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

DECLARATION OF DR. MARK EHSANI IN SUPPORT OF MERCEDES' PETITION FOR INTER PARTES REVIEW OF CLAIMS 1-20 OF U.S. PATENT NO. 9,045,101

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

I, Dr. Mark Ehsani declare as follows:

I. INTRODUCTION

A. Engagement

1. I have been retained by Hogan Lovells US LLP on behalf of Mercedes-Benz Group AG ("Mercedes," or "Petitioner"), as an independent expert

in this proceeding before the Patent Trial and Appeal Board ("PTAB" or "Board"). I understand that Mercedes is requesting that the Board institute an *inter partes revies* ("IPR") proceeding of U.S. Patent No. 9,045,101 ("**'101**") (EX1001), currently assigned to The Phelan Group, LLC

2. Specifically, I have been retained to offer my opinions regarding Claims 1-20 of the'101 Patent and the prior art references forming the basis of unpatentability set forth in the IPR petition. This declaration is directed to the challenged claims of the '101 Patent and details the opinions I have developed, the conclusions I have drawn, and the basis for each.

3. I have no financial interest in either party or the outcome of this case. I am being compensated at my customary rate of $500 per hour for my time on this case. My compensation is not dependent on the contents of my opinions or the outcome of this proceeding.

4. I am familiar with the technology described in the '101 Patent as of its earliest possible priority date of July 2, 2008. I have been asked to provide my technical review, analysis, insights, and opinions regarding the '101 Patent. I have used this experience and insight along with the above-noted references as the basis for the grounds of unpatentability set forth in the Petition for *inter partes* review of the '101 Patent.

B. Background and Qualifications

5. My name is Dr. Mark Ehsani. I am currently a Professor of Electrical Engineering at Texas A&M University at College Station, where I also serve as the Director of Advanced Vehicle Systems Research Program and the Power Electronics and Motor Drives Laboratory. All my opinions stated in this declaration are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my 50 years of experience as an engineer, technical director, researcher, and research professor in energy systems, power electronics, motor drives, hybrid vehicles and their control systems, and sustainable energy engineering.

6. I am over 18 years of age and would be competent to testify as to the matters set forth herein if called upon to do so. I understand that a copy of my current curriculum vitae, which describes my complete education and professional experience, is being submitted by Petitioner as Exhibit 1005. The following provides an overview of some of my experience that is relevant to the matters set forth in this declaration.

7. I earned a bachelor's and master's degree in electrical engineering from the University of Texas at Austin in 1973 and 1974, respectively. After receiving my master's degree, I worked as a Research Engineer with the Fusion Research Center at the University of Texas doing research and equipment development on high power supplies and circuit breaker technology. I then earned

a Ph.D. in electrical engineering in 1981 from the University of Wisconsin-Madison. During my doctoral studies I focused on energy and control systems and served as a Resident Research Associate with Argonne National Laboratory.

8. I have authored over 500 publications in pulsed-power supplies, high-voltage engineering, power electronics, motor drives, and advanced vehicle systems. I have co-authored twenty-four books on power electronics, motor drives and advanced vehicle systems, including Vehicular Electric Power Systems, Marcel Dekker, Inc. 2003, and "Modern Electric Hybrid Vehicles and Fuel Cell Vehicles – Fundamentals, Theory, and Design", Third Edition, CRC Press, 2018. I currently serve on the editorial board of several technical journals and am the associate editor of IEEE Transactions on Industrial Electronics and IEEE Transactions on Vehicular Technology. Additionally, I have over 30 granted or pending US and EC patents.

9. My research has produced more than 500 journal and conference publications. More than 239 publications are in refereed journals. Many of my publications and research grants relate to vehicle control systems. Some examples include:

- M. Ehsani, R. L. Kustom, and R. E. Fuja, "Microcomputer Control of a Current Source DC-DC Converter," IEEE Trans. on Industry

Applications, Vol. IA-19, No. 5, September/October 1983, pp. 690-698

- M. Ehsani, and K. R. Ramani, “Direct Control Strategies Based on Sensing Inductance in Switched Reluctance Motors,” IEEE Trans. on Power Electronics, Vol. 11, No. 1, January 1996, pp. 74-82
- Y. Gao and M. Ehsani "Design and Control Methodology of Plug-in Hybrid Electric Vehicles," IEEE Trans. In Industrial Electronics, Vol. 57, No. 2, February, 2010.
- William Bradley, Kambiz Ebrahimi, Mehrdad Ehsani, “A General Approach for Current Based Condition Monitoring of Induction Motors, Part I: Introduction and General Theory,” submitted to IEEE Systems Journal.
- Y. Gao and M. Ehsani, “Electronic Braking System of EV and HEV – Integration of Regenerative Braking, Automatic Braking Force Control and ABS”, SAE Journal, Paper No. 2001-01-2478, August 2001
- Y. Gao and M. Ehsani, “A Mild Hybrid Drive Train for 42V Automotive Power Systems – Design, Control and Simulation”, SAE Journal, Paper No. 2002-01-1082, March 2002

- Y. Gao and M. Ehsani, “A Mild Hybrid Drive Train with a Floating Stator Motor— Configuration Control Strategy, Design, and Simulation Verification”, SAE Journal, Paper No. 2002-01-1878, June 2002
- H. Moghbelli, K. Ganapavarapu, R. Langari, and M. Ehsani, "A Comparative Review of Fuel Cell Vehicles (FCVs) and Hybrid Electric Vehicles (HEVs) Part I: Control Strategies, Power Train, Total Cost, Infrastructure, New Developments, Manufacturing and Commercialization,” SAE Transactions Volume on Journal of Engines, paper # 2003-01-2299

10. In the past 43 years, I have served as a consulting engineer to over 60 companies in the U.S and internationally on power electronics and its applications, as well as vehicle electrical and electronics systems and controls. I’ve received several honors and recognitions including the Prize Paper Awards in Static Power Converters and motor drives at the IEEE-Industry Applications Society 1985, 1987, and 1992 Annual Meetings and the Avant Garde Award from IEEE Vehicular Technology Society.

11. I have presented several short courses relating to vehicle control in the U.S. and internationally. Some examples include, Invited Short Course at LeTourneau, Longview, Texas and Texas Instruments, Dallas Texas, January 12 &

26, 1996: “Design and Control of Switched Reluctance Motor Drives”, U.S. Army Vetronics Institute 3rd Annual Winter Workshop at U.S. Army Tank-automotive RD&E Center Warren, MI, Jan 13, 2004: “Control of BLDC Machines with Improved Performance”, Invited Short Course at Hyundai Motor Company, Suwon, Korea, June 28, 2000: “Design and Control of Electric and Hybrid Electric Vehicles”, and Short Course at US Army Tank Automotive Command (TACOM), Warren, Michigan, January 2005: “Advanced Mobile Integrated Power System (AMPS).”

12. Based on my experience and education, I believe that I am qualified to opine as to the knowledge and level of skill of one of ordinary skill in the art at the time of the alleged invention of the ’101 Patent, as well as the state of the art at that time.

C. Information Considered

13. I have reviewed the ’101 Patent and its prosecution history, as well as the other materials referenced in Appendix A. Counsel has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the ’101 Patent, at the time of the earliest purported priority date of the ’101 Patent, and I have done so during my review of these materials. I have been asked to assume, for purposes of this Declaration, that the ’101 Patent has a priority date of July 2, 2008 (the “**Critical Date**”).

14. My analysis is based on my years of education, research, and work experience, as well as my investigation and study of relevant materials. In my analyses, I have considered the materials that I identify in this Declaration and those listed in Appendix A.

15. I may rely on these and additional materials to respond to arguments raised by the Patent Owner. I may also consider additional documents and information in further analyses—including documents that may not yet have been provided to me.

16. My review and assessment of the materials provided in this proceeding is ongoing, and I will continue to consider any new material as it is provided. I reserve the right to review, supplement, and amend my analyses based on new information and on my continuing review of the materials already provided.

II. OVERVIEW OF THE '101 PATENT

A. Background of the '101 Patent

17. I have reviewed the '101 Patent and its prosecution history. The '101 Patent is directed toward "[a] driver authentication and safety system and method for monitoring and controlling vehicle usage by high-risk drivers." (EX1001, 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.)

18. When entering the vehicle, a driver loads their identification information and operating profile restrictions 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 by use of a GPS which provides "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 be used to … 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 History of the '101 Patent

19. I understand the '101 Patent was filed on April 8, 2013, as a continuation of U.S. Patent No. 8,417,415 ("**'415**") (EX1003), filed on July 1, 2009, and Provisional application no. 61/077,568, filed on July 2, 2008. The '101 Patent received two office actions. In a Non-Final Rejection, claims 1-20 were rejected over U.S. Patent Pub. No. 2010/0004818 (publication of the '415).

(EX1002, ’101 File History, 99-104.) The Patent Owner overcame this rejection by filing a terminal disclaimer, amending independent claims 1, 11, and 15 to add governing mechanical operations remotely, and amending claim 10 to add “an iButton device; and a USB compatible device.” (*Id.*, 78-86.) In a subsequent Non-Final Rejection, claims 1-9, 11-20 were allowed and claim 10 was rejected as being indefinite because it claimed the trademark/trade name “iButton.” (*Id.*, 59-63.) The Patent Owner amended Claim 10 to remove the limitation “an iButton device.” (*Id.*, 49-52.) Following this, the examiner issued a Notice of Allowance. (*Id.*, 26-32.)

20. I understand that several prior art references relied on in this Petition were not before the PTO during prosecution of the ’101 Patent. Thus, I understand that the Petition presents substantially new arguments that were not considered during prosecution.

C. Priority Date

21. I have been asked to assume, for purposes of this Declaration, that the ’101 Patent has a priority date of July 2, 2008. Assuming this earliest date, I understand that all prior art references asserted in this Petition are prior art.

III. CLAIM CONSTRUCTION AND POSITA DEFINITION

A. Claim Construction

22. I understand that in an *inter partes* review, claims must be given their ordinary and customary meaning, as understood by one of ordinary skill in the art in light of the prosecution history. I apply that standard in my analysis below to the words and phrases in the claims of the ’101 Patent.

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

23. A person of ordinary skill in the art (“**POSITA**”) in the field of the ’101 Patent and 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 with research, design, and/or development of automotive electrical and control systems or an equivalent level of skill knowledge, and experience. The more education one has, the less experience needed to attain an ordinary level of skill. Similarly, more experience in the field may serve as a substitute for formal education.

IV. UNDERSTANDING OF LEGAL STANDARDS

A. Anticipation

24. I understand that a patent claim is invalid when the invention that it claims is not new. To establish that a claimed invention is not new (a.k.a., “not novel”), I understand that one may establish that a single publication, or other reference in the prior art discloses (explicitly or inherently) every element required in a patent claim (i.e., all features or “limitations” recited in the patent claim). I

understand that a reference in the prior art "anticipates" a claimed invention if that reference discloses, either explicitly or inherently, every element of the claim.

25. I understand that "prior art" and "prior art reference" are legal terms of art referring to, for example, devices, methods, and publications that predate the earliest effective filing date of the claimed invention.

26. I understand that a prior art reference that anticipates a claim may disclose an element or limitation of a patent claim expressly or inherently. A prior art reference discloses an element or limitation of a patent claim inherently when the prior art's disclosure necessarily requires or implies that the claimed element or limitation be present in the process, machine, manufacture, or composition disclosed. I understand there is still considered to be an inherent disclosure even if the author of the reference did not describe or understand the underlying inherent principle. I understand that one may establish that a prior art reference inherently discloses a claimed element or limitation through the use of other reference material or through testing.

27. I understand that the description in a written reference does not have to be in the same words as the claim, but all of the requirements of the claim must be there, either stated or necessarily implied, so that a POSITA looking at that one reference would be able to make and use the claimed invention.

28. I understand that any prior art reference that can be considered for purposes of determining whether it anticipates a patent claim may also be used to determine whether the reference renders that claim obvious, as discussed below.

B. Obviousness

29. I understand that, even if a claim is not fully disclosed in a single prior art reference, the patent claim is invalid if the invention would have been obvious to a POSITA at the time of the invention. In particular, I understand that a patent claim is normally invalid as obvious if it would have been an "ordinary innovation" within the relevant field to create the claimed product or method at the time of the invention.

30. I understand that the relevant portion of pre-AIA Section 103, subsection (a) of the Patent Act states:

> "A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

31. I understand that, by way of example only, a claimed invention is obvious if:

it combines prior art elements according to known methods to yield predictable results;

it simply substitutes one known element for another to obtain predictable results;

it uses a known technique to improve similar devices (methods, or products) in the same way;

it applies a known technique to a known device (method, or product) ready for improvement to yield predictable results;

it was "obvious to try" in that the inventor chose from a finite number of identified, predictable solutions, with a reasonable expectation of success;

known work in one field of endeavor prompted variations of it for use in either the same field or a different one based on design incentives or other market forces and those variations were predictable to one of ordinary skill in the art; or

some teaching, suggestion, or motivation in the prior art led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

32. When considering obviousness, I understand that I am to: (i) decide the level of ordinary skill in the field that someone would have had at the time the alleged invention was made; (ii) determine the scope and content of the prior art; (iii) determine what differences, if any, existed between the prior art and the

Asserted Claims; and (iv) consider objective evidence of non-obviousness (also known as secondary considerations). Further, when considering obviousness, I understand that it is not necessary to seek out precise teachings, and it is permissible to consider the inferences, common sense, and creative steps that a POSITA (who is considered to have an ordinary level of creativity and is not an automaton) would employ.

33. I understand that objective evidence relevant to the issue of obviousness may also be considered. This type of evidence is sometimes referred to as "secondary considerations," and may include evidence of commercial success, long-felt but unsolved needs, failure of others, and unexpected results. I understand that any secondary evidence must have a nexus to the relevant claims. For example, I understand that commercial success must have a nexus to features of the alleged invention not disclosed in the prior art, and in particular the prior art references which support an obviousness theory. In other words, I understand that commercial success is material only if it comes from the merits of the claimed invention beyond what the prior art disclosed. With respect to secondary considerations, I understand that Patent Owner bears the burden of proof, and I have seen no evidence to date that any secondary considerations would establish non-obviousness.

V. THE ELEMENTS IN CLAIMS 1-20 OF THE '101 PATENT ARE ANTICIPATED AND RENDERED OBVIOUS BY THE PRIOR ART

34. I have been asked to provide an analysis as to whether the elements of Claims 1-20 of the ’101 Patent (the “**Challenged Claims**”) are disclosed in the primary prior art references: U.S. Patent No. 6,225,890 to Murphy (“**Murphy**”) (EX1006) and U.S. Patent Application Publication No. 2007/0168125 A1 to Petrik (“**Petrik**”) (EX1009). I was also asked to consider these references in view of certain additional prior art for the Challenged Claims, including German Patent DE10323723A1 to Schanz (“**Schanz**”) (EX1007, EX1008) and U.S. Patent Application Publication No. 2008/0136611 A1 to Benco (“**Benco**”) (EX1010).

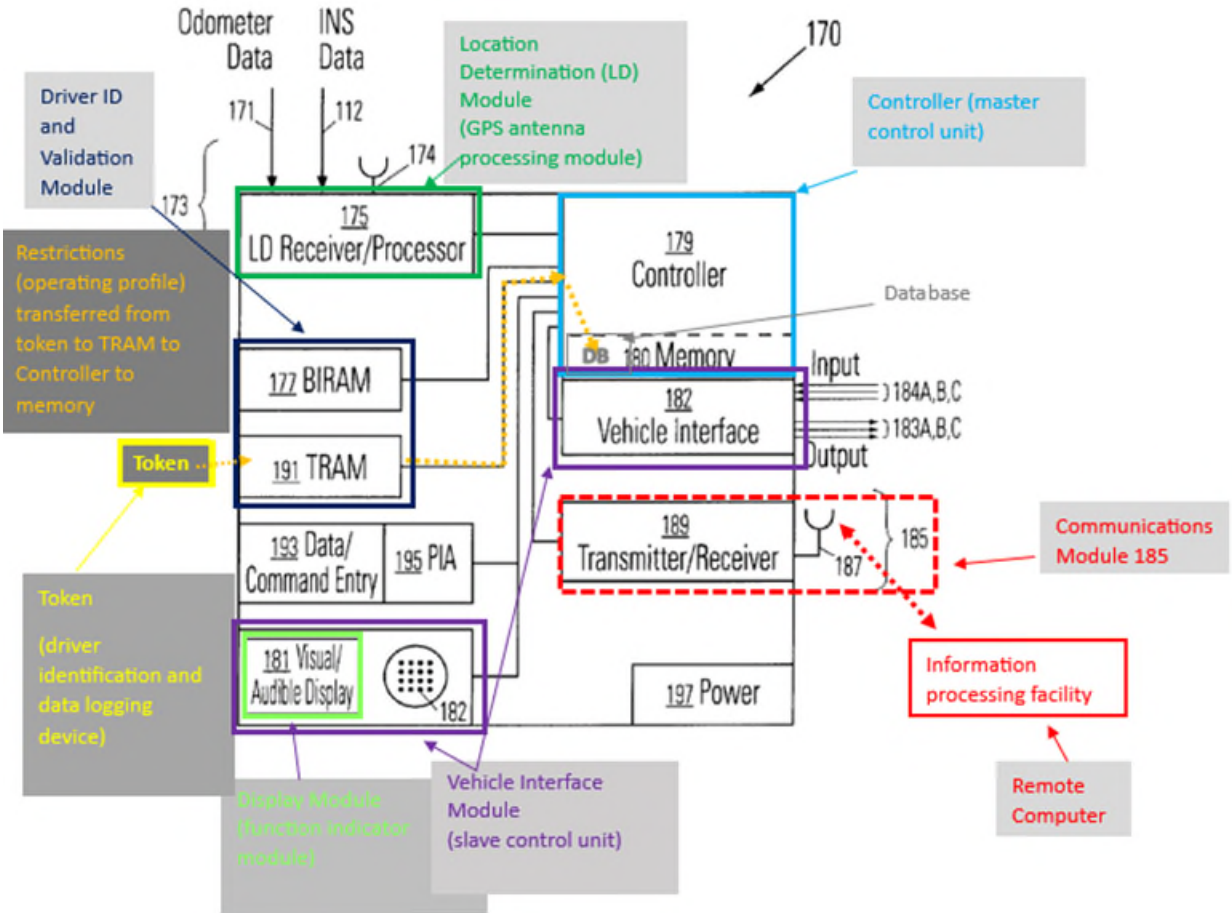
35. My analysis of these prior art references relative to the elements of the Challenged Claims—specifically, how and where the prior art references disclose the limitations of the challenged claims—is provided below. The citations that I have included are not intended to provide an exhaustive list, but rather provide examples of how the references disclose or teach the elements of these claims.

