

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

MERCEDES-BENZ GROUP AG,  
Petitioner,

v.

THE PHELAN GROUP, LLC  
Patent Owner.

---

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

**DECLARATION OF DR. MARK EHSANI  
IN SUPPORT OF MERCEDES' PETITION FOR *INTER PARTES* REVIEW  
OF CLAIMS 1-20 OF U.S. PATENT NO. 11,472,427**

---

Filed on behalf of Petitioner:

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

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* review (“IPR”) proceeding of U.S. Patent No. 11,472,427 (“’427”) (EX1001).

2. Specifically, I have been retained to offer my opinions regarding Claims 1-20 of the ’427 Patent and the prior art references set forth in the IPR petition. This declaration is directed to the challenged claims of the ’427 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 ’427 Patent as of its earliest possible priority date of July 2, 2008.

## **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, vehicle electrical and control systems, electric and 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 1007. 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 45 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 '427 Patent, as well as the state of the art at that time.

### **C. Information Considered**

13. I have reviewed the '427 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 '427 Patent, at the time of the earliest purported priority date of the '427 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 '427 Patent has a priority date of July 2, 2008.

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 '427 PATENT**

### **A. Background of the '427 Patent**

17. I have reviewed the '427 Patent and its prosecution history. The '427 Patent is directed toward “[a] driver authentication and safety system and method for monitoring and controlling vehicle usage by high-risk drivers.” ('427 Patent,

Abstract, 2:34-38.) 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.*, 6:39-7:7.) Restrictions in the operating profile are enforced by a “driver authentication system” which includes a “master control unit” that interfaces with the driver, and a “slave control unit” that alarms upon violating the operating profile. (*Id.*, 2:32-51; 5:68-6:4; Fig. 6.)

18. When entering the vehicle, driver identification information and operating profile restrictions are loaded to the “master control unit” using a “driver identification and data logging” device. (*Id.*, 2:32-51.) Upon identifying an authorized driver, driving activity is monitored by use of a GPS which provides “time of day, speed and location data associated with the vehicle.” (*Id.* at 3:2-4.) If the driver violates an operating profile restriction, a “real time alarm signal” is generated. (*Id.*, Abstract, 2:47-3:4.) “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.*, 7:21-28; *see also* 7:13-29, 2:47-51, Abstract.) Drivers can authenticate themselves via a “driver identification” interface, such as by

presenting an “iButton, radio frequency identification device (RFID), etc.” (*Id.*, 6:64-7:2, 2:64-3:1.)

**B. Prosecution History of the '427 Patent**

19. I understand the '427 Patent was filed on February 28, 2019, as a continuation of U.S. Patent No. 10,259,465 (“’465”), filed on February 16, 2018, which is a continuation of U.S. Patent No. 9,908,508 (“’508”), filed May 14, 2015, which is a continuation of U.S. Patent No. 9,045,101 (“’101”), filed April 8, 2013, which is a continuation of U.S. Patent No. 8,417,415 (“’415”), filed on July 1, 2009, and Provisional application no. 61/077,568, filed on July 2, 2008. The '427 received one substantive Office Action in which claims 1-20 were rejected for double-patenting over several related patents. (EX1002, 130-133.) Patent Owner filed a terminal disclaimer, prompting a second Office Action which rejected the terminal disclaimer because it was not signed by the Patent Owner or an attorney of record. (*Id.*, 112-114, 79-83.) Patent Owner then corrected the signature but received a further Advisory Action because the wrong box was checked. (*Id.*, 69.) Patent Owner again corrected the terminal disclaimer, and a Notice of Allowance issued. (*Id.*, 62; 24.)

20. I understand that several prior art references relied on in this Petition were not before the PTO during prosecution of the '427 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 '427 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 '427 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 '427 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. CLAIMS 1-20 OF THE '427 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 '427 Patent are disclosed in the primary prior art references: U.S. Patent No. 6,225,890 to Murphy (“Murphy”) (EX1006), U.S. Patent Publication No. 2003/0189482 (“Arshad”) (EX1007), and U.S. Patent Application Publication No. 2007/0168125 to Petrik (“Petrik”) (EX1008). I was also asked to consider these references in view of certain additional prior art, including U.S. Patent Application

Publication No. 2008/0046739 to Adams (“Adams”) (EX1009) and U.S. Patent Application Publication No. 2008/0114501 to Wu (“Wu”) (EX1010).

35. My analysis of these prior art references relative to the elements of Claims 1-20—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. Murphy was filed on March 20, 1998, and issued on May 1, 2001. I understand Murphy is prior art under at least pre-AIA 35 U.S.C. § 102(b).

37. My review of the ’427 Patent history reveals that Murphy was not considered during the prosecution of the ’427 Patent or its parent patents.

38. 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.) Specifically, 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). (*Id.*, 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.)

**1. Ground 1: Murphy Anticipates or Renders Obvious Claims  
1-6, 8-11, 13-14, 15-20**

**a) Independent Claim 1**

39. As viewed by a POSITA, Murphy renders obvious independent Claim 1.

**(i) Claim 1[pre]: *A driver authentication and monitoring system, comprising:***

40. Murphy discloses the preamble of Claim 1 to the extent the preamble limits the scope of the claims. Murphy discloses “[a] *system* for restricting use of a vehicle by a selected vehicle operator to permitted time intervals and permitted vehicle travel corridors.” (Murphy, Abstract.)<sup>1</sup> Murphy describes a system with various components, such as a controller module and a token receiving and analysis module (TRAM) that authenticates the identity of a driver through a presented

---

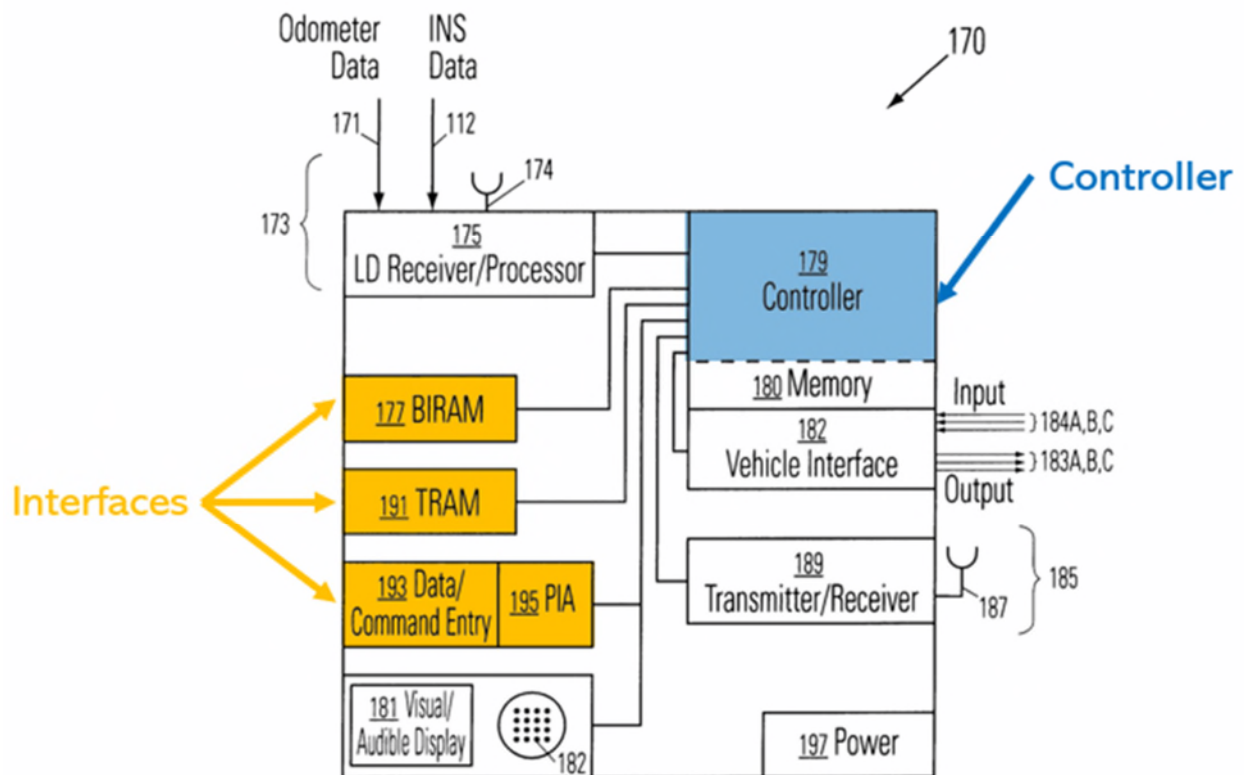
<sup>1</sup> All emphases are added in this Declaration unless otherwise indicated.

identity indicium (e.g., fingerprint and/or encoded information on a token or smart card) and allows the driver to operate the vehicle within specified operating parameters, as well as a BIRAM and a data entry device/PIA (each of which can also be used to authenticate a driver), a location determination (LD) module (which can, for example, determine vehicle location and speed, such as using GPS), an audio/video display, a vehicle interface, and a transmitter/receiver. (Murphy, Abstract, 4:39-44, 5:13-24, 6:55-59, 15:1-8, 11:60-67, 13:28-42, 14:46-15:31, 15:66-16:11, 19:3-12, Figs. 1, 6-7). Murphy's system can be used in motor vehicles like cars and can be "installed in a vehicle dashboard or elsewhere in the vehicle" and "used to monitor operation of the vehicle by a teenager or other inexperienced driver, with restrictions imposed upon vehicle operation channel, total vehicle mileage, vehicle maximum speed and/or time interval of operation of the vehicle." (*Id.*, 15:1-8, 11:60-64; *see also* Fig. 1, Figs. 6-7.) *See also infra* Ground 1, Claim 1[A].

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

41. Murphy discloses Claim 1[A]. Murphy's system includes a "master control unit." As the claim recites, the master control unit is a control unit for authenticating a driver via a "driver identification" interface.

42. Murphy’s in-vehicle system includes a “master control unit” comprising a “controller 179” that can “authenticate” or identify drivers via multiple interfaces in the car. (Murphy, 6:55-7:14, 13:28-42, 14:46-65, Fig. 6 (annotated below).) Such interfaces include, as depicted in Fig. 6, (1) a “biometric indicium receiving and analysis mechanism” (BIRAM), (2) a “token receiving analysis mechanism” (TRAM) that receives and analyzes a “token or smart card,” and (3) a “data entry module” (e.g., keypad) and “personal information analysis (PIA) module”:



(*Id.*, Fig. 6 (annotated), 4:39-62, 6:55-7:14, 13:28-42, 14:46-65.) Similarly, Figure 7

depicts this same controller (209), as well as the same BIRAM (203), TRAM (205) and token, and keypad and PIA (207). (*Id.*, Fig. 7, 7:24-29, 15:8-31.) For these reasons, and as I discuss herein, Figures 6-7 are largely the same and are simply different types of diagrams. As Murphy discloses, Figure 6 is a “schematic view of [an] apparatus,” whereas Figure 7 “illustrates” the “system.” (*Id.*, 3:13-16.)

