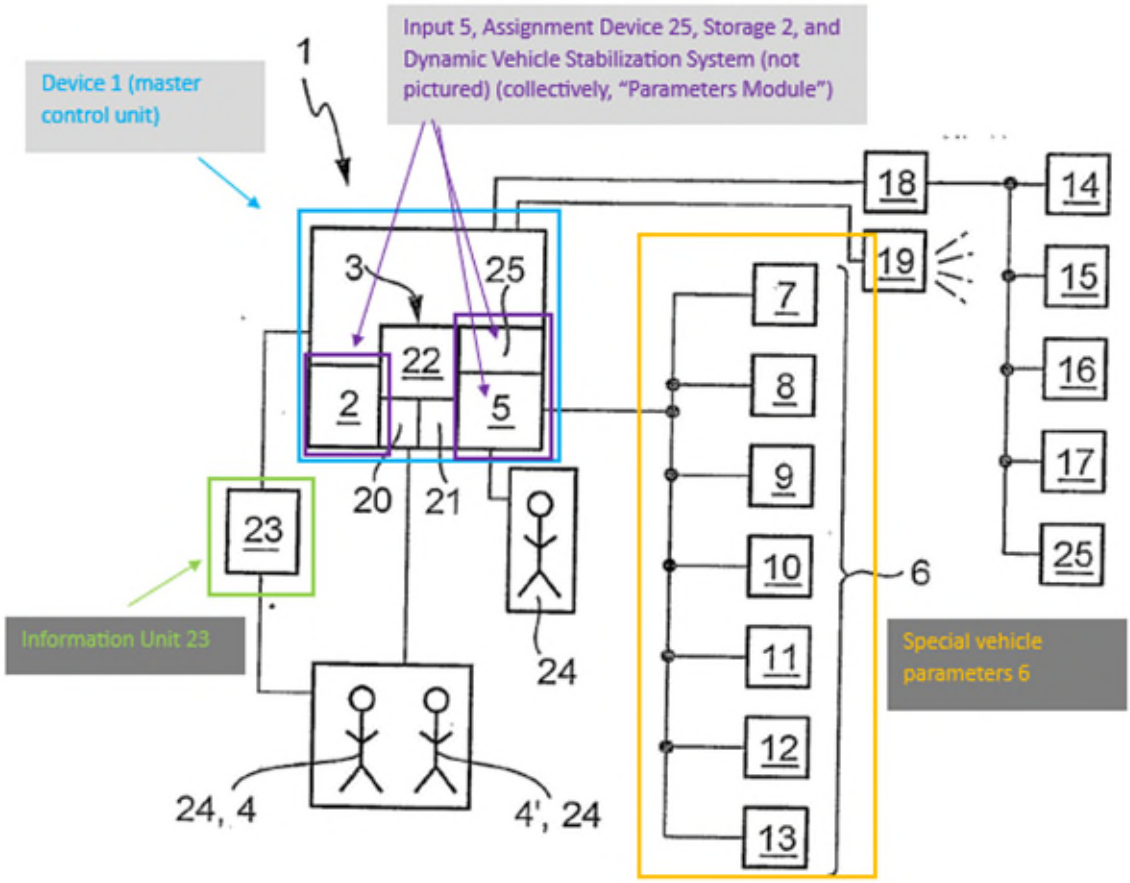
Alternatively, Schanz discloses a unique identification code in that "recognition device 3" within "device 1" (MCU) may include "a reading device…for recognizing an identification code 22." (Schanz, [0018].) A POSITA would have recognized the advantage of including Schanz's reading module in Petrik's in-vehicle unit to receive a driver-specific identification code. (Ehsani ¶182.) A POSITA would have been motivated to integrate Schanz's identification code functionality into Petrik's in-vehicle unit to achieve Petrik's goal of identifying and authenticating the individual driver based on the combination of the smart card (including fingerprint template) and the driver's fingerprint. (*Id.*; Petrik, [0022], [0025].) A POSITA would have had a reasonable expectation of success in combining Petrik's in-vehicle unit with Schanz's reading module because the two structures serve analogous functions and operate in similar ways to improve driver safety. (Ehsani ¶182.) Further, the modification would have been nothing more than the simple combination or substitution of Schanz's identification code to improve Petrik's in-vehicle unit to achieve its purpose of identifying a driver. (*Id.*)

c. Slave Control Unit (1[C]/11[D]/15[D-E])