A. Grounds Based on Murphy

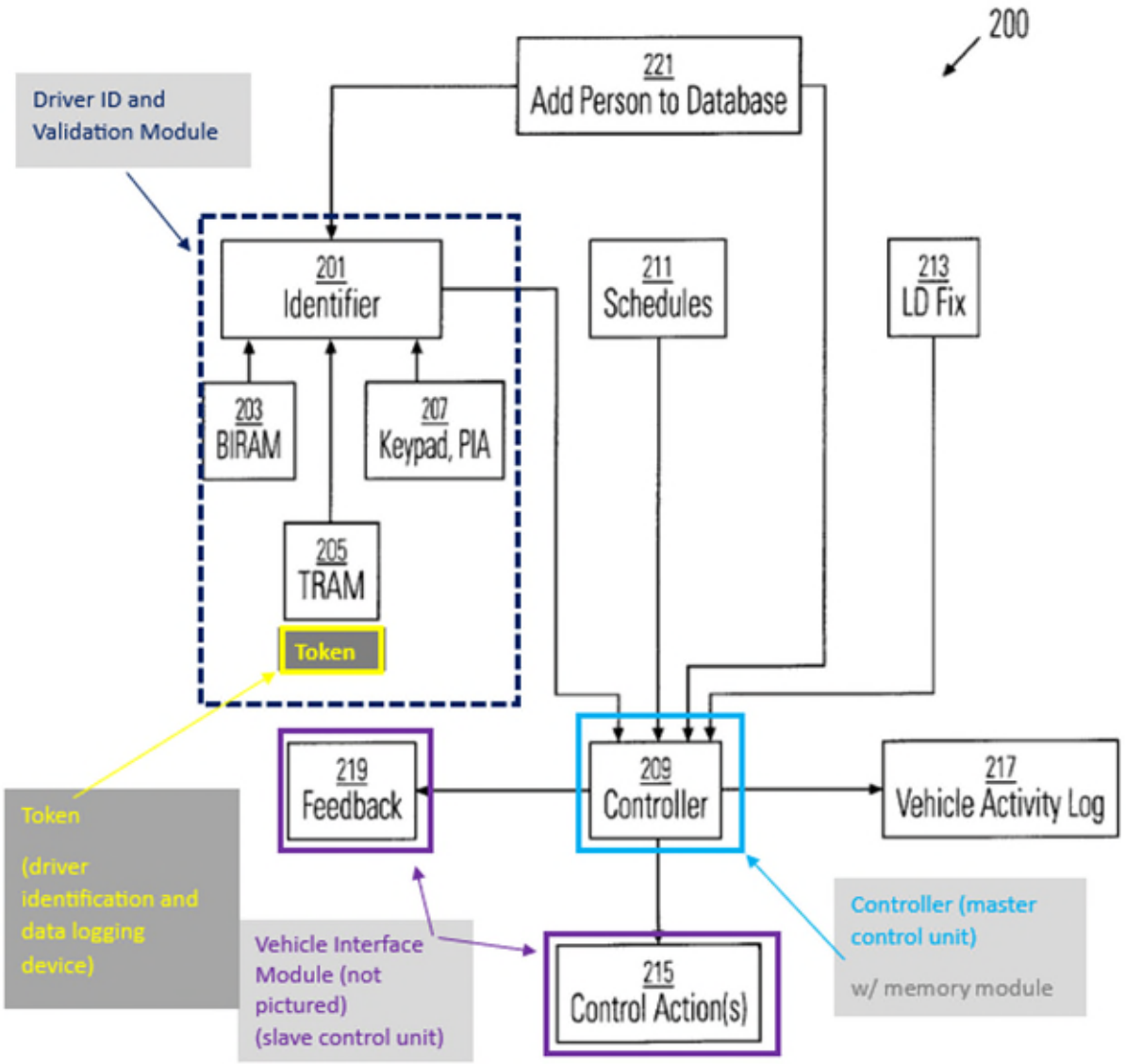
36. I have reviewed Murphy which is U.S. Patent 6,225,890. I understand that Murphy was filed on March 20, 1998, and issued on May 1, 2001. Murphy is directed towards “imposition or restrictions on or control of use, or inappropriate use, of a vehicle by a vehicle operator, in a manner that minimizes the possibility of evasion by a (restricted) operator.” (Murphy, 1:3-7.)

37. My review of the ’101 Patent history reveals that Murphy was not considered during the prosecution of the ’101 Patent.

Murphy discloses a system that monitors a designated vehicle, authenticates the identity of 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 the restrictions are violated, the system “takes at least one of 12 Control Actions” including “disable[ing] the vehicle at a selected time so that the vehicle no longer operates” or “reduc[ing] the vehicle speed to a selected speed range, using a vehicle ‘governor’.” (Id., 5:29-60.)



(Murphy, Fig. 6 (annotated).)



(*Id.*, Fig. 7 (annotated).)

1. Ground 1: Murphy Anticipates or Renders Obvious Claims 1-20

a. Independent Claims 1, 11, 15

38. As viewed by a POSITA, Murphy anticipates or renders obvious Claims 1, 11, and 15.

i. Preamble (1[P])

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

39. Murphy discloses the preamble of claim 1 to the extent the preamble limits the scope of the claims. Murphy describes a system that validates the identity of a driver through a presented identity indicium (e.g. fingerprint or encoded information on a token or smart card) and allows the driver to operate the vehicle within specified operating parameters (e.g. permitted time intervals, accumulated time and/or mileage range, or travel corridors) (Murphy, Abstract, Fig. 1). The vehicle monitors for conformity with the imposed restrictions and can disable the vehicle's operation or activate a coded alarm signal if the operating parameters are exceeded. (*Id.*)

ii. Master Control Unit (1[A])

1[A]	*a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;*

40. Murphy discloses or renders obvious Claim 1[A] ("**Master Control Unit limitations**"). Murphy's controller 170 is a master control unit in a motor vehicle as recited in claim 1[A]. The controller module receives information presented to a TRAM 191 (token receiving and analysis mechanism and/or a BIRAM 177 (biometric indicum receiving and analysis mechanism) and uses that

information to identity and authenticate the driver providing the indicium. (Murphy, 13:35-40, 14:51-54). The token (or smart card) presented to the TRAM may contain "pre-programmed information in a storage medium" which can identity the driver or imposes restrictions on the vehicle's operation. (*Id.*, 6:59-62.) This information corresponds to pre-programmed, driver-specific operating profile, including driver-specific geographical, speed, and temporal restrictions on vehicle operation specific to the token holder. (*Id.*, 6:62-7:14.) This information is loaded to the controller module through the TRAM. (*Id.*, 6:59-14, 14:46-54 ("Information obtained by the TRAM 191 is communicated to the controller 179 for implementation").) The driver-specific geographical, speed, and temporal restrictions information can also be loaded to the controller or changed via the communications module 185. (*Id.*, 12:16-27.) Drivers can also provide a biometric indicum to the BIRAM for additional identification purposes. (Murphy, 13:33-42).

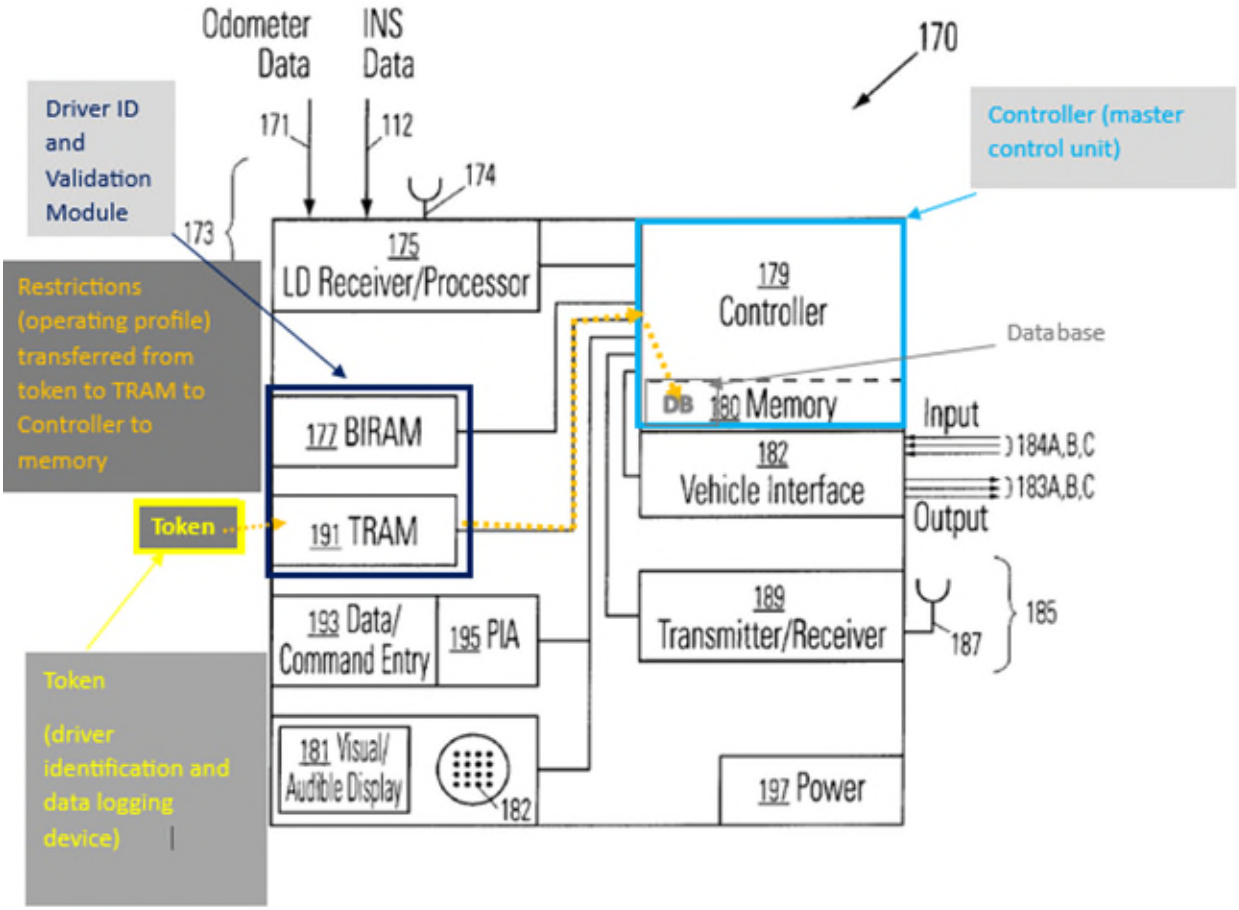
41. The token presented to the TRAM is a driver identification and data logging device, which is used to identify the driver and store information, and the controller module is a master control unit that identifies and authenticates the driver via TRAM and BIRAM. (Murphy, 4:39-44, 5:13-24, 6:55-59, 15:66-16:11.)

42. Once a driver is authenticated, the system monitors operation of the vehicle to determine if operation of the vehicle is within the permitted parameters (permitted time intervals, permitted travel region, and/or permitted speed range).

(Murphy, 5:18-26; Figs. 2A-5.) These time, location, and/or speed restrictions can be assigned individually to each driver. (*Id.*, 6:8-18.) If a driver violates the restrictions, the controller module chooses one of 12 Control Actions to take including "disable[ing] the vehicle at a selected time so that the vehicle no longer operates" or "reduc[ing] the vehicle speed to a selected speed range, using a vehicle 'governor'." (*Id.*, 5:29-60; Figs 2A-5.) The controller module then communicates the chosen Control Action to the vehicle interface module 182/Control Action interface module 215 which in turn implements the Control Action through the "vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory or other appropriate system on the vehicle." (*Id.*, 15:37-42.) Thus, the controller module is programmed with an operating profile including operating restrictions (time, location, and/or speed restrictions which can be loaded from the token and/or communications module) in which the driver is permitted to operate the vehicle.

43. Murphy also discloses a "unique identification code" that the controller receives to allow a driver to operate a vehicle within a specific operating profile. The controller performs a comparison between the information it receives from the token and/or biometric sample and the stored identification indica for the purpose of authenticating the driver. (Murphy, 2:35-45, 5:13-17.) The token corresponds to a vehicle and (at least is some embodiments) is "specific for the

person who presents the token." (*Id.*, 6:55-59, 7:1-2.) "[A]t least part of the information contained on the token is encoded or encrypted, and the token-accepting system is programmed to decrypt or decode and use the token information . . . ." (*Id.*, 7:5-7.) In order for the encoded/encrypted information to be used to identify an individual driver, the encoded/encrypted information within the token and/or biometric sample presented to the controller must necessarily comprise some unique code since the information must be unique to the driver. (*Id.*, 2:20-34, 6:55-7:14, 14:46-54; *see also id*., 16:53-17:2 (listing possible biometric sample types including fingerprint, thumbprint, handprint, retinal scan, blood vein pattern scan, and blood sample analysis); *Id.*, 17:63-19:2 (discussing various methods and systems for analyzing biometric indicia that rely on unique codes such as a blood vein pattern, an eye's "optical fingerprint", and a "24-byte code for storing" fingerprint information).)



(Murphy, Fig. 6, annotated.)

iii. Slave Control Unit (1[B])

1[B]	*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;*

44. Murphy discloses or renders obvious Claims 1[B] ("**Slave Control Unit limitations**"). Murphy's vehicle interface 182 and Control Action(s) interface module 215 are each a slave control unit. With respect to Fig. 6, Murphy teaches that the controller module 179 is "connected to a vehicle interface module 182 that is in turn connected to at least one vehicle component, such as vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories, for use in controlling or restricting" vehicle operation. (Murphy, 13:66-14:4.) A POSITA would understand that there could be one or more electrical control unit (ECU) between the controller module and the vehicle component(s) to implement controlling or restricting the components. Murphy further teaches that "controller module 209 determines which Control Action(s)" "should be imposed on vehicle use and communicates this information to a Control Action interface module 215 for implementation by the vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory or other appropriate system on the vehicle." (*Id.*, 14:37-42.) A POSITA would understand the vehicle interface module 182 and the Control Action(s) interface module 215 as describing the same module in different embodiments because they relate to the same functionality in figures corresponding to different embodiments. Murphy describes both the vehicle interface module 182 and the Control Action interface module 215 as connected to the controller module and responsible for

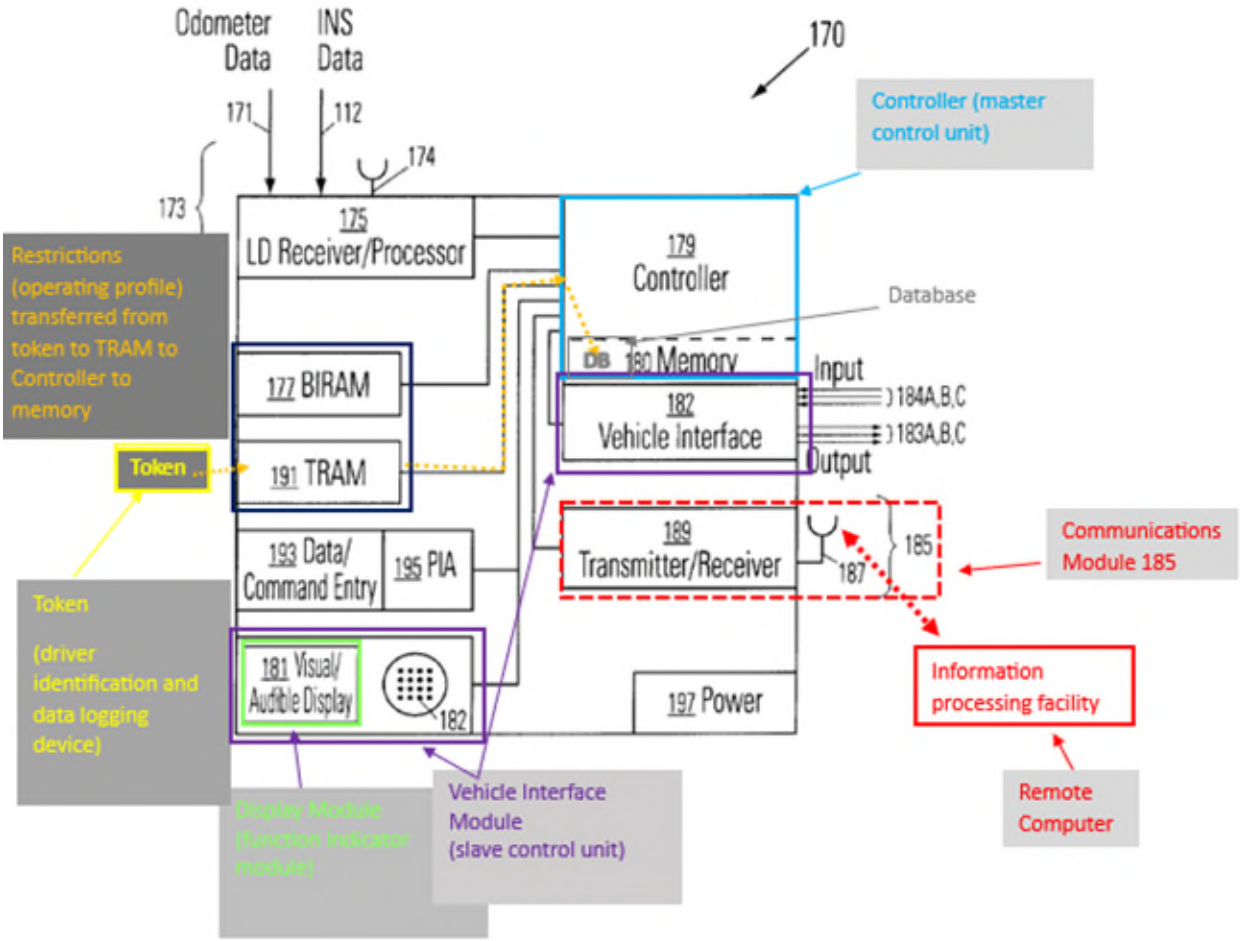
implementing the vehicle operation restrictions via the vehicle components each are connected to. (*See id.*, 13:65-14:17 (vehicle interface 182 connected to "vehicle components to be controlled" such as "the vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories"), 15:39-42 (Control Action interface module 215 implements Control Actions on the "vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory or other appropriate system on the vehicle").) These modules (collectively the "**Control Action module**") control the systems such as the engine, vehicle speed, and vehicle acceleration. The Control Action module interacts with the vehicle components and sends the appropriate signals to cause the components to implement the control action. For example to control the braking system, they would send signal to a controller for the braking system that would then cause the braking components to activate a braking action.

45. Murphy describes 12 different Control Actions including: "(1) the system (temporarily) disables the vehicle at a selected time so that the vehicle no longer operates, through fuel cutoff, air brake disablement or some other similar measure; (2) the system (temporarily) disables use of selected vehicle accessories, such as a winch, pump, cargo lift, cargo lock, dump mechanism, emergency lights or flashers, or door locks; (3) the system reduces the vehicle speed to a selected speed range, using a vehicle "governor" or some other suitable approach; (4) the

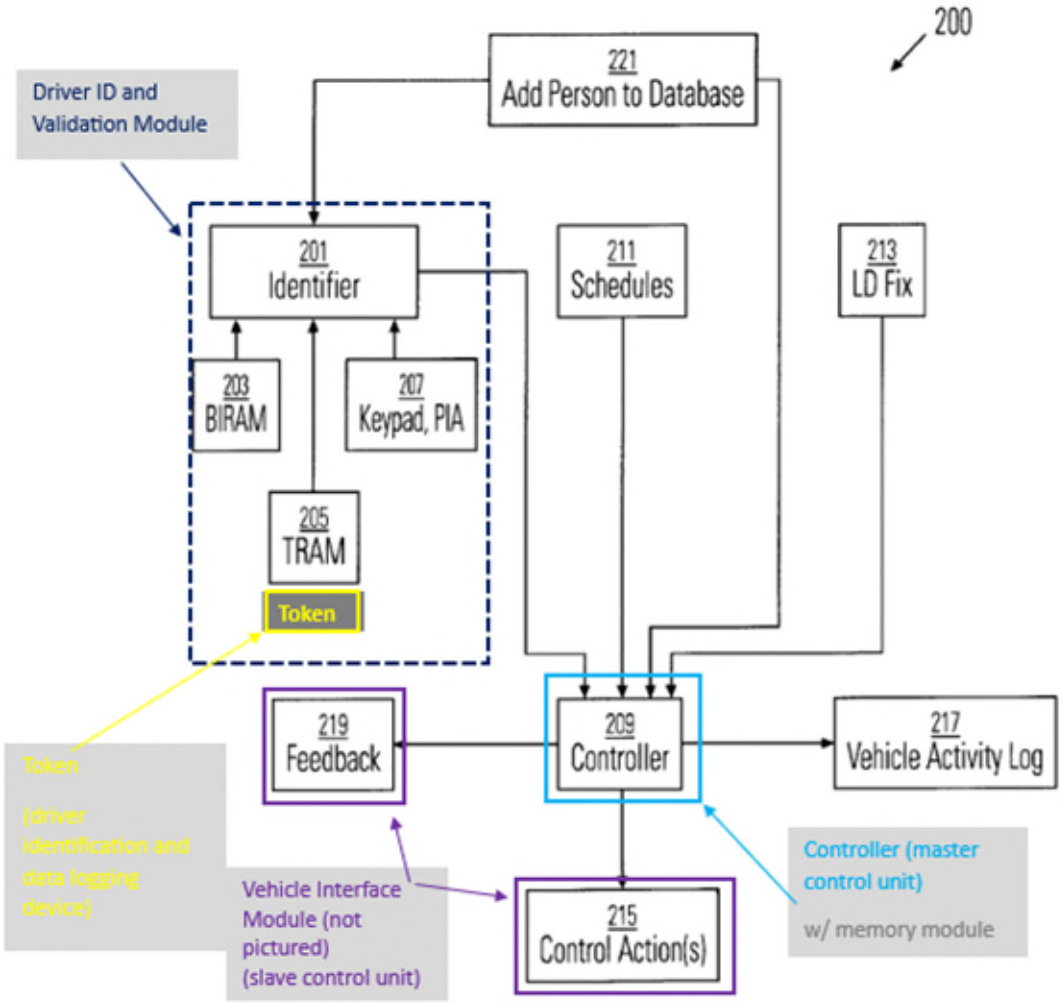
system forces the vehicle to operate only in selected lower gears, such as first and second; (5) the system turns on at least one of the lights, exterior flashers and horn continuously or periodically; (6) the system activates an on-board alarm the is visually or audibly perceptible to a person outside the vehicle; (7) the system transmits an alarm (optionally silent) to a selected facility that is spaced apart from the vehicle; (8) the system activates an air bag or other disabling device on the driver's side of the vehicle; (9) the system allows the vehicle to operate for at most a selected cumulative time interval; (10) the system allows the vehicle to operate only within one or more selected time intervals; (11) the system allows the vehicle to operate for at most a selected cumulative vehicle mileage; and (12) the system takes no action at that time but optionally logs the activity and allows the driver to operate the vehicle without restriction for a selected time interval." (Murphy, 5:29-54.) An option exists for the controller to connect to a display system that verbally announces or visually displays an announcement that a violation has been committed and/or that the vehicle will disable within a selected time interval (e.g., 30-60 sec) and/or that a driver should veer off the road before disablement. (*Id.*, 5:30-60; *see also id.*, 10:36-38 ("the driver can be advised, using a visually perceptible and/or audibly perceptible presentation device, that this specified limit is being approached.").)