43. For example, when a driver of the car or other vehicle “activates the vehicle by turning on the ignition system and thereby activates the driver control system,” Murphy’s system prompts the driver to “provide[] a sample of his/her (first) ident indicium (a biometric indicium and/or token or keypad entries).” (*Id.*, Abstract, 7:49-54, Fig. 2, Abstract.)<sup>2</sup> Murphy’s BIRAM can receive the driver’s “thumbprint, fingerprint, handprint, partial or full facial image, retina, iris, voice sample, cursive signature, blood vein pattern, blood sample or other suitable biometric indicium.” (*Id.*, 4:39-5:12; *see also* 2:20-34, 16:50-17:2, Cl. 37.) Its TRAM can receive a “token or smart card” with “personal information on the (putative) token holder and/or information on limitations under which the token holder can operate a vehicle.” (*Id.*, 6:55-7:14, 14:46-61; *see also* 2:32-34, Cl. 38.) Furthermore, Murphy’s “data entry

---

<sup>2</sup> Murphy states that “ident indicium” refers to “a biometric indicium and/or to a[n] information contained in a token and/or to information entered via a keypad, according to whatever is presented for identification.” (*Id.*, 7:24-29.)

module” (e.g., keypad, floppy drive, CD ROM drive, etc.) and PIA can receive “entry of information that is specific to and known to only the individual who presents the information,” such as a “coded sequence of characters and/or may be entered as one or more responses to questions posed by a personal interrogation system and visual/audible display that are connected to the keypad.” (*Id.*, 7:15-24, 14:55-65, Cl. 39.) Because (1) the BIRAM, (2) TRAM and token, and (3) data entry module and PIA can each interact or interface with the driver and Murphy’s system can use them to identify the driver with the information received, each alone or in combination is a “driver identification interface.”

44. In this regard, Murphy further discloses that the BIRAM, TRAM and token, and data entry module and PIA can be used alone or in combination. (*Id.*, 6:55-61, 7:22-24, Figs. 6-7, 13:28-42, 14:45-65, 15:9-15.) For example, it teaches that that “[i]n addition to, or instead of, presentation of a biometric indicium, the vehicle may require insertion of presentation of a token or a smart card...” (*Id.*, 6:55-59.) Similarly, it teaches that “[t]he keypad entry system may be used in place of, or to supplement, the BIRAM and/or the token, as a means of authenticating the identity of the presenter.” (*Id.*, 7:22-24.)

45. The system of Murphy can use such information received from any or a combination of the BIRAM, TRAM and token, and data entry module and PIA to

“authenticat[e] the identity” of the driver. (*Id.*, 7:15-24.) In particular, the received information is “sent to the controller module 179 and associated memory module 180 to determine, where possible, the identity of a vehicle operator [the driver] who has presented the indicium.” (*Id.*, 13:36-40, 14:51-54, 14:62-65, Fig. 6.) Furthermore, Murphy’s system can include an “identifier module 201” that “analyzes the ident indicium or indicia presented” from the BIRAM, TRAM and token, and/or data entry module and PIA. (*Id.*, 15:8-54, Fig. 7 (depicting the same).) The identifier module then “transmits the ident information, or a representation thereof” to the controller module for “matching indicia for one or more authorized drivers of the vehicle,” which is a process to authenticate the driver’s identity. (*Id.*) Thus, in other words, according to Murphy, the “identifier module” can act as an intermediary between the driver identification interface(s) and the controller (such as to ensure that the “ident information” is in a form that can be used for comparison by the controller), or such functionality can simply be included in the controller.

46. Additionally, Murphy discloses that its controller module can authenticate the would-be driver by “*compar[ing]* the [received] indicium *with stored indicia*,” such as from a “database with identities and matching indicia for one or more authorized drivers of the vehicle.” (Murphy, 5:12-24, 15:8-21; *see also*

2:26-38, Fig. 2, 7:49-63, Fig. 3, 10:45-11:27, Figs. 6-7, 14:46-65, 15:55-16:11, 16:50-17:62.) *See also infra* Ground 1, Claim 1[B].

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

47. Murphy discloses Claim 1[B].

48. Murphy's system authenticates and monitors "restricted operators" ("ROs"). (Murphy, 1:9-28.) In Murphy, an operator may be "restricted" because she has "physical, mental or emotional impairment," "recent convictions" for "driving under the influence of alcohol or drugs," is of "advanced age" or "very young," or is "transport[ing] hazardous materials." (*Id.*, 1:9-28, 3:20-47.) In other words, Murphy is designed to monitor and control vehicle use when a high risk driver is involved. For example, a "very young" driver may have "not yet acquired" safe "driving and reaction skills," and therefore poses a high risk if she is allowed to freely operate a vehicle. (*Id.*, 3:20-47.) Murphy contemplates reducing the risk posed by high risk drivers by, for example, only allowing them to operate the vehicle "within a permitted travel corridor," such as "to commute to and from work during restricted workday hours." (*Id.*)

49. Murphy's system can divide drivers into categories, including (1) ROs ("restricted operators") and (2) drivers who are "identified and authorized[]" but not an RO," as well as (3) "unidentified" drivers, (4) drivers whose "identification indicium (presented) is too degraded to permit determination of the driver's identity," and (5) drivers who have "failed to present a sample of the requested identification indicium." (Murphy, 7:64-8:2, 2:35-53; *see also* 1:66-2:16, Fig. 2, 3:20-47, 7:49-9:44, 5:18-26, 11:60-67, 17:3-13.) "***Different driving restrictions*** are imposed[] depending upon the category to which the operator belongs," including on "permitted time intervals and permitted travel corridor(s) and speeds for travel." (Murphy, 7:64-8:2, 2:35-53; *see also* 1:66-2:16, Fig. 2, 3:20-47, 7:49-9:44, 5:18-26, 11:60-67, 17:3-13.) In other words, for example, if a driver is categorized in the system as a restricted operator, she may be limited to driving at certain times of the day and limited to low speeds, whereas identified and authorized drivers who are not categorized as restricted operators may be able to drive for longer periods of the day and with higher speed restrictions. Similarly, as an additional example, drivers who are categorized as "unidentified" may be limited to driving only in certain nearby corridors or areas.

50. Drivers can also be assigned with their own "***individualized***" driving restrictions, such as individualized restrictions limiting "maximum speed,"

“geographic region” and “routes,” “maximum accumulated” mileage and time, and “time intervals” when the vehicle can be driven. (*Id.*, 6:8-17, 17:14-29; *see also* 15:66-16:11, 17:14-29, 6:55-7:14, Fig. 2, 8:29-53, Fig. 3, 10:45-11, Abstract, Claims 3, 10.) That is, in addition to allowing driving restrictions to be imposed on different categories of drivers, Murphy allows additional driving restrictions to be imposed on each individual driver. For example, driver John Doe may be limited to driving at a maximum speed of 50 mph and driving from 9 am – 5 pm, whereas driver Jane Doe may be limited to driving at a maximum speed of 65 mph and driving from 8 am – 8 pm.

51. Murphy’s driving restrictions for each driver, whether they are “individualized” for the specific driver or are based on the category or classification of the driver (or both), are an “operating profile,” because they specify how the driver can operate the vehicle based on the restrictions. Murphy discloses that the “operating profiles” for different drivers can be stored in a “database” or “memory” in its system that the controller can access. (*Id.*, Fig. 6, 13:35-41, 14:51-65, 15:55-16:11.) Similarly, Murphy teaches that the operating profiles can be stored in other components as well, such as in a “schedule module 211” which is separate from the controller and which provides the profile restrictions to the controller for use. (*Id.*, 15:8-31 (discussing schedule module storing “limitations on operation for each

authorized vehicle operator”), Fig. 7.) Notably, Murphy further discloses that “[f]or *each authorized driver* whose name or other identifying characteristics are contained in the database that is part of the controller module 209, *information in one or more of the following categories may be stored* in the database: (1) name or other identifier; (2) corresponding ident indicium or indicia; (3) schedule applicable to driver; (4) actual range of vehicle locations; (5) actual range of vehicle speed; (6) actual times of vehicle operation; (7) present ‘state’ of the vehicle (vehicle loaded/unloaded, type or vehicle load, passengers present, etc.); and (8) corresponding Control Actions applicable to various circumstances. This information *may be contained in the controller module 209 and/or the schedule module 211 and/or the vehicle activity log module 217.*” (*Id.*, 15:65-16:11.)

52. Moreover, Murphy’s system receives a “unique identification code” that allows a given driver to operate the vehicle using her “operating profile.” In the scenario of the TRAM and token, Murphy teaches its token can be “*specific to the person* who presents” it, has “built into it a *circuit or pre-programmed information* in a storage medium that imposes selected restrictions on operation of the vehicle and/or *that identifies the token holder,*” and may rely upon “digitized data” that is “*encoded* or encrypted” and stored in its memory. (*Id.*, 6:55-7:14; *see also* 2:33-34, 14:46-54, Cl. 38.) Thus, the token provides a “unique identification code,” which is

sent to the system and controller via the TRAM, in the form of “encoded” or “pre-programmed” “information” that is “specific to” and “identifies the token holder.” That the token can be used to authenticate and identify a driver likewise confirms this. For example, if the token did not provide a unique code to identify the driver, then the system could not use it to identify the “token holder” and distinguish her from other drivers.

53. Similarly, when the driver presents her “identification indicium” through Murphy’s data entry device and PIA, “information *that is specific to* and known to only *the individual* who presents the information” is used, which can include a “*coded sequence* of characters ...” (*Id.*, 7:15-28.) Thus, the token provides a “unique identification code,” which is sent to the system and controller via the data entry device (*e.g.*, keypad) and PIA, in the form of a “coded sequence of characters” that is “specific to and known to only” the driver. For example, the system could use the unique code “1029384756” to represent driver John Doe, such that when John Doe inputs this “coded sequence” into the keypad and it is provided to the system, he is identifying himself as the driver. Again, if the “coded sequence” did not provide a unique code to identify the driver, then the system could not use it to identify the driver distinguish her from others.