Petrik in view of Schanz renders obvious the SCU limitations. (Ehsani ¶¶183-

186, 191, 195.) Petrik discloses that the in-vehicle unit (MCU) connects to an engine management system (SCU; not shown in Fig. 1) using 13 "the engine management system connector." (*See* Petrik, [0069], Fig. 1; *see also* VIII.D.1, VIII.D.2, VIII.D.3.) Alternatively, it would have been obvious to a POSITA to implement both the functionalities of Schanz's Parameters Module (input 5, assignment device 25, storage device 2, and dynamic vehicle stabilization system) and Schanz's information unit into Petrik's engine management system. (Ehsani ¶183.)

Like the engine management system in Petrik, Schanz's Parameters Module is connected to device 1 and receives commands from device 1 to "adjust[]" "driving dynamic characteristics of the vehicle" to enforce "vehicle parameters 6" (operating parameters). (Schanz, [0019]-[0020]; §VIII.B.2.c; Ehsani ¶184.)



(Schanz, Fig. 1 (annotated).)

The combined Petrik-Schanz system integrating Schanz's Parameters Module and information unit with Petrik's engine management system would have an SCU for governing mechanical operations of the vehicle remotely and generating an audible alarm. For the reasons discussed in VIII.E.1, a POSITA would have been motivated to combine these features from Schanz with Petrik's engine management system, as Schanz's Parameters Module and Petrik's engine management system serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. (Ehsani ¶185.) Further, the modification would have been

nothing more than the simple combination of known elements to obtain predictable results. (*Id.*)

Furthermore, both the Parameters Module and the "information unit 23" can be integrated as a collection of components in the engine management system to collectively form the SCU, even if the two systems do not otherwise connect with or communicate with one another. (*See* VIII.B.2.c; '101, Fig. 6, 7:57-8:2; *see also* EX1012, 185-186; Ehsani ¶186.)

d. GPS (11[B], 16)

Petrik in view of Schanz discloses Claims 11[B] and 16 via Petrik's GPS module. (Ehsani ¶189; *see* §VIII.D.2 (Ground 4, 11[B]).)

e. Data Logging Device (11[C])

Petrik in view of Schanz discloses Claim 11[C] via the memory and smart card which store the information received from Petrik's GPS module. (Ehsani ¶190; *see* §VIII.D.2.)

3. Claim 5

Petrik in view of Schanz renders claim 5 obvious by way of Petrik's operating profile and in-vehicle unit memory. (Ehsani ¶201; *see* §VIII.D.7.)

Alternatively, a POSITA would have been motivated to modify Petrik's system to incorporate Schanz's "storage unit 2" for storing the "vehicle parameters 6," which can include "special vehicle parameters 6" "stored for the respective driver 4" (operating profile). (Ehsani ¶201; Schanz, [0017], [0020].) If parameters are

stored for the identified driver, they are used to "adjust[]" the "driving dynamic characteristics of the vehicle." (*Id*., [0020].) Therefore the "parameters" (operating profile) stored in "storage device 2" (memory module) are activated (loaded) for controlling operation of the vehicle when the driver is authenticated. For the reasons discussed in VIII.E.1, a POSITA would have been motivated to combine the storage of parameters (operating profile) from Schanz with Petrik's in-vehicle unit, as Schanz's "device 1" and Petrik's in-vehicle unit serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. (Ehsani ¶201.) In the combined system, Schanz's parameters would be loaded to the memory module of Petrik's in-vehicle unit. (*Id.*) Further, the modification would have been nothing more than the simple combination of known elements (Petrik's loading of route plan with Schanz's storage unit 2 for vehicle parameters) to obtain predictable results. (*Id.*)