46. As I explained for the Master Control Unit limitations, the controller module is programed with an operating profile (e.g., time, location, and/or speed restrictions) and communicates a Control Action to the Control Action module when restrictions are violated. (Murphy, 5:18-60, 15:37-42.) A communication module can be used to modify restrictions remotely. (Murphy, 12:16-20.)

47. Thus, the "Control Action module" is a Slave Control Unit that is in communication with and configured to receive instructions from the Master Control Unit (controller module) to generate an alarm if the driver of the vehicle violates restrictions within the specific operating profile (Control Action, e.g., reduce the vehicle speed using a governor), thereby providing feedback about said vehicle usage and govern 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.



(Murphy, Fig. 6 (annotated).)



(Murphy, Fig. 7 (annotated).)

iv. Preamble (11[P])

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

48. Murphy discloses the preamble of claim 11 to the extent the preamble limits the scope of the claims for the same reasons I discussed above for claim 1[A]. (Murphy, Abstract, Fig. 1).

v. Master Control Unit (11[A])

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;*

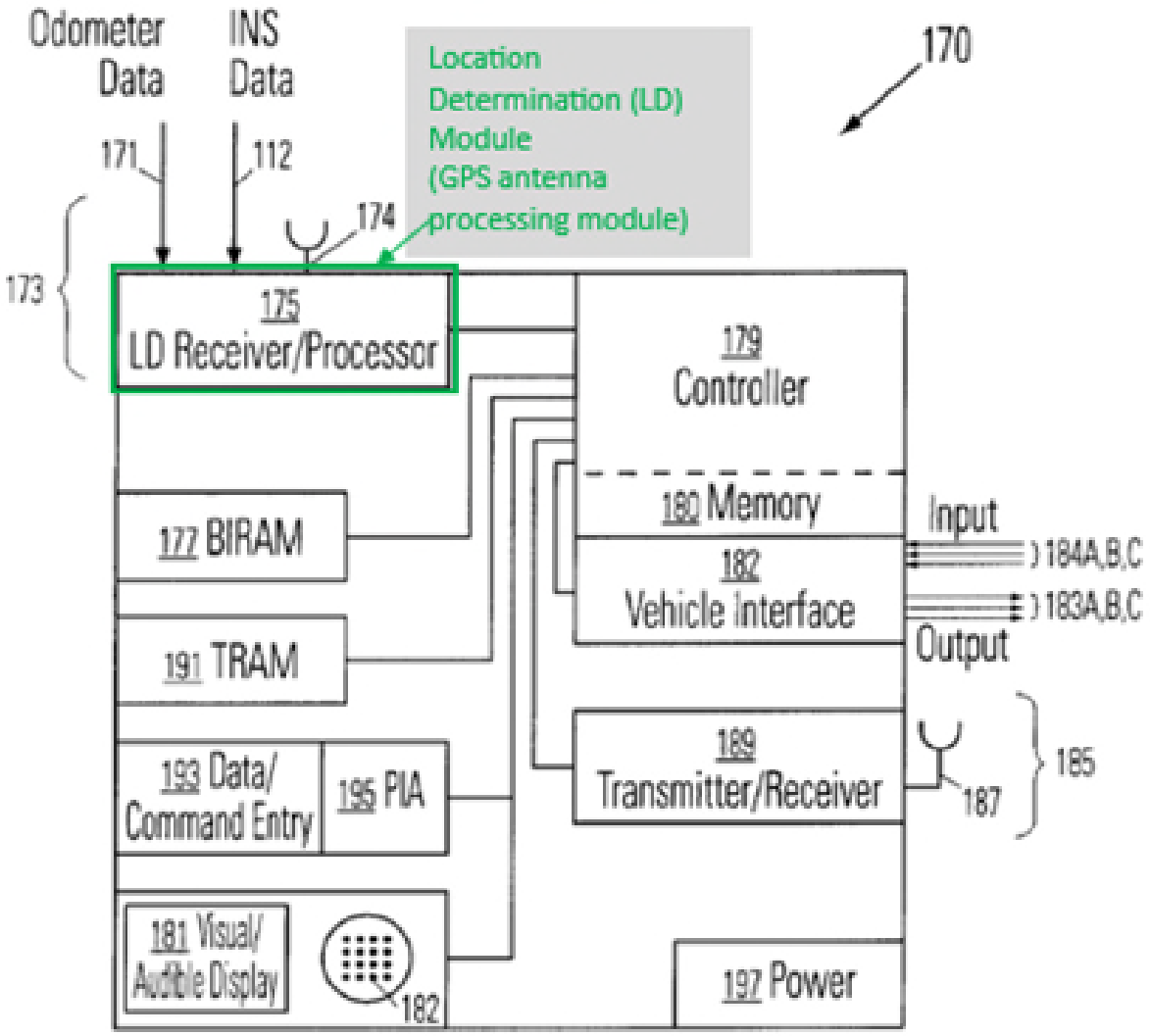
49. Murphy discloses or renders obvious Claim 11[A]. As I previously discussed for claim 1[A], Murphy discloses a master control unit. (*See* Section V.A.1.ii (claim 1[A]) *supra*). In addition to the elements of claim 1[A], Claim 11[A] also requires "associating an operating profile with said at least one driver." Because the controller loads an operating profile containing driver-specific time, location, and/or speed restrictions when a driver is identified, the operating profile is associated with the driver, allowing the driver to operate the vehicle within the parameters of the associated restrictions. (Murphy, 5:18-26, 6:8-18, 6:59-7:14, 14:46-54.)

vi. GPS (11[B])

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

50. Murphy discloses or renders obvious Claim 11[B]. Murphy teaches that an LD (location determination) module 173 collects information on the present time location and/or vehicle speed and/or time and/or accumulated operating time and/or accumulated mileage and sends the information to the controller module. (Murphy, 13:53-65.) The controller module compares information sent by LD module with any vehicle operation restrictions. (Murphy, 13:53-65.) Murphy

further instructs that the LD module can be implemented using GPS to determine present location and/or speed and/or observation time. (*Id.*, Abstract, 3:48-56 ("the LD module 19 determines the present location, present speed (optional) and observation time (optional) of the antenna 21, and thus of the vehicle 13, in a manner well known in the art").)

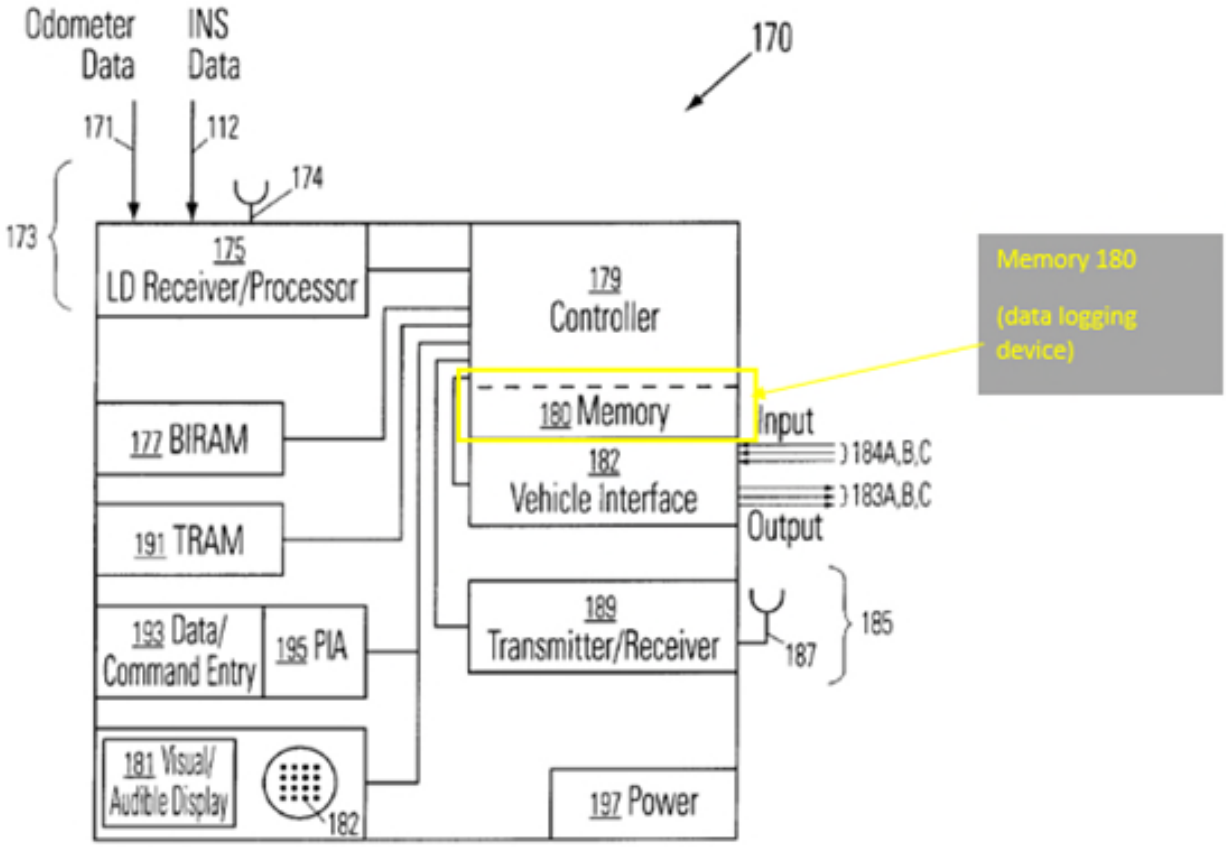


(Murphy, Fig. 6 (Annotated).)

vii. Data Logging Device (11[C])

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*

51. Murphy discloses or renders obvious Claim 11[C] ("data logging device"). Murphy teaches that "[i]nformation on the present vehicle location and/or vehicle speed and/or time and/or accumulated operating time and/or accumulated mileage is sent by the LD module 173 to the controller module 179." (Murphy, 13:53-65.) Murphy teaches the "system can maintain its own operations log, including periodic recording of the present observation time, vehicle location and/or vehicle speed in a memory…." (*Id*., 12:1-3.) Murphy discloses that such location and speed information is recorded to the memory 180 (data logging device) of the controller module 179 by LD module (i.e., GPS module). (*See* supra V.A.1.vi (Ground 1, Claim 11[B]); s*ee also* Murphy, 15:32-54, 15:66-16:11.)



(Murphy, Fig. 6 (annotated).)

viii. Slave Control Unit (11[D])

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;*

52. Murphy discloses or renders obvious Claim 11[D]. As I previously discussed for claim 1[B], Murphy discloses a slave control unit. (*See* Section V.A.1.iii (claim 1[B]) *supra*).

ix. Unique Identification Code (11[E])

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.*

53. Murphy discloses or renders obvious Claim 11[E]. As I previously discussed for claim 1[A], Murphy discloses a master control unit that receives a unique identification code. (*See* Section V.A.1.ii (claim 1[A]) *supra*.) In addition to the elements of claim 1[A], Claim 11[E] also requires permitting the driver to operate within an operating profile if "said at least one driver has not violated said operating profile." Murphy teaches a control action to disable the vehicle when the driver violates one of the operating restrictions that constitute an operating profile. (Murphy, 5:29-60.)

x. Preamble (15[P])

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

54. Murphy discloses the preamble of claim 15 to the extent the preamble limits the scope of the claims for the same reasons I discussed above for claim 1[A]. (Murphy, Abstract, Fig. 1).

xi. Driver Authentication and Monitoring System 15[A]

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

55. Murphy discloses or renders obvious Claim 15[A]. As I discussed above for claim 1[A], Murphy discloses a controller 179 connected to TRAM 191 and BIRAM 203 which monitors for violations of certain operating parameters, which is "providing a motor vehicle with a driver authentication and monitoring system." (*See* Section V.A.1.ii (claim 1[A]) *supra*.)

xii. Operating Profile (15[B])

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

56. Murphy discloses or renders obvious Claim 15[B]. As I discussed above for claim 1[A], Murphy discloses information pre-programed information including operating restrictions into the token that are loaded into the controller, which is "programming said driver authentication and monitoring system with an operating profile associated with a high risk driver." (*See* Section V.A.1.ii (claim 1[A]) *supra*; *see also* Section V.A.1.v (claim 11[A]) *supra*.)

xiii. Monitoring Operation (15[C])

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;*

57. Murphy discloses or renders obvious Claim 15[C]. As I discussed above for claim 1[A], Murphy discloses presenting a token to the TRAM to authenticate a driver and enable operation within the operating restrictions from the token and/or communications module, which is "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." (*See* Section V.A.1.ii (claim 1[A]) *supra*; *see also* Section V.A.1.v (claim 11[A]) *supra*.)

xiv. Alarm Signal (15[D])

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

58. Murphy discloses or renders obvious Claim 15[D]. As I discussed above for claim 1[B], Murphy teaches that when an operating restriction is violated, the vehicle interface module 182 and control action interface module 215 receive a control action from the controller and in response generate a signal to "the vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory or other appropriate system on the vehicle." (*See* Section V.A.1.iii (claim 1[B]) *supra*; Murphy, 14:37-42.) The control action can include a signal to reduce vehicle speed, which is consistent with an alarm signal according

to the ’101 patent. (*Id.*; ’101 Patent at 6:65-7:5 (“alarm signal” includes signal to slow down vehicle).) Therefore, Murphy discloses “generating an alarm signal if said high profile driver violates said operating profile while operating said motor vehicle.”

xv. Governing Mechanical Operations (15[E])

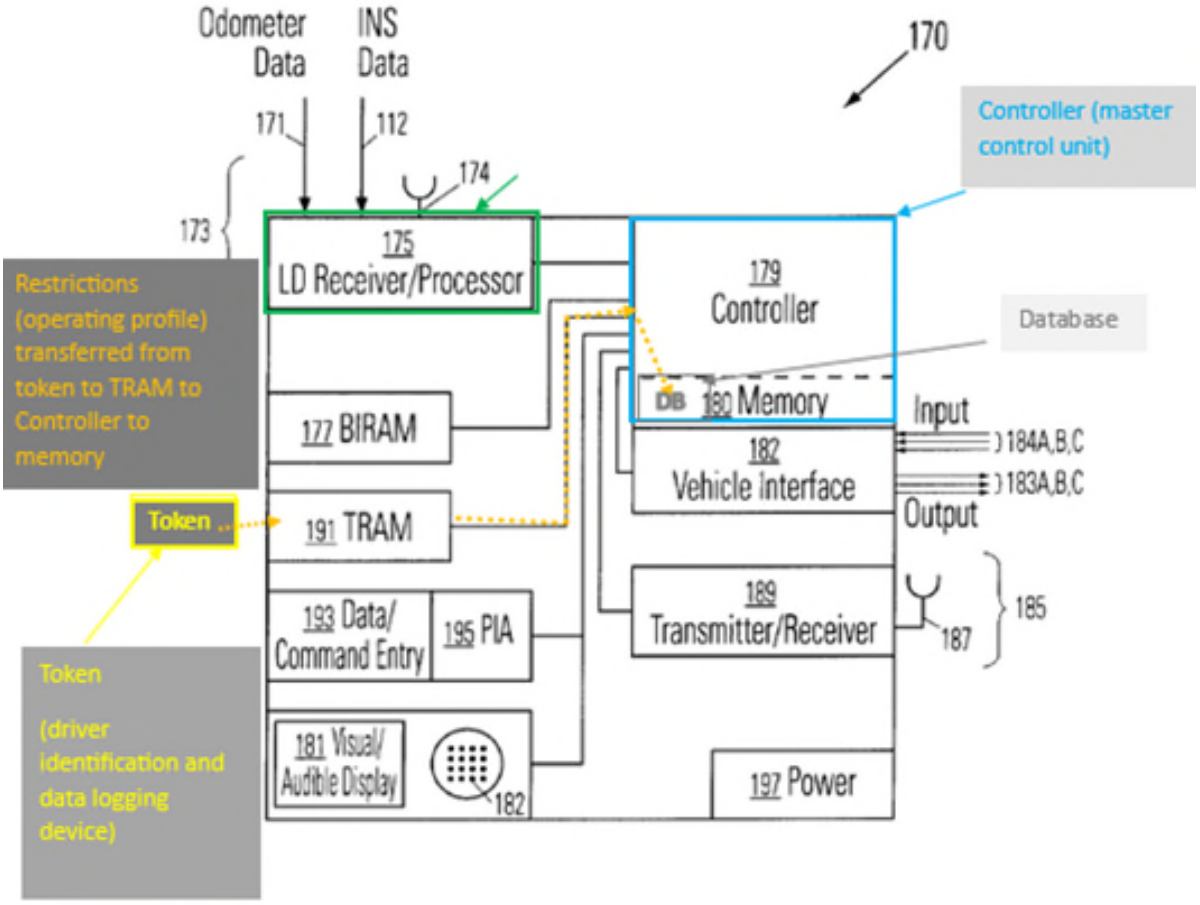
15[E]	*governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.*

59. Murphy discloses or renders obvious Claim 15[E]. As I discussed for claim 1[B], Murphy teaches a control signal to slow down or disable the vehicle when an operating restriction, which can be loaded or changed remotely through the communications module, is violated. (*See* Section V.A.1.iii (claim 1[B]) *supra*; Murphy, 14:37-42.) Therefore, Murphy discloses “governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.

b. Dependent 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.*

60. Murphy anticipates or renders Claim 2 obvious. Murphy teaches that the controller includes a memory unit which a database with information for each authorized driver including identity, indicia, schedules applicable to driver, locations, speed range, times of operation, and other operating parameters associated with the vehicle. (Murphy, 15:15-21, 15:66-16:9.) Operating parameters may be modified remotely through the communications module. (*Id.*, 12:16-27.) Additionally, Murphy instructs that the telecommunication module is part of apparatus 170 and that an "information processing facility can transmit signals that modify, add or delete vehicle operation restrictions, for receipt by the apparatus 170, 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 the conditions under which a vehicle operation restriction is imposed." (*Id.*, 14:27-35.) A POSITA would understand the facility, which is remote from the vehicle, to include at least one computer that transmits the information over a network to the vehicle.