54. Similarly, Murphy discloses that the BIRAM can receive “*samples* of an *ident indicium*” unique to the driver, such as, among other things, “a handprint,” “a full facial scan,” and “a voice sample analysis.” (*Id.*, Abstract, Cl. 37; *see also* 2:20-45, 4:39-5:28, 6:46-54, 15:55-16:28, 16:50-17:2 (listing possible biometric sample types including fingerprint, thumbprint, handprint, retinal scan, blood vein pattern scan, and blood sample analysis), 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).) Thus, each such sample provides a “unique identification code,” which is sent to the system and controller via the BIRAM, in the form of digital representations of “biometric” information (*e.g.*, digital representations of handprints, full facial scans, and voice samples) that uniquely identify the driver. That the biometric samples can be used to authenticate and identify a driver likewise confirms this. For example, if the samples did not provide a unique code to identify the driver, then the system could not use it to identify the driver and distinguish her from others.

55. Furthermore, Murphy discloses that its system can include an “identifier module” that acts as an intermediary between, on the one hand, the BIRAM, TRAM and token, and data entry device and PIA and, on the other hand,

the system's control. (Murphy, 15:9-31, Fig. 7.) Murphy discloses that if such an identifier module is used, then after it receives "ident indicium" from the BIRAM, TRAM, and/or PIA, it can transmit to the controller module either the "ident information, *or a representation thereof*" for comparison to determine the driver's identity. (*Id.*) That the identifier module can provide a "representation" of the "ident indicium," instead of the "ident indicium" itself, is yet another "unique identification code" in Murphy.

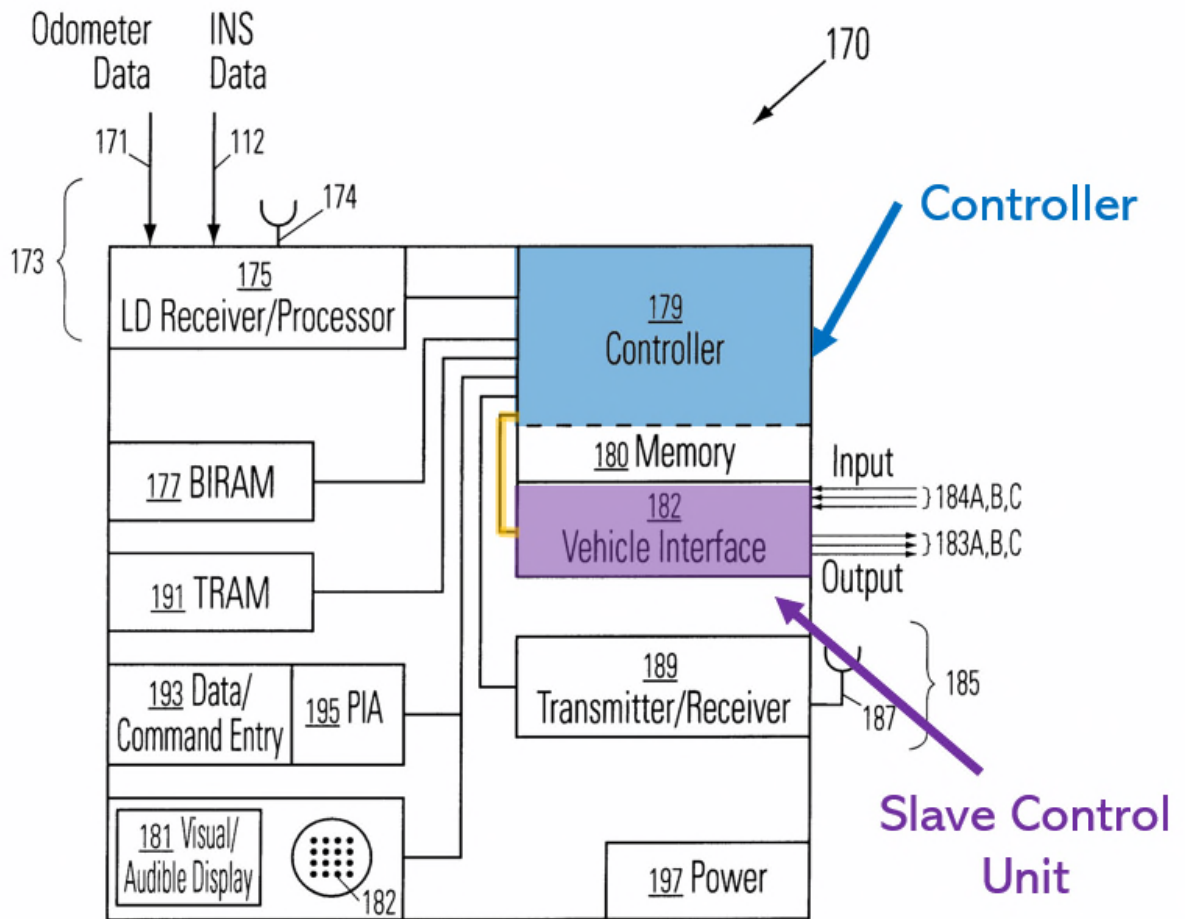
56. Murphy discloses that once the driver is authenticated using the "ident indicium," *see supra* Ground 1, Claim 1[A], Murphy's system accesses her corresponding profile to permit her to operate the vehicle in accordance with it. For example, Murphy discloses that when "[ident] indicum is satisfactorily presented and analyzed, the system allows operation of the vehicle" but will monitor "whether the vehicle location and/or speed are within *permitted ranges for the driver* and whether the present time and/or accumulated time or mileage are within *permitted ranges for the driver*." (Murphy, Abstract, 8:28-49, Fig. 2; *see also* 2:46-53, 5:13-28, 6:55-7:14, 7:49-8:14, 8:54-61, Fig. 3, 10:45-11:19.) In other words, Murphy is specifically disclosing that it is assessing what is specifically permitted for the particular driver that is driving the vehicle, *e.g.*, based on her operating profile.

57. Murphy further teaches that its controller can access the “*limitations* on vehicle operation *for each* authorized vehicle *operator*” and can use this and information it receives on the vehicle to “determine[] which Control Action(s), if any, should be imposed on” vehicle use. (*Id.*, 13:53-65, 14:46-65, 15:9-36; *see also* Figs. 6-7, 15:66-16:11, 17:14-29, 12:6-27.) The driver’s limitations on operation are stored in a database along with specific “Control Actions applicable to various circumstances.” (*Id.*, 15:66-16:11.) In other words, the operating profile indicates the appropriate Control Action to choose in response to specific violations. Such Control Actions can include “(temporarily) disabl[ing] the vehicle,” “(temporarily) disabl[ing] vehicle accessories,” and “reduc[ing] vehicle speed,” among other things. (*Id.*, 5:29-60, Abstract, Fig. 2.) If the controller determines the driver is not operating the vehicle within her “operating profile,” the controller will consult the Control Action rules, choose a Control Action, and command the vehicle (or control action) interface module to implement it by controlling “the vehicle engine, transmission, fuel supply, braking system, air bag system, vehicle accessory, or other appropriate system on the vehicle.” (*Id.*, Fig. 7, 15:32-54, Fig. 6, 13:54-14:17.) *See also infra* Ground 1, Claim 1[D].

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

58. Murphy discloses Claim 1[C].

59. Murphy discloses a “slave control unit” installed in its in-vehicle system in “communication” with the master control unit. Specifically, Murphy’s in-vehicle system includes a “vehicle [or Control Action] interface module 182” “connected to” “controller module 179”:



(Murphy, Fig. 6 (annotated); see also *id.*, 13:28-15:8, Fig. 7, 15:1-54, 16:12-16:49.)

The vehicle interface and controller modules are in “communication” with each other, including about “which Control Action(s), if any, should be imposed” and whether “vehicle components” have been “acivat[ed].” (*Id.*) See also *infra* Ground 1, Claim 1[D].

60. Additionally, the vehicle interface module, or slave control unit, is “coupled to” multiple “computers” associated with the vehicle. A “computer” is simply an electronic device or module for storing and/or processing data.

61. Specifically, the vehicle interface module is connected via its “interface [input/output] terminals” to computers such as the “vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories.” (*Id.*, Fig. 6, 13:53-14:17.) Murphy discloses that the “vehicle interface [module] 182 and associated information bus may, if desired, be provided according to the serial data communications standards between *microcomputers* in a vehicle, as set forth in S.A.E. Documents J1708 and J1587.” (*Id.*, 14:13-17.) Murphy’s vehicle interface module (“slave control unit”) would thus itself have a microcomputer and would communicate instructions to these components and their “*microcomputers*” to “control[] or restrict[] operation of the vehicle,” such as “reduc[ing] the vehicle speed to a selected speed range.” (*Id.*, Fig. 6, 13:53-14:17, Fig. 7, 15:32-54, 16:12-49.) The term “microcomputer” as referenced in Murphy is simply a small (*i.e.*, micro) *computer* which would include, among other things, a processor and memory and store and process data. Indeed, Murphy refers to J1708, which is a standard promulgated by the Society of Automotive Engineers that is used for both serial data communications between microcomputer systems in heavy duty vehicle applications and passenger car applications. The microcomputers (or microcomputer systems) in cars are often referred to as electronic control units or ECUs. ECUs include a microprocessor, memory, inputs and outputs, communication links, and embedded

software. Cars will have many different ECUs to control different systems. Such ECUs will include, for example, an engine control module (ECM) to control subsystems in the engine and a transmission control module (TCM). Thus, as Murphy's vehicle components (*e.g.*, vehicle engine, vehicle transmission system) include microcomputers (or ECUs), each is a "computer."

62. The vehicle interface module is also coupled to a "telecommunication module 185" in the in-vehicle system (via the controller module) and a "remote facility" (via the telecommunication module)—additional computers that are "associated with the motor vehicle." (Murphy, 14:23-45, Fig. 6, 16:12-49.) In operation, the "remote facility" can "transmit signals that modify, add or delete vehicle operation restrictions" to the "telecommunication module." (*Id.*) Murphy notes that discussions of "transmitting" and "receiving," such as transmitting by the remote facility and receiving by the telecommunication module, "refer to actions and processes of a *computer system or* other similar electronic *computing device.*" (*Id.*, 16:12-49.) In other words, because the remote facility and telecommunication module transmit and receive data, Murphy teaches that the remote facility and telecommunication module are "computer systems" or "similar electronic computing devices," *i.e.*, computers.

63. The "alter[ed] restrictions" received from the remote facility are then

used by the in-vehicle system, including the vehicle interface module, to control driver operation of the vehicle. (*Id.*; see also Abstract, 12:16-27, Fig. 1, 16:50-17:63, 4:15-27, Cls. 7, 9, 12, 15, 18.) *See also infra* Ground 1, Claims 2-3. Moreover, the vehicle interface module is further “coupled to” a “visual and/or audible display [or feedback] module”—another “computer”—that provides information to the driver about vehicle operation. (Murphy, Fig. 6, 13:61-14:17, Fig. 7, 15:47-50, 16:12-50, 5:55-60, 12:6-15, 10:29-40.)