4. Claims 8 and 13

Petrik in view of Schanz renders claims 8 and 13 obvious. (Ehsani ¶202.) As discussed in Ground 4, Petrik discloses a maximum speed restriction. (*See* VIII.D.10; Petrik, [0025].) Alternatively, it would have been obvious to combine Schanz's vehicle parameters into Petrik's smart card and in-vehicle unit. Schanz discloses additional definable "vehicle parameters 6" (operating profile) that include "a maximum vehicle speed 9." (Schanz, [0019].) Further, Schanz's "vehicle

parameters 6" can include driver-specific "special vehicle parameters 6" to control the vehicle "in relation to the driving skills of the respective driver." (*Id.*, [0020].) A POSITA would have been motivated to combine Schanz's device 1 with Petrik's analogous in-vehicle unit as discussed in VIII.E.1 to operate similarly with similar goals of providing additional driving restriction options. (*See also* Ehsani ¶202.)

5. Claims 9, 14, 17, 18

Petrik in view of Schanz renders claims 9, 14, 17, and 18 obvious. (Ehsani ¶203.) Petrik teaches an alarm for remotely alerting an authorized user when the operating profile is violated. (§VIII.D.11 (Ground 4); Petrik, [0030].) Further, Schanz discloses that "information unit 23" (part of SCU) "informs the driver 4 and/or the authorized person 24 about the set vehicle parameters 6" and "emits suitable optical and/or acoustic warning signals when the set vehicle parameters 6 are exceeded." (Schanz, [0025].) Schanz does not specify whether the "warning signal" of "information unit 23" is provided "remotely." However, Petrik discloses a "SATELITE/GPRS/GSM" link which connects its in-vehicle unit to a remote facility and allows the unit to report speed limit violations to the remote facility. (Petrik, [0030], [0063].) The combination of features from Petrik with features from Schanz, would enable a POSITA to employ Petrik's remote connectivity to generate Schanz's "warning signal" to the authorized user remotely (Ehsani ¶203; *see also* VIII.E.2.b,c.) A POSITA would have been motivated to combine Schanz's

information unit disclosures with Petrik's in-vehicle unit, as Schanz's "device 1" and Petrik's in-vehicle unit serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. (Ehsani ¶203; *see also* VIII.E.1.) Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results. (*Id.*)

6. Claim 10

Petrik in view of Schanz renders claim 10 obvious. (Ehsani ¶204.) To the extent Petrik does not disclose or render obvious using RFID, a POSITA would have been motivated to modify Petrik's smart card reader/writer based on Schanz to use a smart card capable of transmitting and receiving radio signals and would have looked to use RFID for the implementation, as was commonly used in automobiles. (*Id.*; Benco at [0003]). Schanz teaches a "transmitting and/or receiving unit for sending and/or receiving" "infrared or radio signals." (Schanz, [0018].) Both Petrik and Schanz are directed towards driver authentication and vehicle monitoring and control. (Petrik, [0025], Schanz, [0006], [0019].) A POSITA would have understood the benefits of implementing Petrik's smart card reader/writer with the capability to transmit and receive data signals for use in identifying the driver. (Ehsani ¶204.) A POSITA would accordingly have been motivated to apply Schanz's teachings to Petrik, and would have reasonably expected to succeed in doing so given the references' teachings. (*Id.*)

7. Claims 19 and 20

Petrik in view of Schanz renders claim 19 and 20 obvious. (Ehsani ¶205.) As discussed for the SCU limitations, Petrik's engine management system provides a control signal to slow down or disable the engine. (Petrik, [0025].) Alternatively, it would have been obvious to a POSITA to combine Petrik's engine management system with Schanz's teaching of actively intervening in driving operations to alert the driver. (Ehsani ¶205.) Schanz's "dynamic vehicle stabilization system" "actively intervene[s] in driving operation … to ***alert*** the beginner to critical driving situations." (Schanz, [0022] (emphasis added).) It would have been obvious to a POSITA, who would understand the benefits of and be motivated to combine the teachings of Petrik's control signal with Schanz's intervention to alert the driver, with reasonable expectation of success. (Ehsani ¶205.)