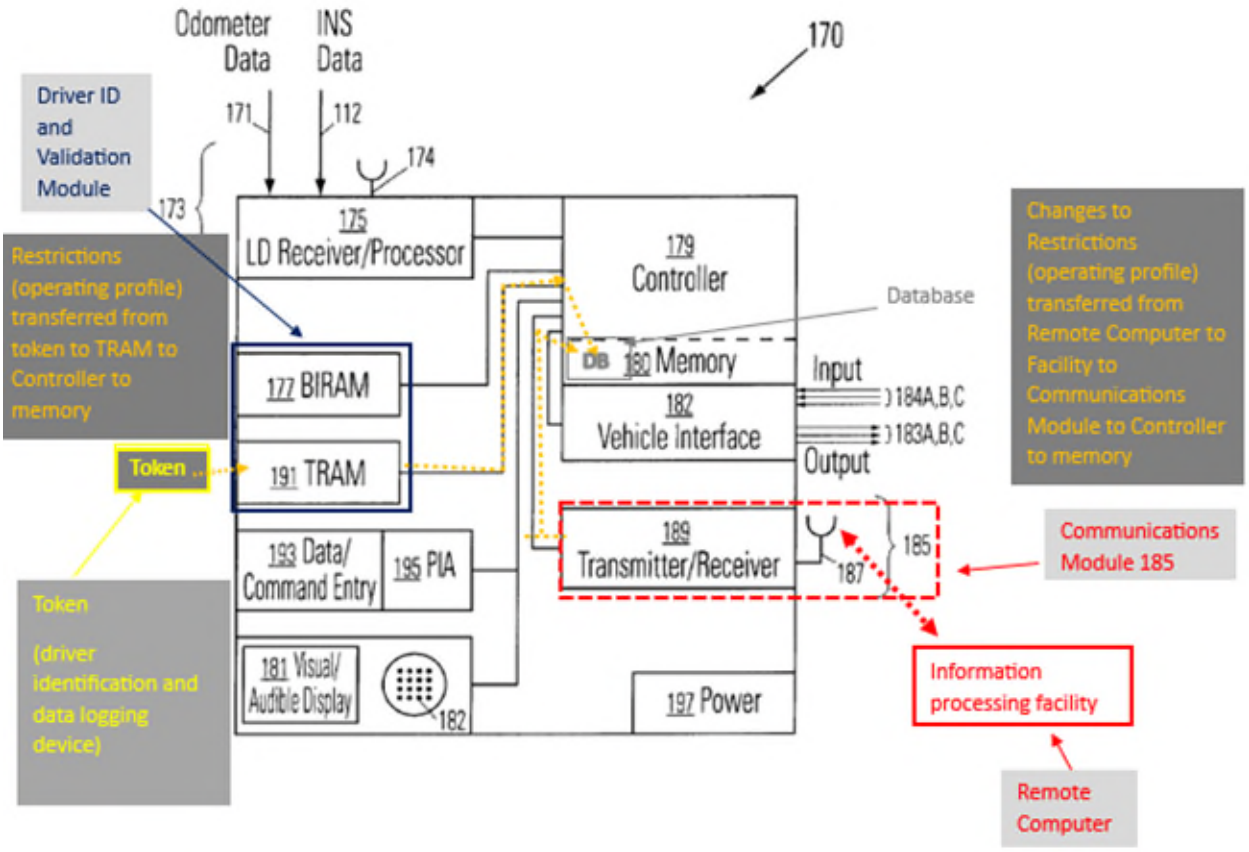
(Murphy, Fig. 6 (annotated).)

c. Dependent 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.*

61. Murphy discloses or renders obvious Claim 3. Murphy teaches that the operating parameters can be loaded or modified remotely through the

communication module. (Murphy, 12:16-27.) Further, Murphy teaches the token or smart card can include a circuit that identifies the token holder and imposes restrictions such as geographical, speed, and time restrictions on vehicle operation. (*Id.*, 6:55-7:14.) These parameters, which can be loaded from the token or smart card and changed remotely via the communications module, after being loaded from the token or remotely, may be stored in the database. (*Id.*, 15:66-16:11.) As discussed above, these parameters constitute at least part of an operating profile. Thus, the token (driver identification and data logging device) loads the operating profile (combination of restrictions from token and from communication module) for the driver to the controller module in conjunction with a remote computer.



(Murphy, Fig. 6 (annotated).)

d. Dependent 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.*

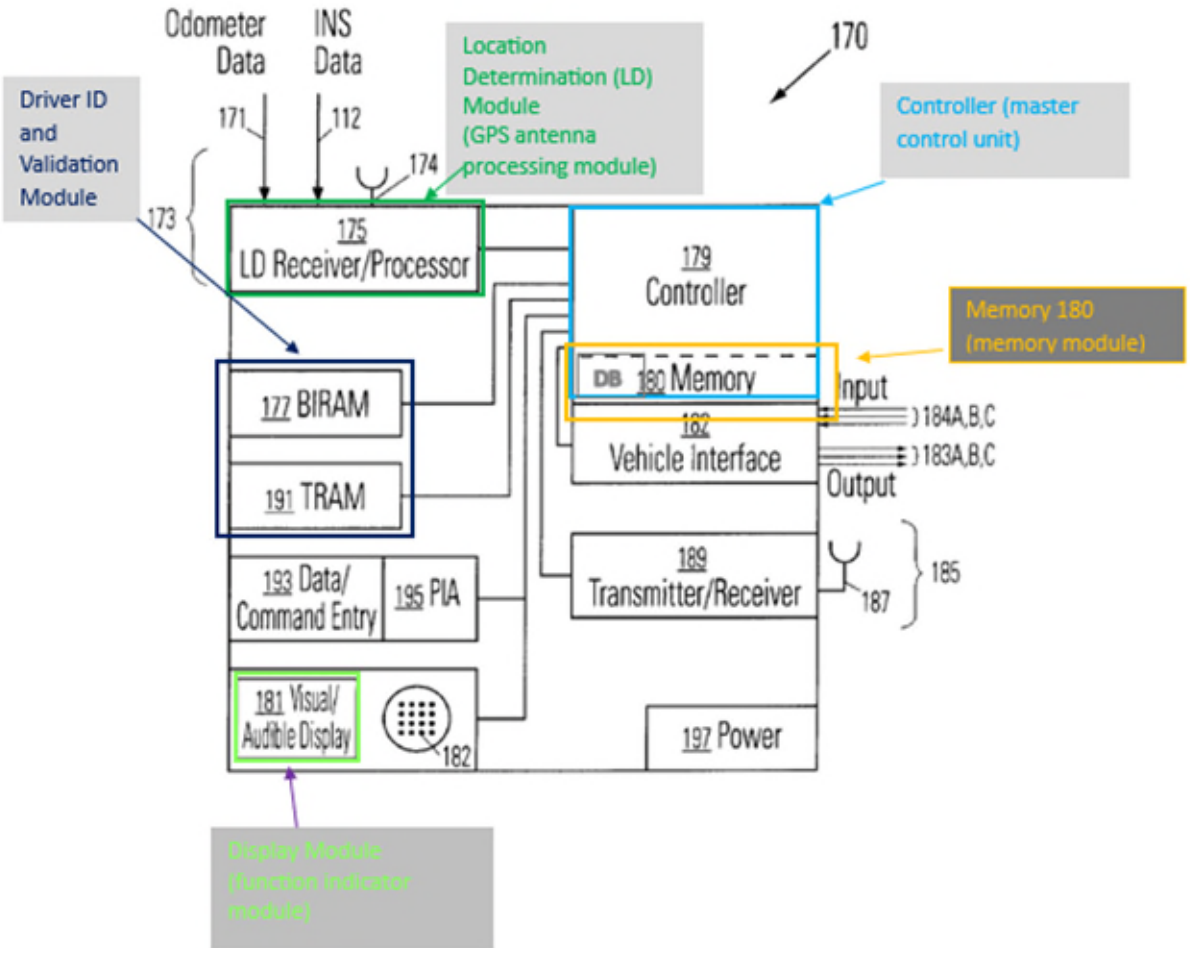
62. Murphy anticipates or renders obvious Claim 4. As I discussed for the Master Control Unit limitations, Murphy discloses a master control unit (controller module) that authenticates at least one driver through a driver identification and

data logging device (token). If a driver is authenticated and within operating parameters the system "enable[es] the ignition circuit so that the engine can be started." (Murphy, 8:21-40.) A POSITA would understand that the system must include a software module that identifies and validates drivers based on indicium presented via the token and/or BIRAM to accomplish the authentication.

63. Additionally, Murphy discloses a GPS antenna processing module. As I discussed in the GPS claim, Murphy provides an LD module that utilizes GPS to determine present location and speed. (Murphy, Abstract, 3:48-63.) The LD module includes an "LD signal antenna" and "an LD signal receiver/processor" (*Id.*) The LD module thus includes a GPS antenna processing module to process signals received through the LD signal antenna.

64. Murphy also discloses a memory module in the controller with a database that includes identities and matching indicia for drivers. (Murphy, 13:35-40, 15:15-21.) The database may store operating restrictions such as schedule applicable to driver or actual range of vehicle speed. (*Id.*, 15:66-16:9.) Alternatively, Murphy teaches that the vehicle restrictions can be stored in a schedule module connected to the controller module. (*Id.*, 15:21-31, 16:9-11.) A POSITA would recognize that the most obvious location to store the operating restrictions is within the memory module.

65. Murphy also discloses a function indicator module. A function indicator module "monitor[s] various functions in association with the vehicle." (*See* '101 Patent at 7:53-56.) Murphy provides that the controller module 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; *Id.*, 13:61-65 (operation restrictions displayed using "visual and/or audible display module").) This requires a module to "monitor various functions in association with the vehicle" in order to generate the audible/visual alert based on the various inputs. (Murphy, 14:7-17 (input terminals 184A-C for monitoring vehicle components).)



(Murphy Fig. 6 (annotated)

e. Dependent 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.*

66. Murphy anticipates or renders obvious Claim 5. As I discussed in Section V.A.1.d (claim 4), Murphy discloses a memory module that stores the driver indicia and operating restrictions (operating profile).

f. Dependent 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.*

67. Murphy anticipates or renders claim 6 obvious. As I've discussed in Section V.A.1.d (claim 4), Murphy discloses a GPS antenna processing module (LD Module), which provides information on the vehicle location. (Murphy, Abstract, 3:48-63, 13:53-65.)

g. Dependent 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.*

68. Murphy renders Claims 7 and 12 obvious. As I discussed for the Slave Control Unit limitations, Murphy discloses a Control Action module (slave control unit). Murphy also provides that power supply 197 "supplies power to operate one or more of the components of the apparatus 170." (Murphy 14:66-67.) In general, power would be supplied by a voltage-regulated power supply. A POSITA would be motivated to include a power regulator in the Control Action module to regulate

a power source for the vehicle to implement the Control Actions. (*see* Murphy, 13:66-17:4.)

69. Murphy further discloses or at least renders obvious a starter relay in the Control Action module. The starter relay 526 in the ’101, “can be enabled by a starter enable signal 518 from the master control unit 430 when the driver 410 is authenticated.” (’101, 8:7-10.) Similarly, 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.) A POSITA would recognize that this function in Murphy requires a starter relay in the Control Action module that is enabled by a signal from the controller when the driver is authenticated using either insertion or presentation of a token or smart card.

70. Murphy further discloses or at least renders obvious a definable relay module in the Control Action module. Based on Fig. 6 and 8:16-17 of the ’101 Patent, a POSITA would understand a definable relay module to be a component that enables the transfer of signals/information between different devices in the system. (’101, 8:16-17, Fig. 6.) For instance, the ’101 Patent teaches that Breathalyzer pin 542 provides a signal to a definable relay 524 in the slave control unit, which can provide status regarding alcohol consumption of the driver 510 while driving the vehicle, which would enable the slave control unit to relay the status to other components including the master control unit. (’101, 7:59-61, 8:16-

18.) Murphy teaches that the Control Action module is connected to one or more vehicle components, and that the controller communicates vehicle operations to a vehicle activity log module. (Murphy, 13:67-14:17, 15:42-46.) A POSITA would understand 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. A POSITA would recognize this to require a definable relay module as claimed by the ’101.

71. Additionally, Murphy renders obvious that the slave control unit comprises a slave microcontroller. Murphy teaches that the Control Action module connects to various components for use in controlling 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.) This can be implemented with a microcontroller and/or microprocessor. A POSITA would understand 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).

72. Finally, Murphy discloses or renders obvious that the slave control unit comprises an alarm synthesizer. As I discussed for the Slave Control Unit limitations, Murphy teaches that the controller 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 and in response generates an alarm (Control Action, e.g., a signal to reduce vehicle speed using governor). (*Id.*, 15:37-42.) Additionally, Murphy teaches providing visual or audible alerts to the driver using a "Visual/Audible Display 181" and/or a "feedback module 219" which are parts of the Control Action module. (*Id.*, 13:60-65,15:47-50.) To the extent the "Visual/Audible Display 181" and "feedback module 219" are not explicitly taught to be part of the Control Action module, it would have been the obvious place to implement them to minimize the messages needed between components.

73. Thus, Murphy discloses or renders obvious that the slave control unit comprises a power regulator module, a starter relay module, a definable relay module, a slave microcontroller, and an alarm synthesizer.

74. Moreover, a POSITA would have understood that the additional components claimed in Claims 7 and 12 are standard electrical components that have been known for decades. There is nothing inventive about including these components in a vehicle control unit. To the extent Murphy does not explicitly

disclose these elements, it would have been obvious for a POSITA to implement these components within the Control Action module of Murphy, as it would amount to nothing more than a simple substation or combination of known elements.

h. Dependent 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.*

75. Murphy anticipates or renders Claims 8 and 13 obvious. As I discussed for the Master Control Unit and Slave Control Unit limitations and dependent 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), allowable locations, and allowable hours of operation. (Murphy, 15:15-21, 15:66-16:9; *see* Sections V.A.1.ii, V.A.1.iii (Claims 1[A], 1[B]).)

i. Dependent 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.*

76. Murphy anticipates or renders Claims 9, 14, 17, and 18 obvious. As discussed for the Slave Control Unit limitations, Murphy discloses or at least renders obvious that the slave control unit (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., vehicle speed operating parameter). (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 ("The apparatus 170 also includes a telecommunication module 185 (optional), including an antenna 187 and associated receiver/transmitter 189 that exchanges information signals with an information processing facility (not shown) that is spaced apart from the apparatus 170.").) Murphy similarly discloses "an information processing facility" that "can transmit signals that modify, add or delete vehicle operation restrictions, for receipt by the apparatus 170, and that allow downloading of commands that alter restrictions . . . that determine the conditions under which a vehicle operation restriction is imposed." (*Id.*, 14:27-34.) Further, Murphy teaches preventing "anyone but an authorized system administrator from permanently or temporarily modifying" the restrictions. (*Id.*, 7:42-44; *see also* 2:6-9 ("Preferably, . . . the permitted time interval(s) and permitted vehicle corridor(s) should be flexible and should be

capable of being changed by an authorized monitoring agency or person.") A POSITA would have recognized that the selected facilities would not be open to the public and would thus limit access to authorized users because Murphy says to restrict facilities capable of changing the parameters to authorized system administrators, authorized monitoring agencies, or authorized persons. (*Id.*, 2:6-9, 7:42-44, 14:27-34.) Further, an POSITA would have wanted to restrict access to such facilities to maintain privacy for the consumers.

j. Dependent 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.*

77. Murphy anticipates or renders Claim 10 obvious. Murphy teaches that the vehicle may require "insertion or presentation of a token or smart card" specific to a driver. (Murphy, 6:55-7:14.) The token includes "digitized data stored in a flash memory, in a (re)programmable ROM or in similar information storage media." (*Id.*, 7:11-14.) A POSITA would understand "presentation" to mean something different than "insertion," specifically that the token or smart card could be presented to the TRAM without requiring insertion. Insertion is a mechanical operation, whereas presentation is through proximity or contact. The system to receive the token through proximity or contact could be implemented with radio frequency identification device ("**RFID**") technology, as was known for use for

vehicle keyless ignition systems. For instance, U.S. Patent Application Publication No. 2008/0136611 A1 ("**Benco**") (EX1010). Benco, which was filed on December 8, 2006, and published on June 12, 2008, before the earliest priority date of the '101, teaches that "many automobiles are sold with remote keyless ignition systems[,]" which use "a coded Radio Frequency Identification (RFID) chip." (Benco at [0002] – [0003].) It would have been a simple implementation of an RFID tag in the token and an RFID reader in the TRAM. This system would have operated in the same manner such that the token is presented to the TRAM, which reads the information from the token, uses at least some of the information to authenticate the token-holder, and sends some of the information to the controller. This would have been well within the skill of a POSITA.

k. Dependent 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.*

78. Murphy anticipates or renders Claim 16 obvious for the reasons I discussed above for claim 11[B]. (Section V.A.1.iii (claim 11[B]) *supra*.)

l. Dependent 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.*

79. Murphy anticipates or renders Claims 19 and 20 obvious. As I've discussed for the Slave Control Unit limitations, Murphy teaches that the Control Action module can implement at least one of 12 Control Actions, including to reduce vehicle speed using a governor. (Murphy, 5:28-60, 15:37-42.) The Control Actions can also limit functionality by disabling vehicle accessories. (*Id.*)

2. Ground 2: Murphy in view of Schanz Renders Obvious Claims 1-20

80. I have reviewed Schanz which is German Patent App. Publication No. DE10323723A1. I understand that Schanz was filed on May 24, 2003, and published on December 9, 2004. Schanz is directed to "individually setting driving dynamic characteristics of a motor vehicle." (Schanz, [0001], [0006].)

81. My review of the '101 Patent file history reveals that Schanz was not considered during prosecution of the '101 Patent.

82. 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.) Like Murphy's controller module, Schanz's "device 1" identifies and authenticates a driver and provides driver-specific parameters. (*Id.*, [0018], [0020].) 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 the "device 1" "check[] whether special vehicle parameters 6 are stored for the respective driver." (*Id.*, [0020].) These vehicle parameters include restrictions such as "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].)

a. Motivation to Combine Murphy and Schanz

83. Murphy and Schanz disclose complimentary methods for driver authentication and monitoring. (Murphy Abstract; Schanz Abstract.) A POSITA would have recognized the benefits of each method and considered combining features to result in a more customizable system.

84. Similar to Murphy's controller module, Schanz's "device 1" identifies and authenticates a driver and implements driver-specific parameters. (Schanz, [0018].) Schanz's "device 1" is comprised of a "recognition device" which" identifies a driver based on "person-specific characteristics" via a "biometric recognition unit," "and acoustic recognition unit," and/or "a reading device" "for recognizing an identification code." (*Id.*). An allocation device 25 within Schanz's "device 1" examines whether specific vehicle parameters are store for the respective driver (*Id.*, [0020].) These vehicle parameters include restrictions such

as “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” monitors for any violations of the set vehicle parameters 6 to which it responds with warnings or other interventions. (*Id.*, [0022], [0025].)

85. A POSITA would have looked to Schanz to improve Murphy given their similarities and benefits. The combined system would provide more flexibility for both the driver and the administrator or vehicle owner, allowing a driver to present a token wirelessly 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.) For example, based on driver-specific parameters (e.g., driver-specific 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 vehicle speed) to improve driver safety.

86. 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/smart card, controller module, and Control Action module) to

improve vehicle occupant safety, as both Murphy and Schanz suggest, (Murphy, 1:9-35, 11:60-67; Schanz, [0004], [0012]), while providing the flexibility for authentication and customizability that Schanz suggests, (Schanz, [0017] – [0018], [0020].)

87. 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 to be successful. For example, the combination of Schanz's identification code, driver-specific restrictions, and use of radio signals with Murphy's token/smart card would have yielded the predictable result of a system that allows the system to identify and authenticate a driver without mechanical interaction of the smart card and to notify the driver and administrator when restrictions are violated. This would have been nothing more than the use of known techniques for identification, authentication, and vehicle monitoring to improve Murphy to provide more granular vehicle safety controls. A POSITA would have had a reasonable expectation of success in combining Murphy with Schanz because both disclose vehicle units (the controller and Control Action modules of Murphy and device 1 of Schanz) that serve parallel functions and operate in similar ways to improve driver safety. A POSITA would have understood that features of Schanz's "device

1" can be easily applied to Murphy's controller and Control Action modules, and vice-versa, with a reasonable expectation of success in doing so.

b. Independent Claims 1, 11, 15

88. Murphy in view of Schanz renders Claims 1, 11, 15 and 16 obvious.

i. Preambles (1[P])

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

89. To the extent the preamble is limiting, Murphy in view of Schanz discloses a driver authentication and monitoring system and method. As I previously discussed for claims 1[P], 11[P], and 15[P], Murphy discloses a driver authentication and monitoring system and method. (Sections V.A.1.i (claim 1[P]), V.A.1.iv (claim 11[P]), V.A.1.x (claim 15[P]) *supra*.) Similarly, Schanz discloses a driver authentication and monitoring system and method using a "recognition device (3)" that identifies a driver, an "assignment device" to check "whether special vehicle parameters," such as a "maximum vehicle speed," "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].)

ii. Master Control Unit (1[A])

1[A]	*a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;*

90. Murphy in view of Schanz discloses or at least renders obvious the Master Control Unit limitations. As I discussed for claims 1[A], 11[A], 11[E], and 15[A-C], Murphy discloses a controller module (a master control unit) which uses a token (driver identification and data logging device) to identify the driver, associates an operating profile with the driver, and permits vehicle operation within the operating profile. (Murphy, 5:55-7:14; Sections V.A.1.ii (claim 1[A]), V.A.1.v (claim 11[A]), V.A.1.ix (claim 11[E]), V.A.1.xi (claim 15[A]), V.A.1.xii (claim 15[B]), V.A.1.xiii (claim 15[C]), *supra*.)

91. Shanz's "device 1" includes a "recognition device 3" (driver identification and data logging device). (Schanz, [0018].) The allocation device 25 within the "device 1" "checks whether special vehicle parameters 6 are stored for the respective driver" in which case the assignment device 25 "assign[s] individual vehicle parameters 6 to the respective driver." (*Id.*, [0020].) 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 visual and/or audible warnings or other interventions. (*Id.*, [0022], [0025].) For the reasons discussed in V.A.2.a (Motivation to Combine Murphy and Schanz), a POSITA would have been motivated to combine these features with the controller module of Murphy, as the

"device 1" of Schanz and the controller module of Murphy serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. For instance, Murphy already teaches driver-specific operating restrictions. (Murphy, 6:8-18, 6:62-7:14.) It would have been a simple implementation and well within the skill of a POSITA to implement Schanz's driver-specific vehicle parameters within Murphy's token and controller, which would have provided greater control for the administrator. This system would have operated in the same manner such that an authenticated driver could operate the vehicle so long as the restrictions of the driver-specific vehicle parameters have not been violated.