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

64. Murphy renders obvious Claim 1[D].

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

- (1)...disabl[ing] the vehicle at a selected time so that the vehicle no longer

operates... (2)...disabl[ing] use of selected vehicle accessories... (3)...reduc[ing] the vehicle speed to a selected speed range... (4)...forc[ing] the vehicle to operate only in selected lower gears... (5)...turn[ing] on at least one of the lights, exterior flashers and horn continuously or periodically... (6)...activat[ing] an on-board alarm the is visually or audibly perceptible to a person outside the vehicle... (7)...transmit[ing] an alarm (optionally silent) to a selected facility that is spaced apart from the vehicle... (8)...activat[ing] an air bag or other disabling device on the driver's side of the vehicle... (9)...allow[ing] the vehicle to operate for at most a selected cumulative time interval... (10)... allow[ing] the vehicle to operate only within one or more selected time intervals... (11)...allow[ing] the vehicle to operate for at most a selected cumulative vehicle mileage... and (12)...tak[ing] no action at that time but optionally log[g]ing the activity and allow[ing] the driver to operate the vehicle without restriction for a selected time interval.

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

66. Murphy discloses that its controller “*determines* which Control Action(s), if any, should be imposed on vehicle use and communicates this information to a Control Action [or vehicle] interface module 215 *for implementation* by the vehicle engine, transmission, fuel supply, braking system, air

bag system, vehicle accessory or other appropriate system on the vehicle.” (*Id.*, 15:36-54; *see also* 13:66-14:17, Figs. 6-7.) Murphy further depicts that its system uses a feedback loop, in which vehicle location, speed, and time are monitored and the controller compares this data to determine whether operating restrictions are being violated. (*Id.*, Cl. 1, Abstract, 2:20-53, Fig. 2, 7:49-9:44, Fig. 3, 10:45-11:27.) If they are being violated, then the system can take a control action. (*Id.*) And if they are not being violated, then the system loops back to determine the latest vehicle location, speed, and time and to compare these against the operating restrictions. (*Id.*)

67. When Murphy’s vehicle interface module receives a command from the controller to implement a Control Action, it will cooperate with the vehicle components that are connected to its “terminals” and that are to be controlled, such as by communicating with such components and their “microcomputers” to “control[] or restrict[]” their operation. (*Id.*, 13:66-14:17, Fig. 6, 15:9-54, Fig. 7; *see also* Cl. 1. Abstract, 2:20-53, Fig. 2, 7:49-9:44, Fig. 3, 10:45-11:27.)

68. For example, if Murphy’s system determines “present vehicle location and/or speed” is not within a “permitted travel region and speed range corresponding to a permitted time interval” for the driver, then the controller module can use this and the “corresponding Control Actions applicable to various circumstances” for the

driver to determine what control action to take. (*Id.*, 5:12-60, 15:55-16:11; *see also* 16:50-17:63, Cl. 10.) If the controller determines that the “corresponding Control Action” for such a situation is to “reduce[] the vehicle speed to a selected speed range, using a vehicle ‘governor’ or some other suitable approach,” then it will send such a command to the vehicle interface module, which in turn will cooperate with the appropriate “vehicle component[s]” to reduce the vehicle’s speed accordingly. (*Id.*; *see also* 13:66-14:17, 15:9-54, Figs. 6-7.)

69. Furthermore, Murphy’s vehicle interface module (*e.g.*, slave control unit) can cooperate with other computers, such as a “telecommunication module,” and “information processing facility,” to control vehicle operation based on commands from the controller module (*e.g.*, master control unit). For example, when the system determines a violation occurs, the telecommunication module transmits a selected “alarm signal” to the remote computer, which, in turn, can send commands back to the telecommunication module, “such as to modify or add to the extant parameters for vehicle operation....” (*Id.*, 5:13-60, Claim 1, 14:23-45; *see also id.*, Abstract, 17:30-63.) The vehicle interface module will cooperate with the controller, telecommunication module, and remote computer (at the facility) to control the vehicle, such as by implementing any modified or new driving restrictions that were received by the telecommunication module from the remote computer and that the

controller now commands it to take. (*Id.*, 14:23-45; *see also* Murphy, Claims 7, 9, 12, 15, 18, Abstract, 12:16-27, 4:15-27.) *See also infra* Ground 1, Claims 2-3. For example, the driver's profile could initially be set up such that the driver such that the "speed limit" or threshold for the driver is 65 mph, but the corresponding "Control Action" is to simply to issue an alarm signal to the remote facility. If the driver has been speeding multiple times and the remote facility has been alerted of these violations, authorized personnel at the remote facility could decide to add a new restriction that says to control the vehicle if it exceeds 55 mph. This command would be downloaded by telecommunication module, passed along to the controller module, and then implemented by the vehicle interface module.

70. Murphy's vehicle interface module also cooperates with the "visual and/or audible display [or feedback] module" (*e.g.*, computer) to control vehicle operation based on commands from the controller, including when the controller commands the display (or feedback) module to alert the driver that she is violating her profile and, if the driver fails to take corrective action, the vehicle interface module disables the vehicle.

71. Thus, the vehicle interface module, or slave control unit, is coupled to the controller, which is coupled to the telecommunication module (a computer). The telecommunication module and vehicle interface module cooperate to control

vehicle operations when the telecommunication module receives modified driving restrictions from the remote facility and those restrictions are implemented by the vehicle interface module. Vehicle operations are controlled based on commands received from the master control unit because restrictions from the remote facility are passed from the telecommunication module to the controller and then to the vehicle interface module (when the controller commands it to implement restrictions).

72. Furthermore, regarding being “configured to monitor” vehicle operation and “generate” a signal if the driver violates her operating profile, thereby providing “feedback” about vehicle usage, Murphy’s controller (e.g., master control unit) is configured to monitor “[i]nformation on the present vehicle location and/or vehicle speed and/or time and/or accumulated operating time and/or accumulated mileage” and “compar[e] this... with any vehicle operation restrictions that may be imposed on an identified or unidentified vehicle operator.” (Id., 13:53-61; see also 13:28-43, 14:18-22, Figs. 6-7, 15:9-16:11, 16:50-17:63, Cls. 1, 10, Abstract, 1:66-2:6, 2:20-53, Fig. 2, 7:49-9:44, Fig. 3, 10:45-11:27.)

73. Further, Murphy’s controller can generate “signals” to other system components to provide feedback about vehicle usage. (Murphy, 5:29-60, 12:1-15, 13:61-65, Fig. 6, 15:42-54, Fig. 7, 10:29-40.) For example, the controller sends

signals to a “display [or *feedback*] *module*,” and “operations [vehicle activity] *log*” *module* when the driver has violated (or will violate) her profile, and these modules can provide feedback. For example, the vehicle activity log module is connected to the controller and used by it to record feedback on “vehicle location and speed,” including when a violation occurs, for “subsequent review and analysis if desired.” (Murphy, 5:53-54, 12:1-5, 15:42-54, Fig. 7.) *See also infra* Murphy, Claim 11[C]. Similarly, the feedback module can “announc[e] or visually display[] an announcement that a violation has occurred...” or will occur. (Murphy, 5:29-60, 13:61-65, Fig. 6, 15:47-50, Fig. 7; *see also* 12:6-15 (discussing display providing feedback), 10:29-40 (same).)

74. It would have been obvious to a POSITA to modify Murphy to configure the vehicle interface module (instead of the controller module) to “monitor” for violations of driver restrictions and generate a “signal” to the controller module if it determines such a violation occurs, thereby providing feedback. That is, it would have been obvious to a POSITA that the same functionality implemented in Murphy’s controller module could be implemented in its vehicle interface module. Both the vehicle interface module and the controller module are computing devices which send and receive and process signals, such as data and commands, and have similar components. Again, Murphy teaches that

“discussions that utilize terms such as ‘receiving,’ ‘transmitting,’ ‘measuring,’ ‘estimating,’ ‘computing,’ ‘performing’ and ‘determining’ and the like refer to actions and processes of a computer system or other similar electronic computing device.” (*Id.*, 16:12-49.) Because the vehicle interface module and the controller module both perform functions such as receiving and transmitting, Murphy teaches that they are similar “computer systems” or “electronic computing devices” and have basic components like a processor and memory. Reinforcing this, Murphy describes that the controller includes a “specially programmed computer,” and thus would have a processor and memory to store, among other things, software and the like. (*Id.*, 14:18-22.) Similarly, Murphy describes the vehicle interface module as including a microcomputer, and as I discussed such a microcomputer in a car (*e.g.*, ECU) would include a processor and memory. (*Id.*, 13:66-14:17.) Given this, it would not require additional hardware to have the vehicle interface module perform a function instead of the controller module. It would be simple substitution of one existing component (*e.g.*, controller module) for another (*e.g.*, vehicle interface module) to perform the same functionality. This substitution would have had predictable results, as a POSITA would have expected the result would be the same regardless of the component used: the system would determine whether the driver has violated her profile.

75. Moreover, Murphy suggests the modification, as its vehicle interface module already monitors vehicle usage and provides feedback to the controller module based on this. For example, the vehicle interface module uses its “input terminals” to monitor operation of “components (doors, ignition, alarm system, vehicle cargo, accessories, etc.) whose activation may indicate that someone is preparing to drive the vehicle, which would activate a driver interrogation sequence.” (Murphy, 14:7-17, Fig. 6; see also Abstract, Fig. 3, 7:49-63.) If it determines such components have been activated, then it will provide this feedback to the controller, so that it can “activate a driver interrogation sequence.”

76. Moreover, Murphy discloses that the “various limitations on vehicle operation for each authorized vehicle operator” can be stored in different modules. Thus, a POSITA would have understood from these suggestions that the vehicle interface module could similarly store or access such limitations and use them to monitor whether a violation has occurred and provide such feedback to the controller module.

77. A POSITA would have also been motivated to modify Murphy to configure the vehicle interface module to itself determine whether the driver has violated her profile and provide this information (e.g., signals) to the controller module. The vehicle interface module is already connected via its “terminals” to

certain vehicle components, “such as vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories..., for use in controlling or restricting operation of the vehicle.” (Murphy, 13:66-14:11.) Thus, by having the vehicle interface module determine, for example, whether the driver is operating the vehicle at a speed that violates her profile, it can simply use the information it already has—rather than providing such information to the controller module for it to make the determination. This would reduce the amount of information being provided to the controller module, as the vehicle interface module could provide information (e.g., signals) about violations to the controller module only when it determines a violation has occurred or will occur.

**b) Independent Claim 11**

78. As viewed by a POSITA, Murphy renders obvious independent Claim 11.

**(i) Claim 11[pre]: *A driver authentication and monitoring system, comprising:***

79. Claim 11[pre] is identical to Claim 1[pre], as both recite “[a] driver authentication and monitoring system, comprising...” Murphy thus 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[pre]. *See supra* Ground 1, Claim 1[pre].