8. Claims 2-4, 6-7, 12, 16

Petrik in view of Schanz renders obvious claims 2-4, 6-7, 12, and 16. (*See* §§VIII.E.1, VIII.D.4-6, 8-9.)

F. Ground 6 – Petrik-Schanz-Benco Render Obvious Claim 10

It would have been obvious to a POSITA to implement Petrik's smart card and reader/writer with RFID in view of Benco. (Benco, [0002]-[0004], Ehsani ¶¶207-210; *see* §VIII.C.) A POSITA would have been motivated to integrate RFID into Petrik's smart card and reader/writer to simplify the log-in process for the driver. (*Id.*) Further, it would be trivial for a POSITA to implement this

combination, as it would involve merely combining a known technology (RFID) into a compatible technology (smart cards). (*Id.*; Benco, [0002]-[0004].)

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

A. The *Fintiv* factors strongly favor institution.

The Board should institute review because Petitioner has been diligent in filing its Petition and the circumstances surrounding the parallel district court case do not warrant discretionary 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 is in the early stages: fact discovery is in infancy; no claim construction proceedings have taken place and the *Markman* hearing is scheduled for August 2025 at the earliest; and trial is not scheduled until February 2026 at the earliest.

B. The *Advanced Bionics* two-part framework strongly favors institution.

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.

Under part one, the same or substantially the same art or arguments were *not* previously presented to the Office, ending the inquiry in favor of institution. 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 Patent Owner attempt to analogize any previously considered art or arguments to those presented here, Petitioner reserves the right to respond.

* * *

The Board should institute review because the merits are strong and the circumstances here trigger none of the discretionary denial policy considerations. Should Patent Owner raise any discretionary denial theory not addressed above, Petitioner reserves the right to respond before institution.

X. CONCLUSION

Petitioner respectfully requests that a Trial be instituted. Claims 1-20 of the '101 should be cancelled as anticipated and obvious over the prior art.

Date: January 6, 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

Counsel for Petitioner Mercedes-Benz Group AG

Table of Exhibits

Exhibit No.	Description
1001	U.S. Patent No. 9,045,101 ("**'101 Patent**")
1002	File History for the '101 Patent
1003	U.S. Patent No. 8,417,415 ("**'415 Patent**")
1004	Declaration of Dr. Mark Ehsani
1005	Curriculum Vitae of Dr. Mark Ehsani
1006	U.S. Patent No. 6,225,890 to Murphy ("**Murphy**")
1007	German Patent Application Publication No. DE 10,323,723 A1 to Schanz ("**Schanz**")
1008	English Translation of Schanz
1009	U.S. Patent Application Publication No. 2007/0168125 A1 ("**Petrik**")
1010	U.S. Patent Application Publication No. 2008/0136611A1 ("**Benco**")
1011	FMVSS No. 126: Electronic Stability Control Systems (March 2007)
1012	File History for U.S. Patent Reexamination Proceeding No. 90/015,287

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **Petition for *Inter Partes* Review** contains 13,819 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 1001 through 1012** were served on January 6, 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 '101:

64064 - Ortiz & Lopez, PLLC
P.O. BOX 4484
Albuquerque, NM 87196
United States

/s/ *Ky-Yen Wong*
Ky-Yen Wong
Hogan Lovells US LLP
4 Embarcadero Center, Suite 3500
San Francisco, California 94111