92. As discussed for claim 1[A], Murphy discloses a "unique identification code." (Section V.A.1.ii (Ground 1, claim 1[A]), *supra*.) However, to the extent that Murphy does not explicitly recite this element, Schanz discloses 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 including a reading module in Murphy's controller module to receive and recognize an identification code for the particular driver. A POSITA would have been motivated to implement Schanz's identification code into Murphy's controller module to achieve Murphy's goal of identifying and authenticating the individual driver based on the token. (Murphy, 6:55-7:14.) A POSITA would have had a reasonable expectation of success in this combination

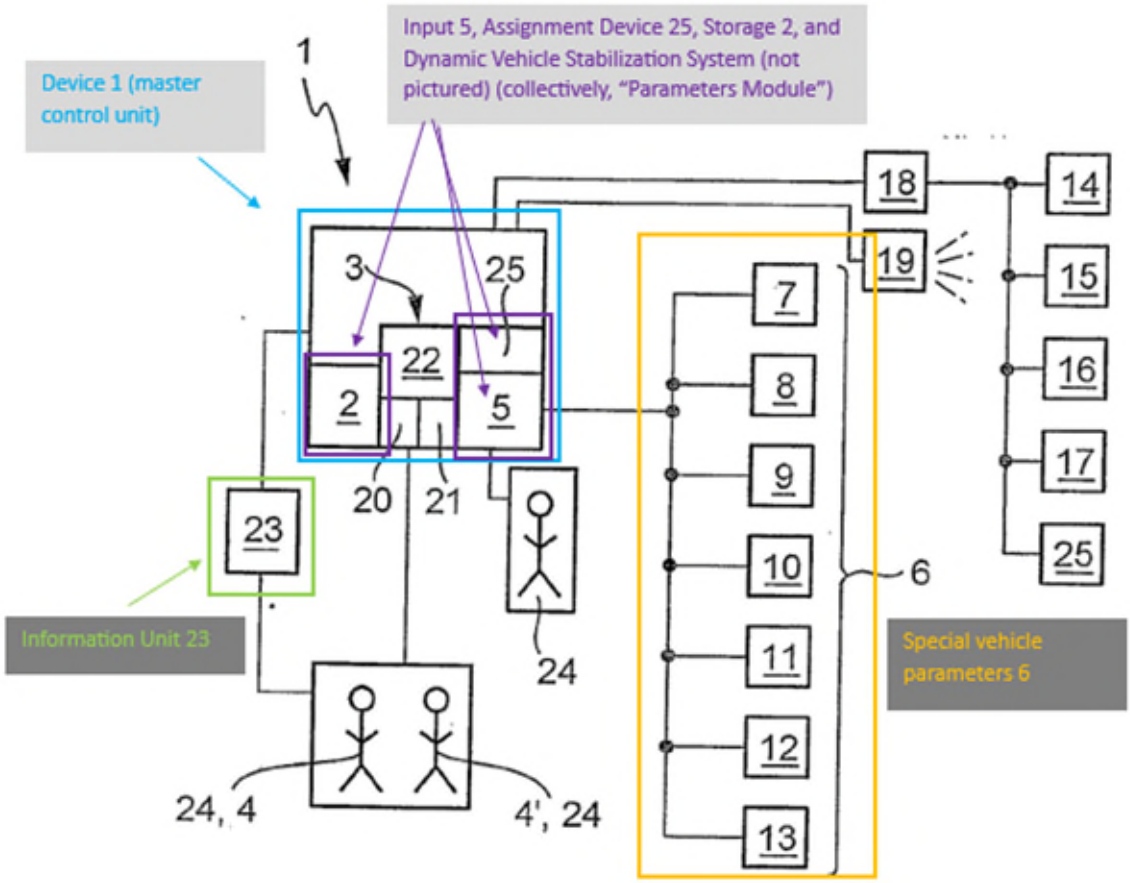
for the reasons discussed in section V.A.2.a (Motivation to Combine Murphy and Schanz). It would have been a simple implementation and well within the skill of a POSITA to implement Schanz's identification code into Murphy's controller. This system would have operated in the same manner such that the token is presented to the TRAM, which reads the information from the token and uses that information (including Schanz's identification code) to authenticate the token-holder, and sends some of the information to the controller.

iii. Slave Control Unit (1[B])

1[B]	*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;*

93. Murphy in view of Schanz discloses or at least renders obvious the Slave Control Unit limitations. As discussed in V.A.1.iii (claim 1[B]), V.A.1.viii (claim 11[D]), and V.A.1.xii (claim 15[B]), Murphy discloses that the controller module (master control unit) connects to a Control Action module (slave control unit). (Murphy, 13:66-14:4, 14:37-42). 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.



(Schanz, Fig. 1 (annotated).)

94. Like the Control Action module in Murphy, Schanz's Parameters Module is connected to device 1 and receives commands from device 1 to "adjust[]" "driving dynamic characteristics" in order to enforce driver-specific "vehicle parameters 6" such as "maximum vehicle speed," "maximum distance 12 to the vehicle driving ahead," and "intervention parameter of a dynamic vehicle stabilization system." (Schanz, [0019]-[0020].) For example, the "device 1" can

"adjust[]," or control, a "dynamic vehicle stabilization system" to cause it to "actively intervene in driving operation of a beginner 'earlier' than in the case of an advanced driver, in order 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].) As shown in Fig. 1, Schanz depicts "information unit 23" as external to the "device 1," but connected to the "device 1." (Schanz, Fig. 1.) This indicates that the "device 1" communicates with the "information unit 23," e.g., to cause it to generate an alarm when the "device 1" detects violation of a "vehicle parameter."

95. The combined Murphy-Schanz system would have a Control Action module for governing vehicle operations remotely (from both Murphy's Control Action module and Schanz's Parameters Module) and generating an audible alarm (from Schanz's information unit). For the reasons discussed in V.A.2.a (Motivation to Combine Murphy and Schanz), a POSITA would have been motivated to combine these features from Schanz with the Control Action module of Murphy, as the Parameters Module of Schanz and Control Action module of Murphy serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety, while providing greater customizability of restrictions for the administrator. This combined system would have operated in the same manner

such that the modified Control Action module sends an alarm signal in response to commands from the master control unit when an operating restriction is violated to control the vehicle and present an alarm.

96. Furthermore, the ’101 Patent specification illustrates the “slave control unit” as a collection of components, and does not require connections or communication between these components. (’101, Fig. 6, 7:57-8:2; *see also* U.S. Patent Reexamination Proceeding No. 90/015,287 (EX1012), 185-186 (commenting on identical figures and text in the specification of related U.S. Patent No. 10,259,470).) 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 “slave control unit,” even if the two systems do not otherwise connect with or communicate with one another.

iv. Preamble (11[P])

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

97. To the extent the preamble is limiting, Murphy in view of Schanz discloses a driver authentication and monitoring system and method. As I previously discussed for claims 1[P], 11[P], and 15[P], Murphy discloses a driver authentication and monitoring system and method. (Sections V.A.1.i (claim 1[P]), V.A.1.iv (claim 11[P]), V.A.1.x (claim 15[P]) *supra*.) Similarly, Schanz discloses a driver authentication and monitoring system and method using a “recognition

device (3)" that identifies a driver, an "assignment device" to check "whether special vehicle parameters," such as a "maximum vehicle speed," "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].)

v. Master Control Unit (11[A])

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;*

98. Murphy in view of Schanz renders obvious Claim 11[A]. In addition to the elements discussed in V.A.2.ii (claim 1[A]), Claim 11[A] also requires "associating an operating profile with said at least one driver." Because the controller, in either Murphy or the Murphy-Schanz system, loads an operating profile containing driver-specific time, location, and/or speed restrictions when a driver is identified, the operating profile is associated with the driver, allowing the driver to operate the vehicle within the parameters of the associated restrictions. (Murphy, 5:18-26, 6:8-18, 6:59-7:14, 14:46-54.)

vi. GPS (11[B])

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

99. Murphy in view of Schanz renders obvious Claim 11[B]. As discussed in V.A.1.iii,vi (Ground 1, claim 1[B], claim 11[B]), Murphy discloses an LD module that can be implemented using GPS to determine present location and present speed. (Murphy, Abstract, 3:48-56.)

vii. Data Logging Device (11[C])

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*

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

viii. Slave Control Unit (11[D])

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;*

101. Murphy in view of Schanz renders obvious Claim 11[D]. As I previously discussed for claim 1[B], Murphy in view of Schanz discloses a slave control unit. (*See* Section V.A.2.iii (claim 1[B]) *supra*).

ix. Unique Identification Code (11[E])

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.*

102. Murphy in view of Schanz renders obvious Claim 11[E]. As I previously discussed for claim 1[B], Murphy in view of Schanz discloses the master control unit receiving a unique identification code. (*See* Section V.A.2.ii (claim 1[B]) *supra*). In addition to the elements of claim 1[A], Claim 11[E] also requires permitting the driver to operate within an operating profile if "said at least one driver has not violated said operating profile." Murphy teaches a control action to disable the vehicle when the driver violates one of the operating restrictions that constitute an operating profile. (Murphy, 5:29-60.)

x. Preamble (15[P])

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

103. To the extent the preamble is limiting, Murphy in view of Schanz discloses a driver authentication and monitoring system and method. As I previously discussed for claims 1[P], 11[P], and 15[P], Murphy discloses a driver authentication and monitoring system and method. (Sections V.A.1.i (claim 1[P]), V.A.1.iv (claim 11[P]), V.A.1.x (claim 15[P]) *supra*.) Similarly, Schanz discloses a driver authentication and monitoring system and method using a "recognition

device (3)" that identifies a driver, an "assignment device" to check "whether special vehicle parameters," such as a "maximum vehicle speed," "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].)

xi. Driver Authentication and Monitoring System 15[A]

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

104. Murphy in view of Schanz renders obvious Claim 15[A]. As I discussed in V.A.1.ii (Ground 1, claim 1[A]), Murphy discloses a controller 179 connected to TRAM 191 and BIRAM 203, which is "providing a motor vehicle with a driver authentication and monitoring system." (*See* Section V.A.1.ii (claim 1[A]) *supra*.) Further, the Murphy-Schanz system described in V.A.2.ii (claim 1[A]) is a driver authentication and monitoring system in a motor vehicle.

xii. Operating Profile (15[B])

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

105. Murphy in view of Schanz renders obvious Claim 15[B]. As I discussed above for claim 1[A], Murphy discloses information pre-programed information including operating restrictions into the token that are loaded into the controller, which is "programming said driver authentication and monitoring

system with an operating profile associated with a high risk driver." (*See* Section V.A.2.ii (claim 1[A]) *supra*; *see also* Section V.A.2.v (claim 11[A]) *supra*.) The Murphy-Schanz system described above in V.A.2.ii also implement Schanz's driver-specific vehicle parameters Murphy's token, which would be loaded into the controller, which is further "programming said driver authentication and monitoring system with an operating profile associated with a high risk driver." (*See* Section V.A.2.ii (claim 1[A]) *supra*; *see also* Section V.A.2.v (claim 11[A]) *supra*.)

xiii. Monitoring Operation (15[C])

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;*

106. Murphy in view of Schanz renders obvious Claim 15[C]. As I discussed above for claim 1[A], Murphy discloses presenting a token to the TRAM to authenticate a driver and enable operation within the operating restrictions from the token and/or communications module, which is "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." (*See* Section V.A.2.ii (claim 1[A]) *supra*; *see also* Section V.A.2.v (claim 11[A]) *supra*.)

xiv. Alarm Signal (15[D])

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

107. Murphy in view of Schanz renders obvious Claim 15[D]. As I discussed above for claim 1[B], Murphy teaches that when an operating restriction is violated, the vehicle interface module 182 and control action interface module 215 receive a control action from the controller and in response generate a signal to "the vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory or other appropriate system on the vehicle." (*See* Section V.A.2.iii (claim 1[B]) *supra;* Murphy, 14:37-42.) The control action can include a signal to reduce vehicle speed, which is consistent with an alarm signal according to the '101 patent. (*Id.*; '101 Patent at 6:65-7:5 ("alarm signal" includes signal to slow down vehicle).) In addition the Murphy-Schanz system includes an "information unit 23" which "emits suitable optical and/or acoustic warning signals when the set vehicle parameters 6 are exceeded." (*See* Section V.A.2.iii (claim 1[B]) *supra*; Schanz, [0025].) Therefore, the Murphy-Schanz system renders obvious "generating an alarm signal if said high profile driver violates said operating profile while operating said motor vehicle."

xv. Governing Mechanical Operations (15[E])

15[E]	*governing mechanical operations of said vehicle remotely if said high*

	profile driver violates said operating profile thereby maintaining occupant safety.

108. Murphy in view of Schanz renders obvious Claim 15[E]. As I discussed for claim 1[B], Murphy teaches a control signal to slow down or disable the vehicle when an operating restriction, which can be loaded or changed remotely through the communications module, is violated. (*See* Section V.A.2.iii (claim 1[B]) *supra*; Murphy, 14:37-42.) Additionally, the combination of functionality of Schanz's Parameters Module into the Control Action Module would result in the Control Action "actively interven[ing] in driving operation of a beginner 'earlier' than in the case of an advanced driver, in order to alert the beginner to critical driving situations." (*See* Section V.A.2.iii (claim 1[B]) *supra*; Schanz, [0022].) Therefore, the Murphy-Schanz system renders obvious "governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety."

c. Dependent 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.*

109. Murphy in view of Schanz renders Claim 5 obvious. As discussed in V.A.1.d, Murphy discloses a memory module that stores the driver indicia and operating restrictions (operating profile).

110. Additionally, a POSITA would have been motivated to modify the system taught in Murphy based on Schanz 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" (i.e., an operating profile). (Schanz, [0017], [0020].) For the reasons I discussed in V.A.2.a (Motivation to Combine Murphy and Schanz) and V.A.2.ii (Claim 1[A]), a POSITA would have been motivated to combine the storage of parameters (operating profile) from Schanz with the controller module of Murphy, as the "device 1" of Schanz and controller module of Murphy serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. For instance, Murphy already teaches driver-specific operating restrictions. (Murphy, 6:8-18, 6:62-7:14.) It would have been a simple implementation and well within the skill of a POSITA to implement Schanz's driver-specific vehicle parameters within Murphy's token and controller, which would have provided greater control for the administrator. This system would have operated in the same manner such that an authenticated driver could operate the vehicle so long as the restrictions of the driver-specific vehicle parameters have not been violated.

d. Dependent 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.*

111. Murphy in view of Schanz renders Claims 8 and 13 obvious. As discussed in V.A.1.h (Ground 1, Claims 8 and 13), 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), allowable locations, and allowable hours of operation. (Murphy, 15:15-21, 15:66-16:9.)

112. Similarly, Schanz discloses that the definable "vehicle parameters 6" (resulting in an operating profile when defined for a driver) includes "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 the 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].) For the reasons discussed in V.A.2.a (Motivation to Combine Murphy and Schanz) and V.A.2.ii (Claim 1[A]), a POSITA would have been motivated to combine these features from Schanz with the controller module of Murphy, as the "device 1" of Schanz and controller

module of Murphy serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. Further, the modification would have been nothing more than the simple substitution or combination of customizable parameters into the parameters in Murphy's controller.

e. Dependent 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.*

113. Murphy in view of Schanz renders Claims 9, 14, 17, and 18 obvious. As I've discussed in V.A.1.i (Ground 1, Claims 9, 14, 17, 18), Murphy discloses or renders obvious that the slave control unit (Control Action module) generates an alarm for remotely alerting an authorized user when the driver violates the operating profile. (Murphy at 5:18-60, 15:37-42.)

114. In addition, Schanz discloses that "information unit 23" (part of "slave control unit") "informs ... 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 the "information unit 23" is provided "remotely." However, Murphy teaches a Control Action that includes "transmit[ting] an alarm

(optionally silent) to a selected facility that is spaced apart from the vehicle. (Murphy, 5:43-45.) As discussed in V.A.2.ii-iii (Claims 1[A] and 1[B]), the combination of features from Murphy with features from Schanz, would enable a POSITA to employ Murphy's Control Action to transmit an alarm to authorized persons at a selected facility. For the reasons discussed in V.A.2.a (Motivation to Combine Murphy and Schanz) and V.A.2.iii (Claim 1[B]), a POSITA would have been motivated to combine these features from Schanz with the Control Action module of Murphy, as the "device 1" of Schanz and Control Action module of Murphy serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results

f. Dependent 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.*

115. Murphy in view of Schanz renders claim 10 obvious. As I've discussed in Section V.A.1.j, Murphy discloses or renders obvious that the driver identification and data logging device comprises a radio frequency identification device. (*See* Section V.A.1.j (Ground 1, claim 10); EX1010.) A POSITA would have further been motivated to modify Murphy's token to use RFID technology based on Schanz's disclosure of a device capable of transmitting and receiving

radio signals. Schanz discloses a transmitting and/or receiving 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 and would have further been motivated to implement Murphy's token using RFID technology as discussed above. (*See* Section V.A.1.j (Ground 1, claim 10); EX1010.) This system would have operated in the same manner such that the token is presented to the TRAM, which reads the information from the token, uses at least some of the information to authenticate the token-holder, and sends some of the information to the controller. This would have been well within the skill of a POSITA.

g. Dependent 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.*

116. Murphy in view of Schanz discloses Claim 16. As discussed in V.A.1.iii,vi,k (claim 1[B], claim 11[B], claim 16), Murphy discloses an LD module that can be implemented using GPS to determine present location and present speed. (Murphy, Abstract, 3:48-56.)

h. Dependent 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.*

117. Murphy in view of Schanz renders Claims 19 and 20 obvious. As I discussed for the Slave Control Unit limitations, Murphy teaches that the Control Action module (slave control unit) can implement Control Actions, including disabling the vehicle or reducing the vehicle speed using a governor. (Murphy, 5:18-60, 15:37-42.) The Control Actions can also limit functionality by disabling vehicle accessories. (*Id.*) Furthermore, 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 also know that for an automotive stabilization system Electronic Stability Program (ESP), the ESP malfunction indicator is required to flash in order to indicate/alert Electronic Stability Control (ESC) operation to the driver. This was standard on vehicles long before the patent priority date and can also be read in standards/regulations (e.g., FMVSS 126, EX1011.). Common examples of ESC interventions in vehicles include collision avoidance systems and alarms, lane change alarms, etc. 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 for the reasons discussed above in V.A.2.a (Motivation to Combine Murphy and Schanz) and V.A.2.iii (Claim 1[B]).

i. Dependent Claims 2-4, 6-7, 12

118. For the reasons discussed in sections V.A.2.a (Motivation to Combine Murphy and Schanz) and V.A.1.b-d, f-g, Murphy in view of Schanz renders obvious Claims 2-4, 6-7, and 12.

3. Ground 3: Murphy in view of Schanz in view of Benco Renders Obvious Claim 10

119. I have reviewed Benco which is U.S. Patent App. Publication No. 2008/0136611 A1. I understand that Benco was filed on December 8, 2006, and published on June 12, 2008. Benco is directed to "assist in providing security for vehicles with keyless ignition systems." (Schanz, [0001], [0006].)

120. My review of the '101 Patent file history reveals that Benco was not considered during prosecution of the '101 Patent.

121. Benco discloses "an apparatus and method to assist individuals in providing security for a vehicle activated by a keyless ignition system by a) receiving, via wireless communications, a signal to start an ignition of the vehicle, b) transmitting, upon receipt of the signal, a message to a server to provide a security key to the vehicle and to one or more mobile phones registered to a driver of the vehicle, and c) starting the ignition when, upon receipt of the security key by

the driver and the vehicle, the security key received by the driver and inputted to the vehicle is identical to the security key received by the vehicle." (Benco, [0004].)

122. Benco teaches in the background that "many automobiles are sold with remote keyless ignition systems" that "allow individuals to start an ignition of an automobile from a short distance away from the automobile, eliminating the need to physically manipulate a key into an ignition of the automobile." (Benco, [0002].) Benco further teaches that "[a] remote keyless ignition system uses a coded Radio Frequency Identification (RFID) chip." (*Id.*, [0003].) "The remote keyless ignition system operates based on a radio frequency signal being emitted from the automobile and received by a fob." (*Id.*) The fob would then send a response to the automobile, and the automobile would be started. (*Id.*)

a. Dependent 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.*

123. To the extent Murphy alone (as described in section V.A.1.j (Ground 1, claim 10)) or Murphy in view of Schanz (as describe in section V.A.2.f Ground 2, claim 10) fails to render obvious claim 10, it would have further been obvious to

implement Murphy's token using a radio frequency identification device in view of Benco.