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

80. Murphy discloses Claim 11[A].

81. The first half of Claim 11[A] is largely identical to Claim 1[A], as both recite “a master control unit ... for authenticating at least one driver via [a] driver identification [interface].” Murphy thus discloses a “master control unit” for “authenticating at least one driver via [a] driver identification [interface]” for the same reasons I discussed above for Claim 1[A]. *See supra* Ground 1, Claim 1[A].

82. For example, Murphy’s in-vehicle system includes (1) the BIRAM, (2) TRAM and token, and (3) data entry module and PIA, each of which interact with the driver and can be used by the system to authenticate or identify the driver with the information received. *Id.* I note that Claim 11[A] also expressly recites that the “master control unit” is in a “motor vehicle.” While I already explained for Claim 1[A] that Murphy’s “master control unit” is included in a vehicle like a car, in any event Murphy is clear that its system is used in a motor vehicle. Indeed, Murphy illustrates its system being used in a car and discloses that the system can be used in “land vehicle[s], such as an automobile, a truck or a bus.” (Murphy, Fig. 1, 15:1-8, 19:3-12.)

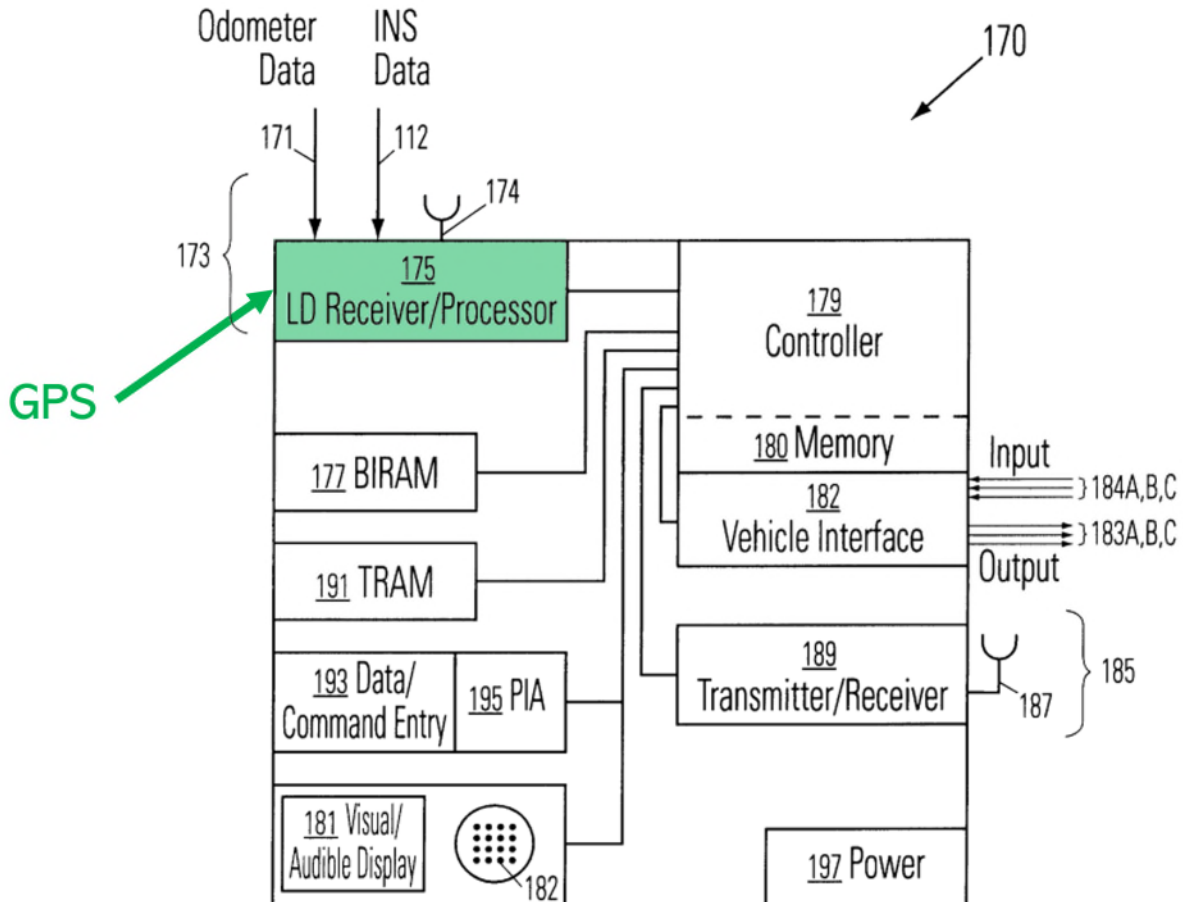
83. Additionally, the second half of Claim 11[A] is likewise reflected in Claim 1[B], which similarly recites “an operating profile associated with the at least one driver.” Murphy’s master control unit thus “associate[s]” an “operating profile with at the least one driver” for the same reasons I discussed earlier for Claim 1[B]. *See supra* Ground 1, Claim 1[B]. For example, drivers can be assigned their own profiles, such as assigned to “categories” (like restricted or non-restricted operators) with particular driving restrictions, as well as given “*individualized*” driving restrictions, like “maximum speed,” “geographic region” and “routes,” “maximum accumulated” mileage and time, and “time intervals” when the vehicle can be driven, and when a driver authenticates or identifies herself, the controller (master control unit) will operate in accordance with her assigned profile. *Id.*

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

84. Murphy discloses Claim 11[B].

85. Murphy discloses that a “location determination (LD) module” that is “part of an LD system, *such as GPS*, GLONASS, LEO, Iridium or LORAN, including an LD signal antenna [] and an LD signal receiver/processor connected to the antenna [], is located on the vehicle [].” (Murphy, 3:48-64.) Murphy further discloses “the LD module [] *determines* the *present location, present speed...* and observation time... of the antenna [], and thus *of the vehicle* [], in a manner well

known in the art.” (*Id.*) Murphy’s LD module can be integrated into its system, and “[i]nformation on... vehicle location and/or... speed and/or... time and/or accumulated operating time and/or... mileage is sent by the LD module 173 to the controller module 179” for use. (*Id.*, Fig. 6 (annotated below), 13:28-65; *see also* Abstract, Fig. 2, 7:49-9:44, 14:23-45, Fig. 7, 15:32-54, 3:64-4:38, Fig. 5, 13:11-26, Claims 1, 10.) One can also see from Figure 6 below that the LD module 175 (*e.g.*, GPS module) is connected and in communication with the controller 179:



(*Id.*, Fig. 6 (annotated), 13:28-65; *see also* Abstract, 14:23-45, Fig. 7, 15:32-54, 3:64-4:38, Fig. 5, 13:11-26, Cls. 1, 10, Fig. 2, 7:49-9:44.) Murphy’s information on vehicle location and/or speed and/or time provided by the LD module thus includes “location and speed information in association with movement of” the vehicle. That is, the location and speed information are determined by the GPS as the vehicle moves. (*See also id.*, Fig. 2 (showing feedback loop that system repeatedly determines vehicle location and speed to assess whether each location and speed as vehicle travels are within permitted ranges), 7:49-9:44, Claim 10 (reciting “when said *vehicle is in motion*, determining the present speed of said vehicle”).

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

86. Murphy discloses Claim 11[C].

87. Murphy’s system can include an “*operations log*” or “*vehicle activity log module*” that includes “*periodic recording of the present observation time, vehicle location and/or vehicle speed in a memory ...*” (Murphy, 12:1-5, 15:42-54, Fig. 7; *see also id.*, Fig. 6, 13:53-15:65, 14:18-22.) The operations or vehicle activity log thus records both vehicle “location” and “speed” information from the LD (or GPS) module. It also allows the vehicle location and speed from the LD module to be stored for “subsequent review and analysis if desired” (including when the driver

violates her profile). (*Id.*, 5:52-54, 15:42-54, Fig. 7; *see also* 15:66-16:11.) Additionally, the controller module can use a “data transfer module” to allow the information logged in the operations or vehicle activity log “to be copied from or removed from the system for subsequent analysis or storage.” (*Id.*)

88. Murphy discloses that the same speed and location data stored in the “vehicle activity log” may also, or alternatively, be recorded in “the controller module 209 and/or the schedule module 211....” (*Id.*, 15:66-16:11.) The controller module 209 and schedule module 211 are thus further examples of “data logging device[s]” which record location and speed data from the LD module (GPS) of Murphy.

89. Moreover, Murphy discloses that “vehicle location and selected status parameters” from the LD module can be stored in a remote “base station” for use in determining whether to take “control actions” remotely. (*Id.*, 4:15-27, 1:66-2:24, 16:30-49.) As discussed, status parameters from the LD (or GPS) module in Murphy include vehicle location and speed. Thus, the “base station” is another example of the claimed “data logging device,” as it is a remote computer that is part of Murphy’s “system” that can record vehicle operation (including location and speed) from Murphy’s LD (or GPS) module.

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

90. Claim 11[D], like Claim 1[C], generally recites (a) a slave control unit installed in the vehicle and coupled to at least one “computer,” and (b) the slave control unit being in communication with the master control unit. Murphy thus discloses Claim 11[D] for the same reasons as I discussed above for Claim 1[C]. *See supra* Ground 1, Claim 1[C].

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

91. Claim 11[E], like Claim 1[D], generally recites (a) the slave control being configured to “monitor operation” of the vehicle and generate a signal to the master control unit if the driver violates her “operating profile,” thereby providing feedback to the master control unit, and (b) the slave control unit cooperating with the “computer” to “control” vehicle operation based on the master control unit’s commands. Murphy thus renders obvious Claim 11[E] for the same reasons as I

discussed above for Claim 1[D]. *See supra* Ground 1, Claim 1[D].

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

92. Murphy discloses Claim 11[F].

93. Claim 11[F] is substantially similar to Claim 1[B], which likewise recites that the master control unit “receives a unique identification code” that “permit[s] the at least one driver to operate the vehicle within an operating profile.” Murphy thus discloses Claim 11[F] for the same reasons I discussed above for Claim 1[B]. *See supra* Ground 1, Claim 1[B].

94. In addition, after a driver is authenticated, Murphy’s controller (master control unit) allows her to use the vehicle within her profile, so long as she does not violate the restrictions therein. *Id.* For example, if the driver violates her operating profile, or is “found to be unauthorized,” the system can “(temporarily) disable[] the vehicle... so that the vehicle no longer operates, through fuel cutoff, brake disablement or some other similar measure.” (Murphy, 5:17-67, 10:41-44; *see also* Abstract, 10:29-40.) *See also supra* Ground 1, Claim 1[C] (discussing system taking

“Control Actions” to control vehicle operation where driver fails to adhere to her operating profile).

**c) Independent Claim 15**

95. As viewed by a POSITA, Murphy anticipates and renders obvious Claim 15.

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

96. Claim 15[pre] is similar to Claim 1[pre], as both recite “authentica[ing] and monitoring” a “driver” (“A driver authentication and monitoring system”/“A method of authenticating and monitoring drivers”). Claim 15[pre] thus covers the same concept as Claim 1[pre], but rephrases it in method form. Murphy therefore 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[pre]. *See supra* Ground 1, Claim 1[pre].

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

97. Claim 15[A] is also similar to Claim 1[pre], merely instructing to “provid[e] a motor vehicle with” the driver authentication and monitoring system. As I discussed above with respect to Claim 1, the driver authentication and monitoring system is provided in a motor vehicle. *See supra* Murphy, Claim 1[pre]-

1[A]. Murphy thus discloses a driver authentication and monitoring system in a motor vehicle.

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

98. Murphy discloses Claim 15[B].

99. Murphy's system includes operating profiles associated with high-risk drivers, including restricted operators. *See supra* Murphy, Claim 1[B]. For example, it can "monitor operation of the vehicle by a teenager or other inexperienced driver, with restrictions imposed upon vehicle operation channel, total vehicle mileage, vehicle maximum speed and/or time interval of operation of the vehicle." (Murphy, 11:60-67; *see also* 1:9-27, 1:66-2:16, 3:21-47, 16:49-17:62.)

100. In Murphy, these profiles can be "programmed" into the system. (*Id.*, 15:66-16:11; *see also* Fig. 7, 5:52-54, Fig. 6, 13:35-41, 14:51-54, 14:62-65.) The profiles can be programmed into the system by: (1) an "authorized system administrator" who "modif[ies]" the "operating restriction tables" using a data entry device (*id.*, 7:40-48, 12:16-27, 13:44-52, Fig. 6); (2) presentation of a "token" with "pre-programmed information" on "restrictions" (*id.*, 6:55-7:14, 2:33-34, 14:46-54, Cl. 38); and (3) receipt of a "reprogramming signal" that "commands" the system to "modify, add, or delete vehicle operation restrictions" (*id.* 14:23-45, Abstract, 2:6-9). *See infra* Ground 1, Claims 2-3. For example, the system can store: "(1) name or

other identifier; (2) corresponding ident indicium or indicia; (3) schedule applicable to driver; (4) actual range of vehicle locations; (5) actual range of vehicle speed; (6) actual times of vehicle operation; (7) present “state” of the vehicle (vehicle loaded/unloaded, type or vehicle load, passengers present, etc.); and (8) corresponding Control Actions applicable to various circumstances.” (*Id.*, 15:66-16:11.) *See also supra* Murphy, Claim 11[C]. Such data may also be stored in “the controller module 209 and/or the schedule module 211 and/or the vehicle activity log module 217.” (Murphy, 15:55-16:11.)

101. Murphy discloses several ways in which operating profiles can be programmed into its system. First, Murphy discusses an “authorized system administrator” can “modif[y]” the “operating restriction tables” using a “keypad or other data entry device,” such as a local device in the vehicle. (Murphy, 7:40-48, 12:16-27, 13:44-52, Fig. 6.) Second, Murphy discloses that a driver can present a “token,” such as a “smart card,” with “pre-programmed information” on the driver’s “restrictions.” (*Id.*, 6:55-7:14, 2:33-34, 14:46-54, Cl. 38.) The “token” transmits this operating profile to the in-vehicle “TRAM,” which “communicate[s]” it to the “controller 179 for implementation.” (*Id.*, 14:46-54.)

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

102. Murphy discloses and renders obvious Claim 15[C].

103. Claim 15[C] discloses similar elements to Claims 1[A] and 1[B] above, but is rephrased as a method step. As I discussed above, Murphy discloses authenticating high-risk drivers to enable their operation of a motor vehicle within their respective operating profiles. *See supra* Ground 1, Claim 1[A]-1[B]; *see also* Ground 1, Claim 15[B]. By “high profile drivers,” the ’427 refers to drivers who are “high-risk” and thus have operating “profile” restrictions. (*See* Response to Non-Final Office Action of November 15, 2018 (U.S. App. No. 15/898,322, later U.S. Patent No. 10,259,465) (in a nearly identical claim, changing “high profile” to “high risk” in response to an antecedent basis rejection).) In other words, “high profile” drivers are those who pose a greater risk than a typical driver, and thus have a need for a strict operating profile. (*See* ’427, Abstract, 1:63-2:5 (discussing high risk drivers).)

104. Further, Murphy discloses “monitoring” vehicle operation to determine if the driver violates her profile. Murphy also renders obvious “monitoring” vehicle operation to determine if the driver violates her profile. *See* Ground 1, Claim 1[D]. For example, Murphy’s controller will monitor “[i]nformation on the present vehicle

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

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

105. Murphy discloses Claim 15[D].

106. Murphy generates multiple “signals” if the high profile driver violates her operating profile. Murphy also renders obvious generating a “signal” if the driver violates her operating profile. *See* Ground 1, Claim 1[D]. For example, if the controller determines the driver has violated her profile, it will then determine which “Control Action(s), if any, should be imposed on vehicle use and communicates this information” to the “interface module” for “implementation” via an “appropriate system on the vehicle.” (*Id.*, 15:36-54; *see also* 13:66-14:17, Figs. 6-7, 16:12-49.) This process involves generating multiple signals: a signal from the controller to the interface module commanding it to implement a Control Action, another signal from the interface module to the vehicle system to cause the system to take a specific

action, and (potentially) the vehicle system's action is itself a signal (such as an alarm signal, or slowing of the vehicle, which signals to the driver that a violation occurred).

107. In addition, "Control Action(s)" can include generating alarm signals, such as "an on-board alarm" signal and a "coded alarm signal" transmitted "to a selected facility that is spaced apart from the vehicle." (Murphy, 5:13-54, Abstract; *see also* 17:30-63.) *See also infra*, Murphy, Claim 15[E]. If there is a violation the controller can also send signals to a "display [or feedback] module" and the "operations [or vehicle activity] log," causing the display module to "announc[e] or visually display[] an announcement that a violation has occurred..." and the operations log to record that a violation has occurred. (*Id.*, 5:29-60, 12:1-15, 15:42-54, Fig. 7, 13:61-65, Fig. 6, 10:29-40.)

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

108. Murphy discloses Claim 15[E].

109. Murphy's system includes "an antenna 187 and associated receiver/transmitter [] that exchanges information signals with an information processing facility." (Murphy, 14:23-45.) If the driver violates her "operating profile," Murphy's system can "transmit[] an alarm (optionally silent) to a selected facility that is *spaced apart from the vehicle*" via the transmitter. (*Id.*, 5:13-54; *see*

*also* 17:30-63, 6:1-18.) The remote facility can, in turn, send “commands” back to the in-vehicle system to “alter restrictions” of the driver’s profile. (*Id.*, 14:23-45, Cl. 1; *see also* Abstract, 2:6-9, 12:16-27, 17:30-63.) The system will then cooperate with the remote facility to govern the vehicle operation, such as by using any new or modified driving restrictions received from the facility to control the driver’s usage of the vehicle. (*Id.*, 14:23-45; *see also* Cls. 7, 9, 12, 15, 18, Abstract, 12:16-27, 4:15-27.) *See also infra* Ground 1, Claims 2-3. For example, if there are any newer or modified driving restrictions from the remote facility, they may result in one of the Control Actions being taking at the vehicle, which affects mechanical operations of the vehicle.

110. For example, Jane Doe’s operating profile might specify that if she exceeds 65 mph, an audible in-vehicle alarm should sound. If Jane Doe violates her operating profile, Murphy’s system will sound the in-vehicle alarm, and also use the transmitter to notify the remote facility. If the remote facility receives notice of repeated violations, a stricter enforcement measure may be warranted. For example, the remote facility could then alter the restrictions of Jane’s profile, specifying that the vehicle should be automatically slowed down if she exceeds 65 mph. The in-vehicle system would receive the alterations to the profile via the transmitter and implement the new commands to govern mechanical operations of the vehicle and

slow it down. In this manner, Murphy's system governs mechanical operations remotely, using the remote facility, in response to violations of the operating profile.

- d) **Dependent Claim 2:** *The driver authentication and monitoring system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.*

111. Murphy renders obvious Claim 2.

112. Murphy's system includes a "database comprising a program module," such as a "*database*" with "various limitations on vehicle operation" (e.g., operating parameters), including on "geographic regions, corridors or routes where the vehicle may be driven, ...permitted time intervals during which the vehicle may be operated, ...permitted speed ranges for operation of the vehicle, and ...limitations on vehicle transmission ranges permitted for operation of the vehicle." (Murphy, 15:9-31, 6:55-7:15.) Murphy further discloses that "[f]or each authorized driver whose name or other identifying characteristics are contained in the database..., information in... the following categories may be stored...: (1) name or other identifier; (2) corresponding ident indicium ...; (3) schedule applicable to driver; (4) actual range of vehicle locations; (5) actual range of vehicle speed; (6) actual times of vehicle

operation; (7) present ‘state’ of the vehicle ...; and (8) corresponding Control Actions applicable to various circumstances.” (*Id.*, 15:66-16:11; *see also* 5:12-6:17). *See also supra* Ground 1, Claim 1[C].

113. Murphy teaches that its “database” can be stored in the memory of its in-vehicle system, such as in the memory of its controller module or another module. (Murphy, 16:9-11; *see also* Fig. 6, 13:35-41, 14:51-54, 14:62-65, Fig. 7, 15:55-15:65.) These limitations on vehicle operation stored in Murphy’s database are “operating parameters” because they are related to how a driver is permitted to operate the vehicle. Moreover, they are a “program module” because they are “components” or “data structures” in the database and, for example, can be used to perform tasks such as control operation of the vehicle.<sup>3</sup>

114. In addition, Murphy’s database can be “programmed” remotely by an “authorized monitoring agency or person.” (*Id.*, 2:6-9; *see also* 7:40-48.) Specifically, Murphy teaches that “[t]he present invention allows downloading from a *remote facility to modify or add* to the extant *parameters* for vehicle operation or

---

<sup>3</sup> The ’427 broadly describes “program modules” as including “routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types.” (’427, 4:55-58.)

for vehicle driver identification, where the parameters are *included in the operating code, stored data* and the like.” (*Id.*, 14:40-45.)