124. Benco teaches in the background that "many automobiles are sold with remote keyless ignition systems" that "allow individuals to start an ignition of an automobile from a short distance away from the automobile, eliminating the need to physically manipulate a key into an ignition of the automobile." (Benco, [0002].) Benco further teaches that "[a] remote keyless ignition system uses a coded Radio Frequency Identification (RFID) chip." (*Id.*, [0003].) "The remote keyless ignition system operates based on a radio frequency signal being emitted from the automobile and received by a fob." (*Id.*) The fob would then send a response to the automobile, and the automobile would be started. (*Id.*)

125. A POSITA would have been motivated to combine Murphy (or Murphy in view of Schanz) with Benco to provide convenience to the drivers with a remote keyless ignition system. As Benco explains, many automobiles were sold with remote keyless ignition systems" that "use[d] a coded Radio Frequency Identification (RFID) chip." (Benco, [0002].) As taught by Murphy, the token could be merely presented rather than inserted to the TRAM, and the token would use RFID to communicate with the TRAM. (Murphy, 6:55-7:14.) It would have been well within the skill of a POSITA to implement Murphy's token using RFID

as taught by Benco, as RFID was commonly used for remote keyless ignition systems within the automotive industry.

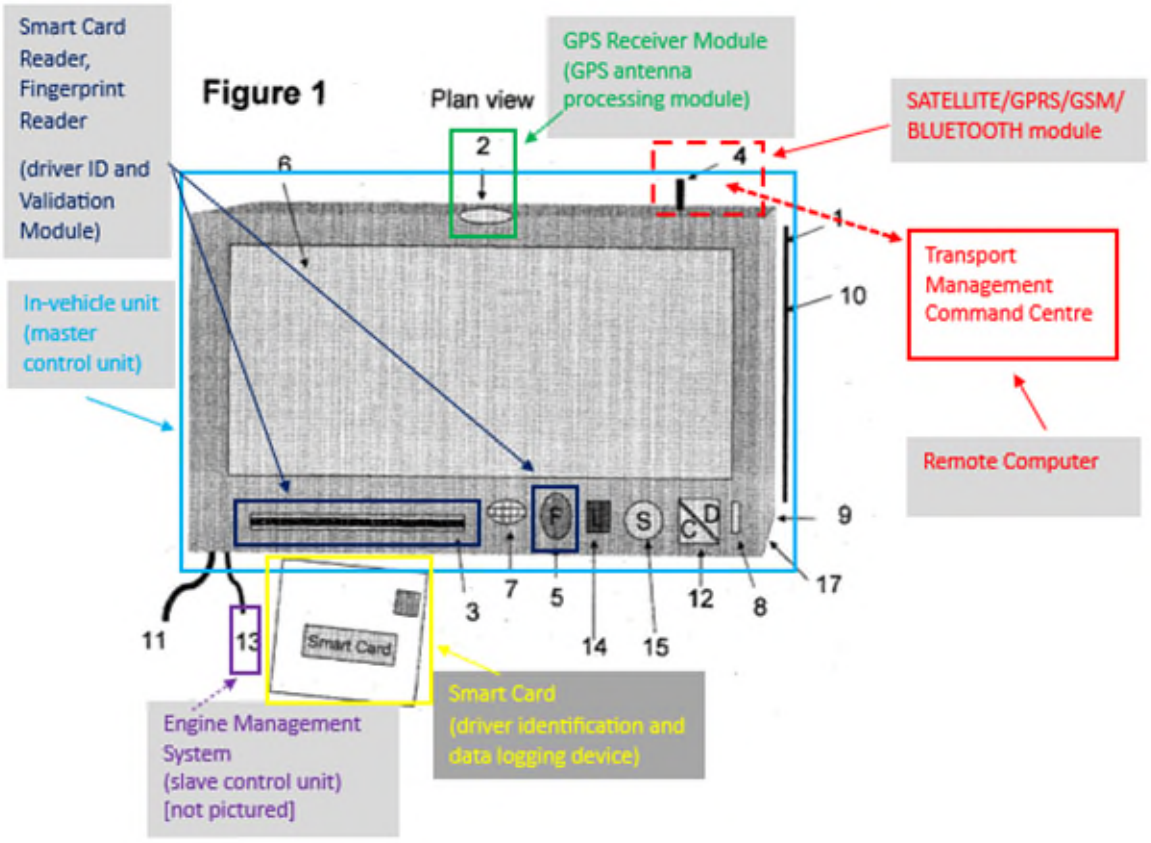
B. Grounds Based on Petrik

126. I have reviewed Petrik which is US 2007/0168125 A1. Petrik is directed to a driver authentication and monitoring system and method that confirms a driver's identity via a fingerprint reader and smart card reader, during authentication, an operating profile for the driver loads into the vehicle for the driver. The system monitors the operation of the vehicle and takes certain actions (sending an alarm, or restricting vehicle usage and operation) if the driver violates the operating profile. I understand that Petrik was filed on August 9, 2005, and published on July 19, 2007.

127. My review of the '101 Patent file history reveals that Petrik was not considered during prosecution of the '101 Patent.

128. Petrik discloses an in-vehicle monitoring unit that incorporates 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].) And "[t]he 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 on

the smart card and in 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, Fig. 1 (annotated).)

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

a. Independent Claims 1, 11, 15, Dependent Claim 16

129. Petrik anticipates or renders independent Claims 1, 11, and 15 obvious.

i. Preambles (1[P])

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

130. To the extent the preamble is limiting, Petrik discloses a driver authentication and monitoring system and method. Petrik discloses a system that 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." (Petrik, [0025].) If the presented driver card and fingerprint do not match, the engine will not start. (*Id.*) The system "provides real time GPS based vehicle monitoring" with an "in-vehicle monitoring unit." (*Id.*, Abstract, [0001].)

ii. Master Control Unit (1[A])

1[A]	*a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;*

131. Petrik discloses or at least renders obvious the Master Control Unit limitations. With reference to FIG. 1 (annotated below), which depicts one embodiment ("form one"), Petrik discloses an in-vehicle monitoring unit (a master

control unit) 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.) Petrik explains that "[d]rivers are issued with their logbook smart cards with their fingerprint template recorded in the card." (*Id.*, [0022].) The in-vehicle monitoring 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.

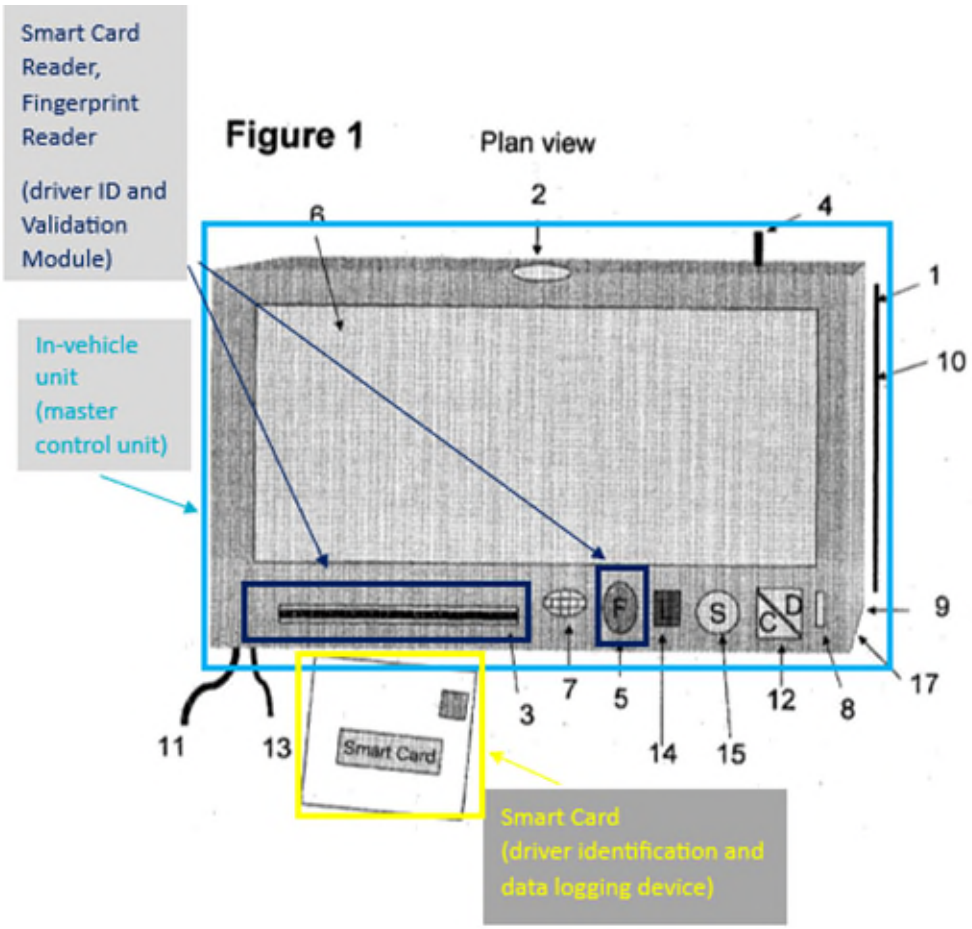
132. In response to a smart card and fingerprint combination, the in-vehicle unit logs in the authenticated user "as the current driver and enables engine ignition[,]" but the "engine will not start if . . . an invalid driver card and fingerprint combination is presented." (*Id.*) Thus, Petrik discloses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

133. Petrik does not explicitly recite a "unique identification code." However, a POSITA would have understood that confirmation of a driver's identity using both the smart card and fingerprint would necessarily require the in-vehicle unit (master control unit) to receive information comprising or consist with a unique identification code from the combination of the smart card reader/writer and fingerprint reader in order to authenticate the driver. (Petrik, [0025].) As discussed by Petrik, a POSITA would understand that "smart cards supported by

biometric fingerprints" are "secure forms of information storage." (Petrik, [0013].) In order for the "[s]mart cards supported by indisputable biometric fingerprints" to identify and authenticate a particular driver, the combination of a smart card with a biometric fingerprint must necessarily contain some indicia unique to the driver, which would be at least consistent with a unique identification code.

134. During authentication, intended vehicle route plan, speed limits, and rest parameters are loaded into the in-vehicle unit. (Petrik, [0025].) Once authenticated, a driver can operate the vehicle within certain restrictions, including at least the intended vehicle rout plan, speed limits, and rest parameters. (*Id.*) A POSITA would understand that the intended vehicle route plan, speed limits, and rest parameters are consistent with an operating profile, as they provide a set of parameters, or a profile, within which the driver can operate the vehicle. Parameters of the operating profile may also include distance and duration of driving, without stops. 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." (Petrik, [0025].) 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 within which the authenticated driver is permitted to drive the vehicle. The system monitors vehicle operation to determine if the driver is violating the operating profile.



(Petrik, Fig. 1 (annotated).)

iii. Slave Control Unit (1[B])

1[B]	*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;*

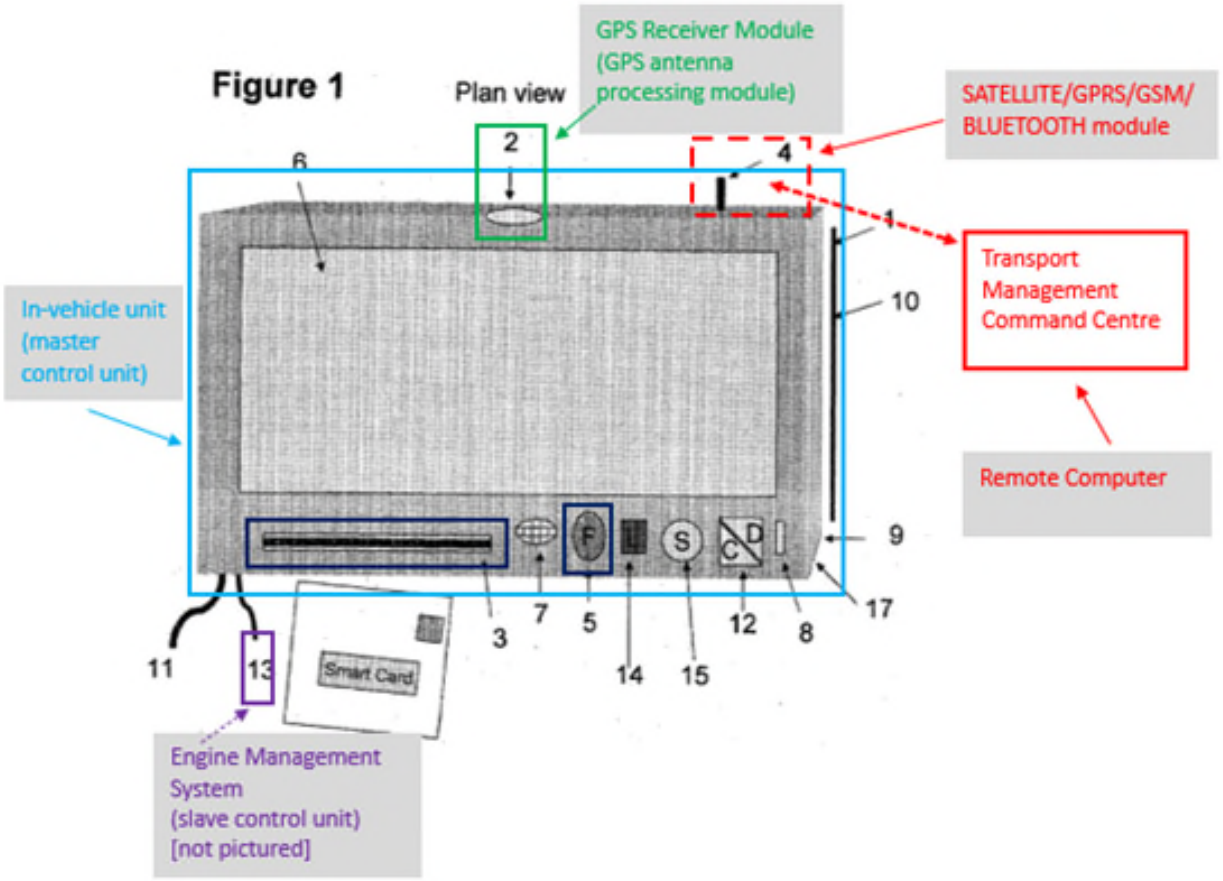
135. Petrik discloses or at least renders obvious the Slave Control Unit limitations. As shown by Fig. 1 (annotated below), Petrik discloses that the in-vehicle monitoring unit (master control unit) connects to an engine management system (slave control unit; not shown in Fig. 1) using "the engine management system connector." (Petrik, [0069], Fig. 1.) Petrik further explains that "[a]t the time of installation on the vehicle the unit is connected to the engine management system which is programmed to take instructions from it." (*Id.*, [0020].) Petrik also teaches that the in-vehicle unit (master control unit) can interact with the engine management system (slave control unit). (*Id.*, [0025], [0047].) Thus, Petrik discloses a slave control unit in communications with said master control unit.

136. Petrik teaches that the GPS in the in-vehicle unit can "interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025], [0047].) The '101 Patent specification explicitly teaches that slowing down the vehicle can constitute the "alarm signal." ('101 at 6:65-7:5.) Petrik also teaches

that the engine management system can control the vehicle in response to commands from the remote national 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 that the slave control unit (engine management system) is configured to receive commands from said master control unit (in-vehicle monitoring unit) and to generate at least one kind of alarm signal (e.g., "disable" command to lock up the engine management unit, command to slow down) if said at least one driver violates said operating profile unique to said at least one driver (encompassing at least operating parameters including the intended vehicle rout plan and speed limits) thereby providing feedback about said vehicle usage and governing mechanical operations (e.g., slow down vehicle or disable engine management system) of said vehicle remotely (via SATELITE/GPRS/GSM) thereby maintaining occupant safety.

137. Alternatively, Petrik renders obvious that the slave control unit (engine management system) is configured to generate at least one alarm signal by beeping if said at least one driver violates said operating profile unique to said at least one driver (e.g., exceeding a speed limit on the intended route plan). Petrik discloses that "[a]s the vehicle approaches each new speed zone, the unit using its' intelligent speed adaptation and geographically based speed zone location tables,

beeps to warn the driver of the zone change and if allowed, interacts with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025].) A POSITA would recognize that there are a limited number of ways to implement the beep signal and would 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 zone's speed limit. 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 the vehicle's speed and would be in the best position to send a signal to the beeper when the speed is different from the new zone.



(Petrik, Fig. 1 (annotated).)

iv. Preamble (11[P])

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

138. To the extent the preamble is limiting, Petrik discloses a driver authentication and monitoring system and method. (*See* Section V.B.1.i (Claim 1[P]).)

v. Master Control Unit (11[A])

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*

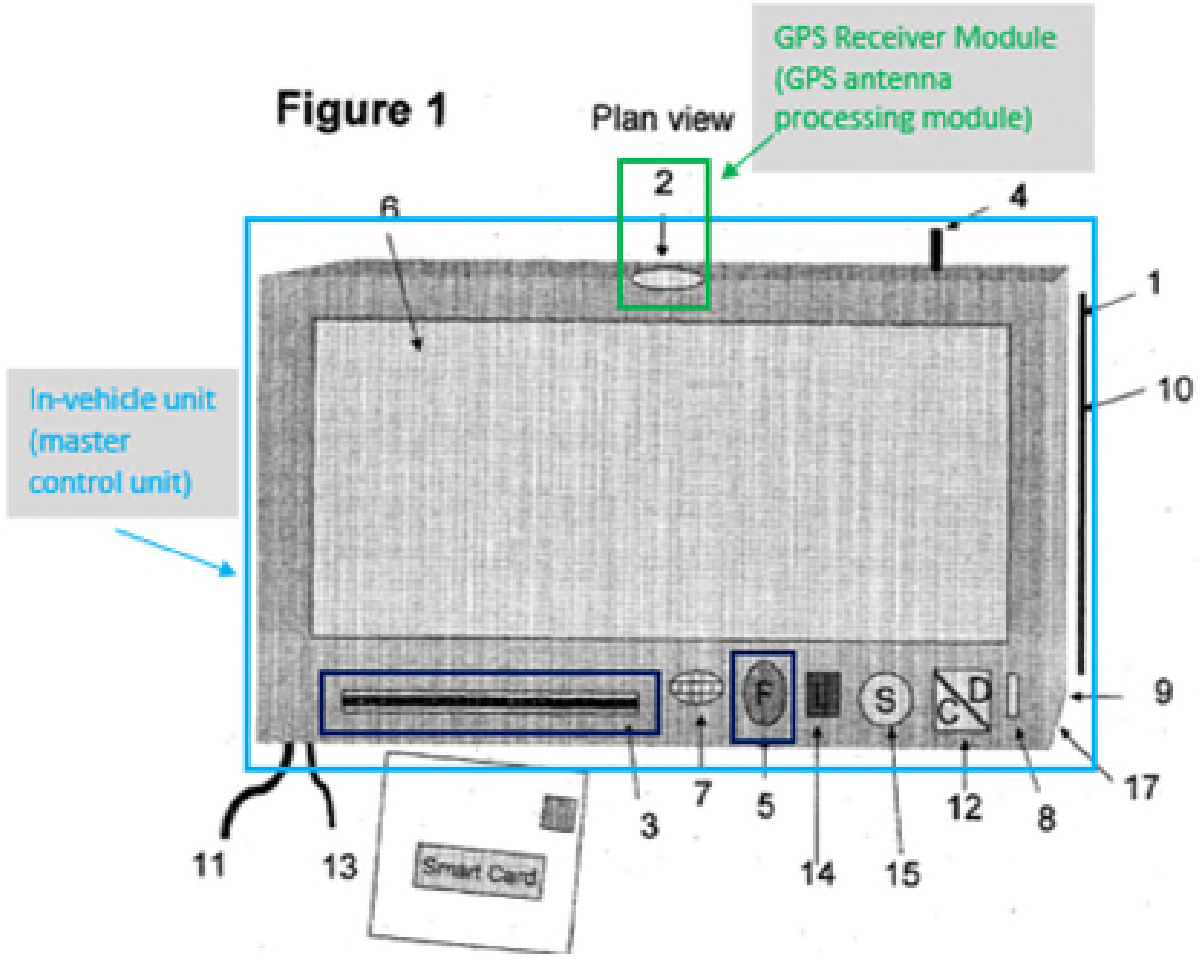
	with said at least one driver;

139. Petrik discloses or renders obvious Claim 11[A]. In addition to the elements discussed in V.B.1.ii (claim 1[A]), Claim 11[A] also requires "associating an operating profile with said at least one driver." Because Petrik's in-vehicle unit loads an operating profile containing driver-specific intended vehicle route plan, speed limits associated with the route plan, and rest parameters when a driver is identified, the operating profile is associated with the driver, allowing the driver to operate the vehicle within the parameters of the associated restrictions. (Petrik, [0025]-[0026].)

vi. GPS (11[B])

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

140. Petrik discloses Claims 11[B]. As discussed for the Slave Control Unit limitations (and shown as GPS Receiver Module 2 in Fig. 1 annotated below), Petrik discloses a GPS module. The GPS module "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].)



(Petrik, Fig. 1 (annotated).)

vii. Data Logging Device (11[C])

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*

141. Petrik discloses Claim 11[C]. Petrik teaches "a method and system of automatically and irrefutably logging via GPS, . . . , vehicle location, vehicle speeds, speeding offences, distance covered etc. and recording these on a secure

smart card as well as in the vehicle units' memory." (Petrik, [0009].) Petrik further discloses that 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 or monitoring unit's memory are a data logging device.

viii. Slave Control Unit (11[D])

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;*

142. As I previously discussed for claim 1[B], Petrik in view of Schanz renders obvious a slave control unit. (*See* Section V.B.2.iii (claim 1[B]) *supra*).

ix. Unique Identification Code (11[E])

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.*

143. Petrik discloses or renders obvious Claim 11[E]. As I previously discussed for claim 1[A], Petrik discloses or renders obvious a master control unit that receives a unique identification code. (*See* Section V.B.1.ii (claim 1[A]) *supra*.) In addition to the elements of claim 1[A], Claim 11[E] also requires

permitting the driver to operate within an operating profile if "said at least one driver has not violated said operating profile."

144. As discussed above in V.B.1.iii (claim 1[B]), Petrik teaches that the GPS in the in-vehicle unit can "interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025], [0047].) The '101 Patent specification explicitly teaches that slowing down the vehicle can constitute the "alarm signal." ('101 at 6:65-7:5.) Petrik also teaches that the engine management system can control the vehicle in response to commands from the remote national 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].)

x. Preamble (15[P])

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

145. To the extent the preamble is limiting, Petrik discloses a driver authentication and monitoring system and method. (*See* Section V.B.1.i (Claim 1[P]).)

xi. Driver Authentication and Monitoring System 15[A]

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

146. Petrik discloses or renders obvious Claim 15[A]. As I discussed above for claim 1[A], Petrik discloses an in-vehicle unit with a smart card and fingerprint reader for identifying and authenticating a driver and monitoring compliance with certain parameters, which is "providing a motor vehicle with a driver authentication and monitoring system." (*See* Section V.B.1.ii (claim 1[A]) *supra*.)

xii. Operating Profile (15[B])

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

147. Petrik discloses or renders obvious Claim 15[B]. As I discussed above for claim 1[A], Petrik discloses loading a driver-specific intended vehicle route plan, speed limits, and rest parameters into the in-vehicle unit, which is "programming said driver authentication and monitoring system with an operating profile associated with a high risk driver." (*See* Section V.B.1.ii (claim 1[A]) *supra*; *see also* Section V.A.1.v (claim 11[A]) *supra*.)

xiii. Monitoring Operation (15[C])

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;*

148. Petrik discloses or renders obvious Claim 15[C]. As I discussed above for claim 1[A], Petrik discloses inserting a smart card to the smart card

reader/writer to authenticate a driver and enable operation so long as it is consistent with the driver-specific intended vehicle route plan, speed limits, and rest parameters, which is "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." (*See* Section V.B.1.ii (claim 1[A]) *supra*; *see also* Section V.B.1.v (claim 11[A]) *supra*.)

xiv. Alarm Signal (15[D])

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

149. Petrik discloses or renders obvious Claim 15[D]. As I discussed above for claim 1[B], Petrik teaches that the GPS in the in-vehicle unit can "interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025], [0047].) The '101 Patent specification explicitly teaches that slowing down the vehicle can constitute the "alarm signal." ('101 at 6:65-7:5.) Petrik also teaches that the engine management system can control the vehicle in response to commands from the remote national 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].)

(*See* Section V.B.1.iii (claim 1[B]) *supra*; Petrik, [0025], [0030], [0047].) The engine management system must send a signal to the engine to reduce vehicle speed, which is consistent with an alarm signal according to the '101 patent. (*Id.*; '101 Patent at 6:65-7:5 ("alarm signal" includes signal to slow down vehicle).) Therefore, Petrik discloses "generating an alarm signal if said high profile driver violates said operating profile while operating said motor vehicle."

xv. Governing Mechanical Operations (15[E])

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

150. Petrik discloses or renders obvious Claim 15[E]. As I discussed for claim 1[B], Petrik teaches a signal to reduce vehicle speed when a driver violates an operating profile (including a driver-specific intended vehicle route plan, speed limits, and rest parameters), which can be loaded or changed remotely through the SATELITE/GPRS/GSM, is violated. (*See* Section V.B.1.iii (claim 1[B]) *supra*; Petrik, [0025], [0030], [0047].) Therefore, Petrik discloses "governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.

b. Dependent 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.*

151. Petrik anticipates or renders Claim 2 obvious. Petrik explains that the driver authentication and monitoring system includes a "Transport Management Command Centre with an up to date database of road conditions" which is in communication with the in-vehicle unit. (Petrik, [0010].) "Prior to each departure, dispatch automatically 'files' the intended vehicle rout 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 rout plan" includes operating parameters (e.g., speed limits) associated with the vehicle. Thus, Petrik discloses a database comprising a program module (software that allows filing of an intended vehicle rout plan and cargo details) including at least one operating parameter associated with the vehicle (driver rout plan), said program module being 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 the intended vehicle rout plan).

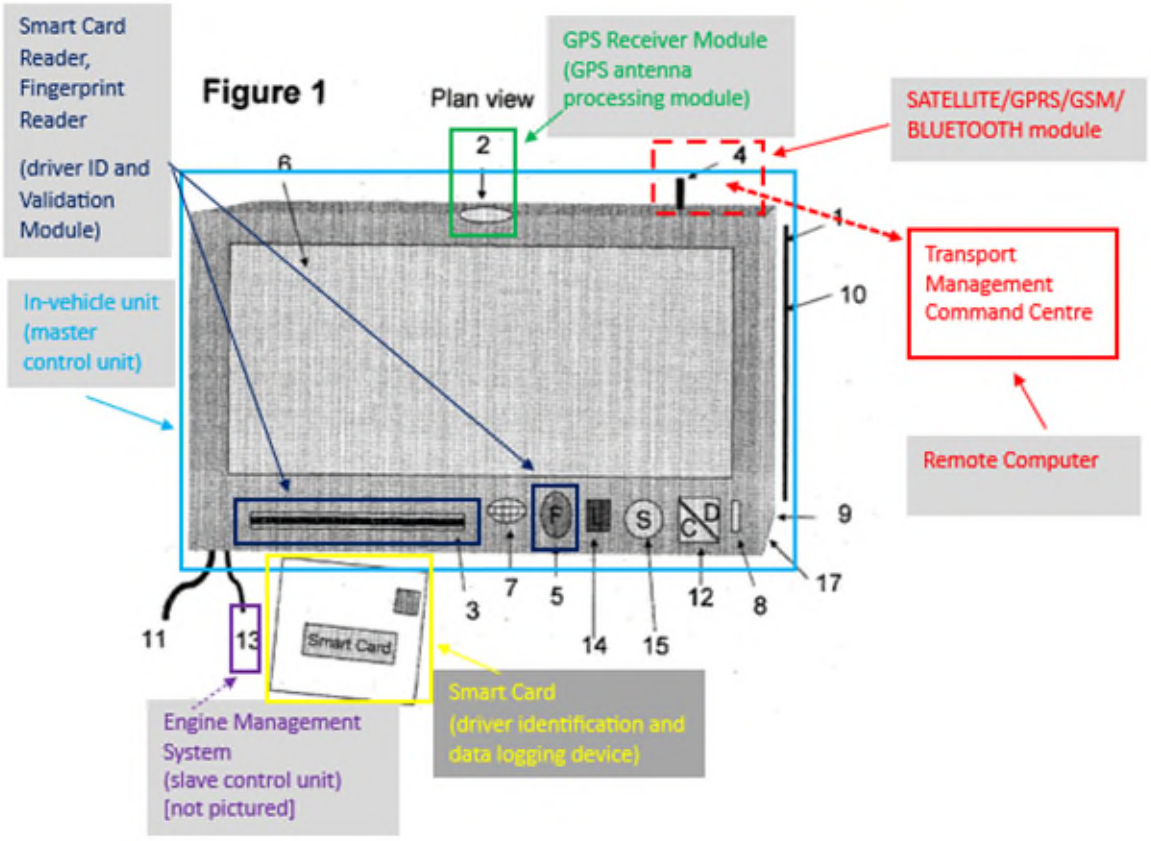
152. Petrik also teaches that the dispatcher can "create, file, store, and track route plans" using "a computer network supporting an internet on-line facility." (Petrik, cl. 49.) Further, a POSITA would have understood that the dispatcher would need to use a remote computer to file the intended vehicle rout plan and cargo details "via the SATELITE/GPRS/GSM" (via a network) because the dispatcher would have to use a computer to cause the information to be sent over the network. (Petrik, [0024], [0030].)

c. Dependent 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.*

153. Petrik discloses or renders obvious Claim 3. As I've discussed in V.B.1.ii (claim 1[A]), prior to each departure, a dispatcher files "the intended vehicle rout plan and cargo details ... in the in-vehicle unit via the SATELITE/GPRS/GSM." (Petrik, [0024].) As I discussed for the Slave Control Unit limitations, 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].) "Simultaneously the monitoring unit displays the 'filed' truck rout plan and a time chart showing the driver rest times calculated from the drivers' current work/rest status recorded on the smart card." (*Id.*) A POSITA would recognize that loading the operating profile (at least the intended vehicle rout plan)

can be performed in conjunction with the driver identification and data logging device (smart card) and a remote computer necessary to transmit the rout plan to the in-vehicle unit via the SATELITE/GPRS/GSM. Petrik explains that the dispatcher loads the intended vehicle route plan and cargo details to the in-vehicle unit prior to each departure, and that when the driver inserts the smart card into the unit's smart card reader/writer and uses the fingerprint reader, the system logs the driver in as the current driver, enables ignition, and displays the filed route plan. (Petrik, [0024], [0025].)



(Petrik, Fig. 1 (annotated).)

d. Dependent 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.*

154. Petrik anticipates or renders Claim 4 obvious. As discussed in Section V.B.1.ii (claim 1[A]), Petrik discloses a master control unit in a motor vehicle (in-vehicle monitoring unit) for authenticating at least one driver via a driver identification and data logging device (smart card). The in-vehicle unit enables the engine ignition if the driver is authenticated, but will not start the engine if "an invalid driver card and fingerprint combination is presented." (Petrik, [0025].) To authenticate the driver, the in-vehicle monitoring unit necessarily has a software module that identifies and validates a driver based on the smart card and fingerprint.

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

156. Petrik also discloses a memory module, both in the in-vehicle monitoring unit and a smart card memory. Petrik teaches that the in-vehicle monitoring unit "is supplied with an upgradable software program[,]" that "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].)

157. Petrik also discloses a function indicator module. Petrik discloses a beeper 7 which is an indicator. (Petrik, [0016]; *see also* Fig. 1 (annotated above).) The in-vehicle unit is programed such that using its "intelligent speed adaptation and geographically based speed zone location tables, beeps to warn the driver of the zone change and if allowed, interacts with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025].) A POSITA would recognize the beep as a response to a restriction being violated when the speed is higher than the limit in the new zone requiring the engine management to slow it down. 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.

e. Dependent 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.*

158. Petrik anticipates or renders Claim 5 obvious. As I've discussed in Section V.B.1.d (claim 4), Petrik discloses a memory module, both in the in-vehicle monitoring unit and a smart card memory module. Petrik teaches that the intended route plans are "filed" in the unit. (Petrik, [0011].) A POSITA would understand that the operating profile, including intended route plans, are stored within the in-vehicle unit memory module. (S*ee* Petrik, [0018] (operating parameters are records are stored within memory).)

f. Dependent 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.*

159. Petrik anticipates or renders Claim 6 obvious. As I've discussed in V.B.1.d (claim 4), Petrik discloses a GPS Receiver Module 4, which is a GPS antenna processing module. (Petrik, [0016].) Petrik further teaches that during a trip, "the GPS 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].)

g. Dependent 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.*

160. Petrik renders Claims 7 and 12 obvious. As I discussed in V.B.1.iii (claim 1[B]), Petrik discloses an engine management system (slave control unit). Petrik also teaches a power connector 11 in one embodiment and a power/cigarette lighter connector in another embodiment of the in-vehicle unit. (Petrik, [0016], [0040].) A POSITA would understand either one to imply a power regulator to regulate a power source for the vehicle to allow Petrik's engine management to control vehicle operations, as all vehicle electronic systems require power supplies that have regulated voltage. A POSITA would be motivated to implement a power regulator in the engine management system, as a power regulator or an equivalent would be necessary for operation of the corresponding powertrain ECU for the engine management system to slow down the vehicle. (Petrik, [0025].)

161. Petrik further discloses or at least renders obvious a starter relay in the engine management system. Petrik teaches that 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, which "can be enabled by a starter enable signal 518 from the master control unit 430 when the driver 410 is authenticated." ('101, 8:7-10.) A POSITA would recognize that this function requires a starter relay in the engine management system.

162. Petrik also discloses or at least renders obvious a definable relay module in the engine management system. Petrik teaches that the engine

management system (the slave control unit) 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. The ’101 Patent teaches that Breathalyzer pin 542 provides a signal to a definable relay 524 in the slave control unit, which can provide status regarding alcohol consumption of the driver 510 while driving the vehicle, which would then enable the slave control unit to relay the status to other components including the master control unit. (’101, 7:59-61, 8:16-18, FIG 6.) A POSTIA 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 the engine management system in Petrik receives information that it logs and passes it along to another part of the system to transmit to the Transport Management Command Centre. Thus, Petrik discloses that the slave control unit (engine management system) comprises a definable relay module.

163. Alternatively, Petrik teaches that the engine management system prevents the vehicle from starting if authentication fails. (Petrik, [0025].) Petrik further teaches that 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. 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 in order to signal when to cause the engine to slow or stop.

164. Petrik further discloses or renders obvious that the slave control unit comprises a slave microcontroller. Petrik teaches that the engine management system includes an engine management computer. (Petrik, claims 64, 68, 70, 89, 98, 100.) A POSITA would understand 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). Thus, Petrik discloses or renders obvious that the slave control unit (engine management system) comprises a slave microcontroller.

165. Finally, Petrik discloses or renders obvious that the slave control unit comprises an alarm synthesizer. As discussed for the Slave Control Unit limitations, Petrik teaches that the in-vehicle unit can "interact[] with the engine management system [(slave control unit)] to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone" 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 (teaching that slowing down the vehicle can constitute an “alarm signal”.) Additionally, Petrik teaches generating a beep if a driver exceeds a speed limit on the intended rout plan. (Petrik, [0025].) Thus, Petrik discloses or at least renders obvious that the slave control unit (engine management system) is configured to generate at least one of an alarm signal (e.g., disable command to lock up the engine management system or 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 based on, for instance, the current speed and speed limit.

166. Thus, Petrik discloses or renders obvious that the slave control unit comprises a power regulator module, a starter relay module, a definable relay module, a slave microcontroller, and an alarm synthesizer.

167. Further, as I discussed above in V.A.1.g (Ground 1, claims 7 and 12), a POSITA would have understood that the additional components claimed in Claims 7 and 12 are standard electrical components that have been known for decades. There is nothing inventive about including these components in a vehicle control unit. To the extent Petrik does not explicitly disclose these elements, it would have been obvious for a POSITA to implement these components within the

engine management control system of Petrik, as it would amount to nothing more than a simple substation or combination of known elements.

h. Dependent 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.*

168. Petrik anticipates or renders Claims 8 and 13 obvious. As I discussed in V.B.1.ii (claim 1[A]) and V.B.1.iii (claim 1[B]), Petrik teaches that the in-vehicle unit uses "its' intelligent speed adaptation and geographically based speed zone location tables, beeps to warn the driver of the zone change and if allowed, interacts with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025].) Petrik further discloses that the GPS cruise control "can be programmed never to allow the vehicle to exceed a set absolute maximum speed" and even though the "driver can always override the system by using the break, or the accelerator," the driver can only accelerate "to the set absolute maximum speed." (*Id.*, [0025] – [0026].) A POSITA would have recognized that such maximum speed limit could be driver-specific and would recognize that such a driver-specific maximum speed limit would provide greater customizability for the system. Thus,

Petrik discloses or at least renders obvious that the at least one operating parameter comprises at least a maximum allowable vehicle speed.

i. Dependent 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.*

169. Petrik anticipates or renders Claims 9, 14, 17, and 18 obvious. As discussed in V.B.1.iii (claim 1[B]), Petrik discloses or at least renders obvious that the slave control unit (engine management system) is configured to generate an alarm signal (e.g., disable command to lock up the engine management system) if the driver violates the operating profile (e.g., operating parameters including at least the intended vehicle rout plan). Petrik further teaches that "[i]f a driver diverts inappropriately from the 'filed' route plan the unit notifies the Centre." (Petrik, [0030].) Thus, a signal (alarm signal) is generated by the engine management system (slave control unit) when the driver violates the operating profile, and the signal is used to notify the Centre (authorized user).

j. Dependent 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.*

170. Petrik renders Claim 10 obvious. As discussed in V.B.1.ii (claim 1[A]), the smart card is the driver identification and logging device. As I've discussed in V.A.1.j (Ground 1, claim 10), smart cards were known at the time of the invention of the '101 Patent to incorporate RFID technology for automatic identification. (*See, e.g.*, EX1010.) A POSITA would have been motivated to incorporate RFID technology into the smart card (or the smart card reader writer) to simplify the log-in process for the driver. For example, instead of "insert[ing]" the smart card, the driver could tap the card if RFID technology was incorporated. This has long been recognized as desirable to consumers. (*See, e.g.*, EX1010.)

k. Dependent 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.*

171. Petrik anticipates or renders Claim 16 obvious. As I have discussed in V.B.1.vi (Claim 11[B]), Petrik discloses a GPS module. The GPS module "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].)

l. Dependent 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.*

172. Petrik anticipates or renders Claims 19 and 20 obvious. As I have discussed in V.B.1.iii (claim 1[B]), Petrik teaches that the in-vehicle monitoring 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].) This would necessarily require sending a control signal to the engine to slow down or disable to engine.

2. Ground 5: Petrik in view of Schanz Renders Obvious Claims 1-20

173. Petrik in view of Schanz renders Claims 1-20 obvious.

a. Motivation to Combine Petrik and Schanz

174. It would have been obvious for a POSITA to combine Petrik with Schanz, which disclose complimentary methods for driver authentication and monitoring. (Petrik, Abstract, [0001] – [0015], [0025] – [0026]; Schanz, Abstract, [0006] – [0010], [0017] – [0027].) Like Petrik's in-vehicle monitoring unit, Schanz's "device 1" identifies and authenticates a driver and provides driver-specific parameters. (Schanz, [0018], [0020].) *See* section V.A.2.a (discussion of Schanz in Motivation to Combine Murphy and Schanz).

175. A POSITA would have looked to Schanz to improve Petrik given their similarities and benefits. 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].) 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 safety of the driver. (*Id.*)

176. 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].)

177. Combining Petrik and Schanz would have been nothing more than the simple combination of known elements to obtain predictable results. 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 can identify and authenticate a driver without mechanical interaction of the smart card and can notify the driver and

administrator when any of those restrictions are violated. 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. A POSITA would have had a reasonable expectation of success in combining Petrik with Schanz because both disclose vehicle units (in-vehicle unit of Petrik and device 1 of Schanz) that serve analogous functions and operate in similar ways to improve driver safety. A POSITA would have understood that features of Schanz's "device 1" can be easily applied to Petrik's in-vehicle monitoring unit, and vice-versa.

b. Independent Claims 1, 11, 15

178. Petrik in view of Schanz renders independent Claims 1, 11, and 15 obvious.

i. Preambles (1[P])

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

179. To the extent the preamble is limiting, Petrik in view of Schanz discloses a driver authentication and monitoring system and method. As discussed in V.B.1.i (Ground 4, claim 1[P]), Petrik discloses a driver authentication and monitoring system and method. 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," such

as a "maximum vehicle speed," "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].) (Id., [0024]-[0025].)

ii. Master Control Unit (1[A])

1[A]	*a master control unit in a motor vehicle for authenticating at least one driver via a driver identification and data logging device wherein master control unit receives a unique identification code to permit said at least one driver to operate said vehicle within an operating profile;*

180. Petrik in view of Schanz renders obvious claim 1[A]. As discussed in V.B.1.ii (Ground 4, claim 1[A]), Petrik discloses an in-vehicle monitoring unit (a master control unit in a motor vehicle) which uses a smart card (driver identification and data logging device) with a "smart card reader/writer" and "fingerprint reader" "to confirm [a driver's] identity." (*See* Petrik, [0025].) The in-vehicle monitoring unit of Petrik associates a driver with an operating profile when the driver is identified, and permits vehicle operation within the operating profile. (Petrik, [0025]-[0028].)