115. Murphy’s in-vehicle system facilitates such remote access through a “telecommunication module 185 (optional) ... including an antenna 187 and associated receiver/transmitter 189 that exchanges information signals with an information processing facility... that is spaced apart” from the system. (*Id.*, 14:23-27, Fig. 6.) Murphy discloses that using “[s]uitable telecommunication systems,” including “cellular phone, trunked radio, unlicensed radio band, packet radios in LAN or MAN or WAN operation and the like” (*e.g.*, networks), the remote facility can transmit “change or *reprogramming signal[s]*” that “modify, add or delete vehicle operation restrictions, for receipt by the apparatus [], and that allow downloading of commands that alter restrictions on present location, speed and/or present time, accumulated operating time and accumulated mileage items that determine the conditions under which a vehicle operation restriction is imposed.” (*Id.*, 14:27-40, Abstract; *see also id.*, 12:16-27, Fig. 1, 16:12-50, 16:50-17:63, 4:15-27, Claims 7, 9, 12, 15, 18.)

116. Thus, Murphy discloses that its system includes a remote computer or base station that can be used by authorized users to remotely program, via a network, drivers’ operating profiles in the in-vehicle system’s database. As a further example,

the authorized user in Murphy can use the remote computer to “transmit[] a change signal from [the] monitoring station to [the] vehicle that modifies [its] permitted speed range,” thereby modifying this operating parameter in the driver’s profile in the in-vehicle database, such that if at any time thereafter the “present vehicle speed” is not within the new “permitted speed range,” the in-vehicle system will “tak[e] at least one Control Action to control use of said vehicle. (*Id.*, Claims 12, 10.) *See also supra* Ground 1, Claim 15[B].

- e) **Dependent Claim 3: *The driver authentication and monitoring system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the master control unit for the at least one driver.***

117. Murphy renders obvious Claim 3.

118. Murphy’s in-vehicle system allows for “*downloading from a remote facility* to modify or add to the extant *parameters for vehicle operation* or for vehicle *driver identification*, where the parameters are included in operating code, stored data and the like.” (Murphy, 14:23-45; *see also* Fig. 6, 2:6-9; 7:40-48, Abstract, 12:16-27, Fig. 1, 16:12-50, 16:50-17:63, 4:15-27, Claims 7, 9, 12, 15, 18.) That is, Murphy’s remote computer can modify or add both the parameters used in the vehicle for driver identification *and* the parameters used to restrict or control a driver’s operation of the vehicle. As such, Murphy’s “driver identification

interfaces” (e.g., BIRAM, TRAM and token, and data entry device and PIA) work with its “remote computer” (e.g., the remote facility) in multiple different ways to “load” a driver’s operating profile into the system for the controller.

119. *First*, Murphy’s “remote facility” or computer can transmit new “parameters for... *driver identification*” to the in-vehicle system, which the driver can use in conjunction with Murphy’s driver identification interface to authenticate and identify herself and “load” her operating profile in the controller. (*Id.*, 13:28-15:8, Fig. 6; *see also* Abstract, Fig. 7, 15:8-54, Fig. 2, 7:40-8:53, 4:39-5:12, 6:55-7:14.) For example, if Murphy’s system “downloads” from the remote computer a new “biometric indicium,” like a new “facial image” of a particular driver for use with the BIRAM, then that driver can use this new parameter from the remote computer to authenticate herself to operate the vehicle. That is, if the driver presents her facial image to the BIRAM in the vehicle and it matches the new facial image received from the remote computer, then the driver will be authenticated and permitted to operate the vehicle according to her corresponding profile that was loaded into the controller.

120. Similarly, Murphy’s in-vehicle system could download a new “coded sequence of characters” from the remote computer for use with the data entry module, such as code “1029384756” known and unique to driver John Doe. The

driver (*e.g.*, John Doe) can then use this new coded sequence to authenticate himself using the data entry module and PIA and operate the vehicle according to his corresponding profile loaded in the system. *See also supra* Murphy, Claim 1[A] (discussing driver providing “ident indicium” via driver identification interfaces to authenticate herself).

121. Murphy teaches that the profiles are loaded into its “controller” (*e.g.*, the master control unit) once the driver is authenticated. (Murphy, 13:35-41, 14:51-54, 14:62-65, Fig. 6, 15:15-21, Fig. 7, 15:66-16:11; *see also* 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.) For example, as I explained above with respect to the independent claims, Murphy’s operating profiles can be stored in a “database,” located in the “controller module 209,” the “schedule module 211,” and/or the “vehicle activity log module 217.” (*Id.*, 15:66-16:11, 15:21-31.) When a driver is authenticated, the controller loads her operating profile so it can monitor for violations of the profile. The operating profile may be loaded from the schedule module into the controller, or from the vehicle activity log into the controller, or can become activated (load)<sup>4</sup> within the controller itself. It is important to point out that

---

<sup>4</sup> For example, the operating profile may load from the memory of the controller into the processor of the controller, or from one memory location into another memory location within the controller (such as from RAM to cache).

the in-vehicle system contains profiles for *all* authorized drivers, and thus of course will have to load and use the correct one out of the myriad available.

122. Thereby, the in-vehicle system's driver identification interfaces (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA) work in conjunction with Murphy's remote computer to load the "operating profile" of the driver into the master control unit, because these new "driver identification" parameters can be downloaded from the remote computer and used by a driver to authenticate herself in the vehicle, allowing her to operate the vehicle in accordance with her corresponding profile loaded in the controller. *See also supra* Ground 1, Claim 1[B] (discussing system allowing driver to operate vehicle in accordance with profile loaded based on identity of driver).

123. *Second*, the "remote facility" can "*transmit signals* that modify, add or delete vehicle operation restrictions, for receipt by the [in-vehicle system], and that allow downloading of commands *that alter restrictions* on present location, speed and/or present time, accumulated operating time and accumulated mileage items *that determine the conditions under which a vehicle operation restriction is imposed.*" (Murphy, 14:27-37.) After being "download[ed]" to Murphy's system, the "alter[ed] restrictions" would be stored in the operating profiles of the drivers whose restrictions are being altered. (*Id.*, 15:66-16:11, Fig. 6, 13:28-15:8, Fig. 7, 15:9-65,

16:50-17:62.) For example, if the remote computer transmits a signal to reprogram the speed at which John Doe is permitted to operate the vehicle from 75 mph to 60 mph, then such modified restriction would be stored in John Doe's corresponding profile in the system. Similarly, if the remote computer transmits a signal to add a new restriction for Jane Doe that she is not permitted to operate the vehicle from 12 am to 6 am, then such new restriction would be stored in Jane Doe's corresponding profile in the system. *See also supra* Ground 1, Claim 1[B] (discussing system storing different operating profiles for different drivers).

124. In conjunction with this, when a driver whose restrictions were altered or modified authenticates herself using a "driver identification interface" (e.g., BIRAM, TRAM and token, and data entry device and PIA), the master control unit (e.g., controller) will use the "operating profile" with the "alter[ed] restrictions" or "modified or additional parameters" that were "download[ed]" from the "remote facility" (e.g., remote computer). (Murphy, 15:66-16:11, Fig. 6, 13:28-15:8, Fig. 7, 15:9-65, 16:50-17:62.) To take the John and Jane Doe examples given above again, the system will use John Doe's "operating profile" with the modified 60 mph speed limit that was loaded into it, and will similarly use Jane Doe's "operating profile" with the new 12 am – 6 am restriction that was loaded into it, such that if either John or Jane violates her respective restrictions when operating the vehicle, the system

will take corresponding “control actions.” As such, in this additional way, the system’s driver identification interfaces work in conjunction with the remote computer to load the driver’s “operating profile” to the controller module.

125. Similarly, if the driver uses a driver identification interface to authenticate herself, and in conjunction with this, the system *later* downloads from the “remote facility” additional restrictions that are applicable to the driver, then the system will load the restrictions into the “operating profile” of the driver, such that her use of the vehicle thereafter is restricted according to her original profile *as altered by the new restrictions* loaded into the system. For example, there may be scenarios when a driver has already been authenticated (*e.g.*, as John or Jane Doe) and is using the vehicle, but then the remote computer subsequently transmits a change signal to change her operating profile while she is driving. In such a situation, Murphy’s in-vehicle system will load these updated parameters (*e.g.*, updated profile), such that these new parameters or restrictions will thereafter be used—instead of, for example, earlier restrictions that may have now been modified. For example, in the John Doe scenario discussed above, if John Doe is authenticated and is initially permitted to operate the vehicle at 75 mph according to his profile, but the remote computer later modifies this restriction to 60 mph, then the in-vehicle system will load this modified parameter into the operating profile in the system,

such that it (and not the prior 75 mph restriction) is used to determine whether to take any control actions when John Doe is operating the vehicle.

126. It is also worth noting that “operating profiles” can additionally be loaded *from the token* into the in-vehicle system. For example, Murphy discloses that the token (*e.g.*, smart card) can be specific to the token holder and can contain “pre-programmed information in a storage medium that imposes selection restriction on operation of the vehicle.” (*Id.*, 6:55-7:14, 14:46-54, Claim 38.) *See also supra* Ground 1, Claims 1[A]-1[B] (discussing token and TRAM). Thus, if the in-vehicle system has downloaded modified or additional restrictions for the driver from the remote computer (whether before or after the driver is authenticated or identified using the token), then the system will load these modified or additional restrictions into the operating profile for the driver that was received into the system from the token. In this way, too, the system’s driver identification interfaces (*e.g.*, the TRAM and token) work in conjunction with the remote computer to load the “operating profile” of the driver.

**f) Dependent Claim 4: *The driver authentication and monitoring system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.***

127. Murphy renders obvious Claim 4. Claim 4 recites three things: (a) a GPS module; (b) a memory module; and (c) a function indicator module.

128. First, with respect to the “GPS module,” this same limitation is in Claim 11[B]. Thus, Murphy discloses that its system includes a “GPS module” for the same reasons that I discussed above for Claim 11[B]. *See supra* Murphy, Claim 11[B].

129. Second, with respect to “memory module,” Murphy discloses that its system includes numerous memories. For example, Murphy’s in-vehicle system includes “controller 179 and *associated memory module 180.*” (Murphy, 13:35-41, Fig. 6; *see also* 15:15-21 (discussing same controller with memory), Fig. 7 (depicting same).) Similarly, Murphy discloses that this memory and its system include a “*database* of authorized vehicle operators.” (*Id.*, 15:15-21, 13:35-41, 14:51-54, 14:62-65; *see also* 15:66-16:11, 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.)

130. Murphy further discloses that the system can include a “schedule module 211” that “*contains* various limitations on vehicle operation and each authorized operator...” (*Id.*, 15:21-31, Fig. 7.) Thus, the “schedule module” would additionally include memory that “contains” such limitations. Indeed, Murphy states that its “database” (*e.g.*, memory) of “authorized vehicle operators” can be included in the schedule module (in addition to in the controller or the operations or vehicle activity log). (*Id.*, 15:66-16:11.)