181. In addition, Schanz discloses a "device 1" which performs functions analogous to the in-vehicle monitoring unit of Petrik. For example, the "device 1" of Schanz includes a "recognition device 3" (driver identification and data logging device) "which identifies the driver." (Schanz, [0018].) Subcomponents of the "device 1" "check[] whether special vehicle parameters 6 are stored for the

respective driver." (*Id.*, [0020].) In Schanz, vehicle parameters include restrictions such as "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].) For the reasons discussed in V.B.2.a, a POSITA would have been motivated to combine these features with the in-vehicle monitoring unit of Petrik, as the "device 1" of Schanz and in-vehicle monitoring unit of Petrik serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety.

182. As discussed in V.B.1.ii (Ground 4, Claim 1[A]), Petrik does not explicitly recite a "unique identification code." However, Schanz discloses that "recognition device 3" within "device 1" (master control unit) may include "a reading device…for recognizing an identification code 22." (Schanz, [0018].) A POSITA would have recognized the advantage of including a reading module in the in-vehicle unit of Petrik to receive and recognize an identification code for the particular driver. A POSITA would have been motivated to implement Schanz's teachings of recognizing an identification code into Petrik's in-vehicle monitoring unit in order to achieve Petrik's goal of identifying and authenticating the individual driver based on the combination of the smart card (which contains the fingerprint template) and the driver's fingerprint. (Petrik, [0022], [0025].) A

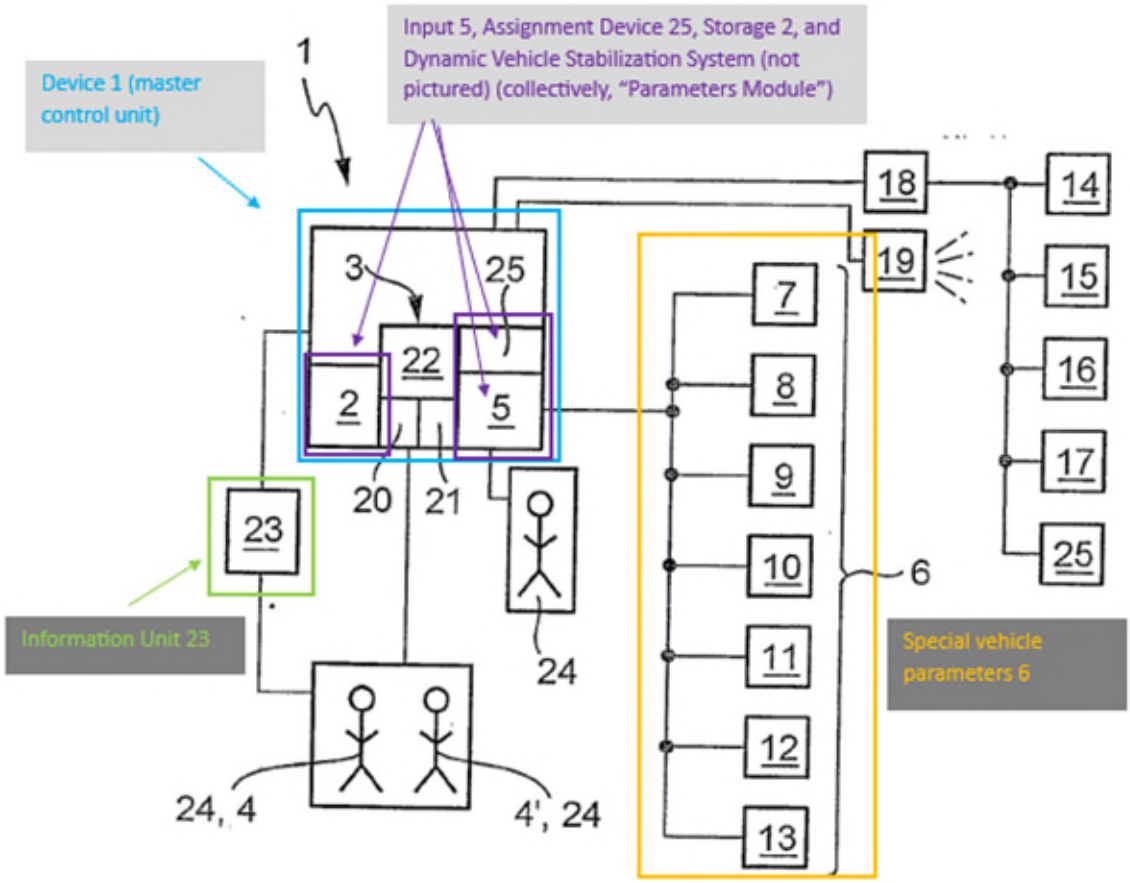
POSITA would have had a reasonable expectation of success in combining Petrik's in-vehicle unit with Schanz's module for recognizing an identification code because the in-vehicle unit of Petrik and device 1 of Schanz serve analogous functions and operate in similar ways to improve driver safety. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results.

iii. Slave Control Unit (1[B])

1[B]	*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;*

183. Petrik in view of Schanz renders obvious the Slave Control Unit limitations. As I've discussed in V.B.1.iii (Ground 4, Claim 1[B]), Petrik discloses that the in-vehicle unit (master control unit) connects to an engine management system (slave control unit; not shown in Fig. 1) using 13 "the engine management system connector." (*See* Petrik, [0069], Fig. 1 (annotated above).) 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.



(Schanz, Fig. 1 (annotated).)

184. 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" in order to enforce "vehicle parameters 6" such as "maximum vehicle speed," "maximum distance 12 to the vehicle driving ahead," and "intervention parameter of a dynamic vehicle stabilization system." (Schanz, [0019]-[0020].) For example, the "device 1" can

"adjust[]," or control, a "dynamic vehicle stabilization system" to cause it to "actively intervene in driving operation of a beginner 'earlier' than in the case of an advanced driver, in order 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." (*Id.*, [0025].) As shown in Fig. 1, Schanz depicts "information unit 23" as external to the "device 1," but connected to the "device 1." (Schanz, Fig. 1.) This indicates that the "device 1" communicates with the "information unit 23," e.g., to cause it to generate an alarm when the "device 1" detects violation of a "vehicle parameter."

185. The combined Petrik-Schanz system would have an engine management system for governing mechanical operations of the vehicle remotely (from both Petrik's engine management system and Schanz's Parameters Module) and generating an audible alarm (from Schanz's information unit). For the reasons discussed in V.B.2.a, a POSITA would have been motivated to combine these features from Schanz with the engine management system of Petrik, as the Parameters Module of Schanz and engine management system of Petrik serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results.

186. Furthermore, the ’101 Patent specification illustrates the “slave control unit” 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 (commenting on identical figures and text in the specification of related U.S. Patent No. 10,259,470).) Therefore, 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 “slave control unit,” even if the two systems do not otherwise connect with or communicate with one another.

iv. Preamble (11[P])

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

187. Petrik in view of Schanz discloses a driver authentication and monitoring system and method. As discussed in V.B.1.i (Ground 4, claim 1[P]), Petrik discloses a driver authentication and monitoring system and method. 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,” such as a “maximum vehicle speed,” “are stored for the respective driver,” and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].) (Id., [0024]-[0025].)

v. Master Control Unit (11[A])

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;*

188. Petrik in view of Schanz renders obvious Claim 11[A]. In addition to the elements discussed in V.B.2.ii (claim 1[A]), Claim 11[A] also requires "associating an operating profile with said at least one driver." Because the in-vehicle unit in either Petrik or the Petrik-Schanz system loads an operating profile containing driver-specific intended vehicle route plan, speed limits associated with the route plan, and rest parameters when a driver is identified, the operating profile is associated with the driver, allowing the driver to operate the vehicle within the parameters of the associated restrictions. (Petrik, [0025]-[0026].)

vi. GPS (11[B])

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

189. Petrik in view of Schanz renders obvious Claims 11[B] and 16. As discussed in V.B.1.iii, V.B.1.vi (Ground 4, claims 1[B], 11[B]), Petrik discloses a GPS module which "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].)

vii. Data Logging Device (11[C])

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

190. Petrik in view of Schanz renders obvious Claim 11[C]. As discussed in V.B.1.vii (Ground 4, claim 11[C]), Petrik discloses storing speed and location information received from a GPS module in the monitoring unit's memory and in a secure smart card, each of which are a data logging device. (Petrik, [0018], [0009].)

viii. Slave Control Unit (11[D])

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;*

191. Petrik in view of Schanz renders obvious Claim 11[D]. As I previously discussed for claim 1[B], Petrik discloses a slave control unit. (*See* Section V.A.2.iii (claim 1[B]) *supra*).

ix. Unique Identification Code (11[E])

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.*

192. Petrik in view of Schanz renders obvious Claim 11[E]. As I previously discussed for claim 1[B], Petrik in view of Schanz renders obvious the master control unit receiving a unique identification code. (*See* Section V.B.2.iii (claim 1[B]) *supra*). In addition to the elements of claim 1[A], Claim 11[E] also requires permitting the driver to operate within an operating profile if "said at least one driver has not violated said operating profile." As discussed above in V.B.1.iii (Ground 4, claim 1[B]), Petrik teaches that the GPS in the in-vehicle unit can "interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025], [0047].) The '101 Patent specification explicitly teaches that slowing down the vehicle can constitute the "alarm signal." ('101 at 6:65-7:5.) Petrik also teaches that the engine management system can control the vehicle in response to commands from the remote national 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].)

x. Preamble (15[P])

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

193. Petrik in view of Schanz discloses a driver authentication and monitoring system and method. As discussed in V.B.1.i (Ground 4, claim 1[P]), Petrik discloses a driver authentication and monitoring system and method.

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," such as a "maximum vehicle speed," "are stored for the respective driver," and sensors to monitor activity and generate alerts. (Schanz, Abstract, [0019]-[0020], [0024]-[0025].) (Id., [0024]-[0025].)

xi. Driver Authentication and Monitoring System 15[A]

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

194. Petrik in view of Schanz renders obvious Claim 15[A]. As I discussed above for claim 1[A], Petrik discloses an in-vehicle unit with a smart card and fingerprint reader for identifying and authenticating a driver and monitoring compliance with certain parameters, which is "providing a motor vehicle with a driver authentication and monitoring system." (*See* Section V.B.1.ii (claim 1[A]) *supra*.)

xii. Operating Profile (15[B])

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

195. Petrik in view of Schanz renders obvious Claim 15[B]. As I discussed above for claim 1[A], Petrik discloses loading a driver-specific intended vehicle

route plan, speed limits, and rest parameters into the in-vehicle unit, which is "programming said driver authentication and monitoring system with an operating profile associated with a high risk driver." (*See* Section V.B.1.ii (Ground 4, claim 1[A]) *supra*; *see also* Section V.B.2.v (claim 11[A]) *supra*.) The Petrik-Schanz system described above in V.B.2.ii (claim 1[A]) also implement Schanz's driver-specific vehicle parameters Petrik's smart card, which would be loaded into the in-vehicle unit, which is further "programming said driver authentication and monitoring system with an operating profile associated with a high risk driver." (*See* Section V.B.2.ii (claim 1[A]) *supra*; *see also* Section V.B.2.v (claim 11[A]) *supra*.)

xiii. Monitoring Operation (15[C])

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;*

196. Petrik discloses or renders obvious Claim 15[C]. As I discussed above for claim 1[A], Petrik discloses inserting a smart card to the smart card reader/writer to authenticate a driver and enable operation so long as it is consistent with the driver-specific intended vehicle route plan, speed limits, and rest parameters, which is "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." (*See* Section V.B.1.ii (claim 1[A]) *supra*; *see also* Section V.B.1.v (claim 11[A]) *supra*.)

xiv. Alarm Signal (15[D])

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

197. Petrik in view of Schanz renders obvious Claim 15[D]. As I discussed above for claim 1[B], Petrik teaches that the GPS in the in-vehicle unit can "interact[] with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits in each zone." (Petrik, [0025], [0047].) The '101 Patent specification explicitly teaches that slowing down the vehicle can constitute the "alarm signal." ('101 at 6:65-7:5.) Petrik also teaches that the engine management system can control the vehicle in response to commands from the remote national 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].) (*See* Section V.B.1.iii (claim 1[B]) *supra*; Petrik, [0025], [0030], [0047].) The engine management system must send a signal to the engine to reduce vehicle speed, which is consistent with an alarm signal according to the '101 patent. (*Id.*; '101 Patent at 6:65-7:5 ("alarm signal" includes signal to slow down vehicle).)

Therefore, Petrik discloses "generating an alarm signal if said high profile driver violates said operating profile while operating said motor vehicle."

198. In addition the Petrik-Schanz system includes an "information unit 23" which "emits suitable optical and/or acoustic warning signals when the set vehicle parameters 6 are exceeded." (*See* Section V.B.2.iii (claim 1[B]) *supra*; Schanz, [0025].) Therefore, the Petrik-Schanz system renders obvious "generating an alarm signal if said high profile driver violates said operating profile while operating said motor vehicle."

xv. Governing Mechanical Operations (15[E])

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

199. Petrik in view of Schanz renders obvious Claim 15[E]. As I discussed for claim 1[B], Petrik teaches a signal to reduce vehicle speed when a driver violates an operating profile (including a driver-specific intended vehicle route plan, speed limits, and rest parameters), which can be loaded or changed remotely through the SATELITE/GPRS/GSM, is violated. (*See* Section V.B.1.iii (claim 1[B]) *supra*; Petrik, [0025], [0030], [0047].) Therefore, Petrik discloses "governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety.

200. Additionally, the combination of functionality of Schanz's Parameters Module into the engine management system would result in the engine management system "actively interven[ing] in driving operation of a beginner 'earlier' than in the case of an advanced driver, in order to alert the beginner to critical driving situations." (*See* Section V.B.2.iii (claim 1[B]) *supra*; Schanz, [0022].) Therefore, the Petrik-Schanz system renders obvious "governing mechanical operations of said vehicle remotely if said high profile driver violates said operating profile thereby maintaining occupant safety."

c. Dependent 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.*

201. Petrik in view of Schanz renders Claim 5 obvious. As discussed in V.B.1.e (Ground 4, claim 5), Petrik discloses the operating profile is loaded into the memory module for enabling operation of the vehicle when the driver is authenticated. In addition, Schanz discloses that an "assignment device 25" "checks whether special vehicle parameters are stored" in "storage device 2" (memory module) "for the respective driver 4." (Schanz, [0017], [0020].) If parameters are stored for the identified driver, the parameters 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 enabling controlled operation of the vehicle when the driver is authenticated. For the reasons discussed in V.B.2.a, a POSITA would have been motivated to combine these features from Schanz with the in-vehicle unit of Petrik, as the "device 1" of Schanz and in-vehicle unit of Petrik serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. In the combined system, Schanze's parameters would be loaded to the memory module of Petrik's in-vehicle unit. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results.

d. Dependent 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.*

202. Petrik in view of Schanz renders Claims 8 and 13 obvious. As discussed in V.B.1.h, Petrik discloses a maximum speed limit operating parameter. (Petrik, [0025].) Similarly, Schanz discloses additional definable "vehicle parameters 6" (operating profile) that 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" "so that the driving dynamic characteristics of the vehicle can be adjusted in

relation to the driving skills of the respective driver." (*Id.*, [0020].) For the reasons discussed in V.B.2.a, a POSITA would have been motivated to combine these features from Schanz with the in-vehicle unit of Petrik, as the "device 1" of Schanz and in-vehicle unit of Petrik serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results.

e. Dependent 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.*

203. Petrik in view of Schanz renders Claims 9, 14, 17, and 18 obvious. In addition to Petrik's alarm for remotely alerting an authorized user when the operating profile is violated, (*supra* V.B.1.i; Petrik, [0030]), Schanz discloses that "information unit 23" (part of the "slave control unit") "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 the "information unit 23" is provided "remotely." However, Petrik

discloses a "SATELITE/GPRS/GSM" link which connects its in-vehicle monitoring unit to a remote facility and allows the unit to report speed limit violations to the remote facility. (Petrik, [0030], [0063].) As discussed in Section V.B.2.ii-iii, 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. For the reasons discussed in section V.B.2.a, a POSITA would have been motivated to combine these features from Schanz with the in-vehicle unit of Petrik, as the "device 1" of Schanz and in-vehicle unit of Petrik serve analogous functions, operate in similar ways, and serve similar goals of improving driver safety. Further, the modification would have been nothing more than the simple combination of known elements to obtain predictable results.

f. Dependent 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.*

204. Petrik in view of Schanz renders Claim 10 obvious. 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. 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 using a unit capable of transmitting and receiving data signals for use in identifying the driver. 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.

g. Dependent 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.*

205. Petrik in view of Schanz renders Claims 19 and 20 obvious. As discussed for the Slave Control Unit limitations, Petrik teaches its engine management system provides a control signal when it slows down or disables the engine. (Petrik, [0025].) Furthermore, 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).) It would have been obvious to a POSITA to combine the teachings of Petrik's control signal with Schanz's teaching of intervening in driving operations to alert the driver. A POSITA would have understood the benefits of this combination. 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.

h. Dependent Claims 2-4, 6-7, 12, 16

206. For the reasons discussed in sections V.B.2.a and V.B.1.b-d, f-g, k (Ground 4, Claims 2-4, 6-7, 12, and 16), Petrik in view of Schanz renders obvious Claims 2-4, 6-7, 12, and 16.

3. Ground 6: Murphy in view of Schanz in view of Benco Renders Obvious Claim 10

207. As I discussed in V.A.3 (Ground 3), Benco teaches in the background that "many automobiles are sold with remote keyless ignition systems" that "allow individuals to start an ignition of an automobile from a short distance away from the automobile, eliminating the need to physically manipulate a key into an ignition of the automobile." (Benco, [0002].) Benco further teaches that "[a] remote keyless ignition system uses a coded Radio Frequency Identification (RFID) chip." (*Id.*, [0003].) "The remote keyless ignition system operates based on a radio frequency signal being emitted from the automobile and received by a fob." (*Id.*) The fob would then send a response to the automobile, and the automobile would be started. (*Id.*)

i. Dependent 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.*

208. To the extent Petrik alone (as described in section V.B.1.j (Ground 4, claim 10)) or Murphy in view of Schanz (as describe in section V.B.2.f (Ground 5, claim 10) fails to render obvious claim 10, it would have further been obvious to implement Petrik's smart card using a radio frequency identification device in view of Benco.

209. Benco teaches in the background that "many automobiles are sold with remote keyless ignition systems" that "allow individuals to start an ignition of an automobile from a short distance away from the automobile, eliminating the need to physically manipulate a key into an ignition of the automobile." (Benco, [0002].) Benco further teaches that "[a] remote keyless ignition system uses a coded Radio Frequency Identification (RFID) chip." (*Id.*, [0003].) "The remote keyless ignition system operates based on a radio frequency signal being emitted from the automobile and received by a fob." (*Id.*) The fob would then send a response to the automobile, and the automobile would be started. (*Id.*)

210. A POSITA would have been motivated to combine Petrik (or Petrik in view of Schanz) with Benco to provide convenience to the drivers with a remote keyless ignition system. As Benco explains, many automobiles were sold with remote keyless ignition systems" that "use[d] a coded Radio Frequency Identification (RFID) chip." (Benco, [0002].) Petrik's smart card would use RFID to communicate with the in-vehicle unit's smart card reader/writer. (*See* Petrik,

[0025], Fig. 3.) It would have been well within the skill of a POSITA to implement Petrik's smart card using RFID as taught by Benco, as RFID was commonly used for remote keyless ignition systems within the automotive industry.

VI. CONCLUSION

211. For the reasons stated above, I believe that Claims 1-20 of the '101 Patent are unpatentable in view of the prior art.

VII. CERTIFICATION

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the U.S. Code.

_____

Mark Ehsani, Ph.D., P.E., LF IEEE, F. SAE

Dated: December 9, 2024

APPENDIX A

Materials Considered

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	FMBSS No. 126: Electronic Stability Control Systems (March 2007)
1012	File History for U.S. Patent Reexamination Proceeding No. 90/015,287