131. Moreover, Murphy adds that its system can include other memories as well, such as in its token (for use with TRAM) and in its operations log. (*Id.*, 6:55-7:14, 12:1-5; *see also* 16:30-49.) For example, with respect to the former, Murphy discloses that the token used in its TRAM can have “built into it a circuit or pre-programmed information in a *storage medium*” and rely upon “digitized data” that is “encoded or encrypted” and stored in its memory. (*Id.*, 6:55-7:14; *see also* 2:33-34, 14:46-54, Cl. 38.) *See also supra* Murphy, Claim 1[B]. And with respect to the latter, Murphy expressly states that the “operations log” (or “vehicle activity log module”) can include, for example, “*a memory* that cannot be modified and that cannot be read out without presentation of a confidentially maintained access code.” (Murphy, 12:1:5, 15:42-54, Fig. 7.) *See also supra* Claim 11[C].

132. Murphy also discloses that its in-vehicle system includes numerous “function indicator modules.” The specification of the ’427 broadly describes “function indicator module” as a module that can “monitor various functions in association with the vehicle... such [] for example, power, fault detection and monitoring, and other functions.” (’427, 8:11-14.) Moreover, the ’427 broadly describes the term “module” as a “physical hardware component and/or a software module.” (*Id.*, 6:4-17.)

133. For example, Murphy's system, such as its controller module, can monitor the functioning of the "location determination (LD) module" (or GPS module). (Murphy, 13:11-26, Fig. 5; *see also* 3:64-4:14, Fig. 6, 13:28-52.) In particular, Murphy discloses that the system "determines if sufficient LD signals of acceptable quality are being received so that the vehicle location can be determined," and, if they are not, it can "take one or more of the 12 Control Actions" I discussed earlier. (*Id.*, 13:11-26, Fig. 5; *see also* 3:64-4:14, Fig. 6, 13:28-52.) The system can also include an "inertial navigation system [INS] device... or similar *location indicating device*" that can monitor whether "LD [*e.g.* GPS] information is lost or corrupted," and, if it is, can use its own "INS information" to "estimate the present location and/or speed and/or accumulated mileage." (*Id.*, 4:28-38, 13:28-52.) Thus, the controller and INS device are "function indicator modules" because they can monitor the sufficiency of the LD signals and determine whether the LD information is lost or corrupted, or, in other words, include hardware and/or software that can monitor the functioning of the GPS module.

134. As an additional example, Murphy's system can include an "interface module" with "one or more interface input terminals" for monitoring the functioning of certain "components (doors, ignition, alarm system, vehicle cargo, accessories, etc.) whose activation may *indicate* that someone is preparing to drive the vehicle."

(Murphy, 13:66-14:17, Fig. 6.) In Figure 6, Murphy refers to this as the “vehicle interface module.” (*Id.*) In Figure 7, Murphy refers to this as the “Control Action interface module 215.” (*Id.*, 15:37-54, Fig. 7.) If the vehicle (or Control Action) interface module receives an indication that any such component is being used, such as the ignition being turned on, the door being opened, the tailgate being powered to open, or the like, then it can “activate a driver interrogation sequence” requesting the driver to provide identification information. (*Id.*, 13:66-14:17, 15:37-54, Figs. 6-7; *see also* Abstract, 13:28-15:8, Fig. 2, 7:49-63.) Thus, the vehicle (or Control Action) interface includes a “function indicator module” because it can monitor powering or other functioning of vehicle components.

135. As yet another example, Murphy’s system can further include a “display system” which can be used to monitor how the vehicle has been functioning and indicate to the driver that “a violation has occurred and/or that the vehicle will become disabled” after a period of time if no corrective action is taken. (*Id.*, 10:29-40, 5:29-60.) For example, Murphy discloses that “[a]s the number of consecutive hours of vehicle operation approaches the specified limit” that the vehicle can be driven without a rest, “the driver can be advised, using a visually perceptible and/or audibly perceptible presentation device, that this specified limit is being approached” and “the vehicle can be disabled (or some other suitable penalty

imposed) when this specified limit is exceeded.” (*Id.*, 10:29-40; *see also id.*, 12:6-15, Fig. 6, 13:61-65, Fig. 7, 15:47-50.) Thus, the “display system” is a “function indicator module” because it can monitor vehicle operation restrictions, and, for example, indicate if a limit is being approached or is exceeded.

136. Murphy includes several further examples of “function indicator modules.” For example, its system can include (1) “a vehicle odometer... or similar *distance indicating device*” that monitors the distance the vehicle has traveled and can use this to supplement LD module or GPS information (*id.*, 13:44-48); (2) a BIRAM that can monitor how many times it has been used with “biometric indicium” that is not “legible/interrogatable” and take a “control action” after a “sequence of N consecutive” failed attempts (*id.*, 5:13-16, 6:19-39); and (3) a “governor” that can monitor “vehicle speed” to “reduce[] the vehicle speed to a selected speed range” (*id.*, 5:29-60, 6:8-17, 17:30-63).

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

137. Murphy renders obvious Claim 5.

138. As I discussed for Claim 1[B], Murphy discloses that different vehicle drivers can have different “operating profiles” loaded in the in-vehicle system’s “database” and/or “memory.” *See supra* Murphy, Claim 1[B]. Murphy specifically

teaches that this memory that the operating profiles are loaded into can be the “memory” of its “controller” (*e.g.*, the memory module). (Murphy, 13:35-41, 14:51-54, 14:62-65, Fig. 6, 15:15-21, Fig. 7, 15:66-16:11; *see also id.* 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.) Murphy’s “operating profiles” can also be loaded into the system from the token. (*Id.*, 6:55-7:14, 14:46-54, Abstract, 2:33-35, Claim 20.)

139. After a driver authenticates herself using the system, her corresponding profile loaded in the memory is used to control operation of the vehicle within the loaded operating profile. *See supra* Ground 1, Claim 1[B]. One can readily see this with reference to Figure 2, for example, in which Murphy discloses there being a loop in which “vehicle present location and velocity and present time” are repeatedly determined and, after each determination, the system confirms, among other things, if such “vehicle location, speed, present time accum. time and/or accum. mileage” are within the driver’s “permitted ranges” loaded in the system’s memory. (Murphy, Fig. 2, 7:49-9:44.) If they are within the permitted ranges for the driver as stored in the memory, then the loop will repeat, and if they are not, then a control action may be taken. (*Id.*)

140. Additionally, Murphy discloses that its system can also include a “schedule module 211” (*e.g.*, including memory) that contains the “various

limitations on vehicle operation for each authorized vehicle operator.” *See supra* Murphy, Claim 4 (discussing schedule module). Murphy discloses that this information, along with “ident information” of the “authorized drivers,” can be loaded into the “controller” (with its “memory unit”) to enable it to authenticate the driver and “determine[] which Control Action(s), if any, should be imposed on vehicle use.” (Murphy, 15:9-54, Fig. 7; *see also* 16:30-49.) For example, if John Doe is driving the vehicle, then the “operating profile” of John Doe will be loaded into the controller’s memory from the schedule module, so that the controller can use the operating restrictions in his profile to determine whether he is operating the vehicle within his “permitted ranges” and, if not, what control actions should be taken.

**h) Dependent Claim 6: *The driver authentication and monitoring system of claim 4, wherein the GPS module provides location information to at least the master control unit in association with a physical location of the vehicle.***

141. Murphy renders obvious claim 6.

142. Claim 6 is similar to Claim 11[B], which likewise recites a “GPS module” that provides to the system “at least location... in association with movement of said motor vehicle.” Thus, Murphy discloses Claim 6 for the same reasons that I discussed above for Claim 11[B]. *See supra* Ground 1, Claim 11[B]. I also note that, as I explained in Claim 11[B], the GPS location information is

provided by the LD (or GPS) module “to the controller module 179” so the controller can determine whether to take control actions. *Id.*

- i) **Dependent Claims 8/13: *The driver authentication and monitoring system of claim [2/11], wherein [the/the 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.***

143. Murphy renders obvious Claims 8 and 13.

144. Murphy’s operating profiles include parameters for at least “maximum allowable vehicle speed,” “allowable vehicle location,” and “allowable hours of operation.” By way of example, Murphy discloses that its operating profiles can include “*parameters for vehicle operation*” and that these parameters can include, without limitation, (a) “restriction to a selected maximum speed” (*i.e.*, maximum allowable vehicle speed), (b) “restriction to a selected geographic region” and “restriction to one or more specific routes,” *i.e.*, allowable vehicle locations, and (c) “restriction of vehicle operation to one or more selected time intervals during the day, or to selected days of the week,” *i.e.*, allowable hours of operation. (Murphy, 17:14-28, 14:40-45; *see also* Abstract, 5:12-54, 11:60-67, 2:46-53, 6:8-17, Fig. 2, 8:5-67, 12:16-35, 15:66-16:11.) For example, a driver John Doe can have an operating profile including operating parameters such as: a maximum allowable speed limit of 65 mph; a specific allowable vehicle location between New York and

Boston (including via a specific route, such as via Route I-95); and allowable operating hours from 9 am to 11:30 am and from 12:30 pm to 4:30 pm. *See also supra* Ground 1, Claim 1[B].

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

145. Murphy renders obvious Claims 9 and 14.

146. As I discussed in Claim 1[C], Murphy’s system monitors whether a driver is operating the vehicle in accordance with her operating profile, and, if she violate the profile, the system can take numerous “Control Actions,” including generating “alarm signals.” *See supra* Ground 1, Claim 1[D].

147. For example, Murphy discloses that if the system determines the “present time” of operating the vehicle is not within the driver’s “permitted time intervals,” or the “vehicle present location and/or speed” is not within the driver’s “permitted travel region or speed range,” the system can issue several different alarm signals to authorized users and others. (Murphy, 5:13-60, Cl. 1; *see also* Abstract, 17:30-63, Cl. 20, 2:6-9, 4:15-27, 12:8-12, Fig. 6, 13:60-65, 14:23-45, Fig. 7, 15:37-50, 16:11-49.) First, it can “***audibly announce[] or visually display[]*** an announcement that a ***violation has occurred...***” (*Id.*) This alarm signal would alert the driver, as well as others within the vehicle (including those who may be

authorized users of the system), that the driver has violated her operating profile. Second, the system can “*transmit[] a selected alarm signal to a selected facility* that is spaced apart from the vehicle.” (*Id.*) This alarm signal would alert the authorized person at the remote facility that the driver has violated her operating profile. And third, the system can “activate[] an on-board alarm the [sic] is visually or audibly perceptible *to a person outside the vehicle.*” (*Id.*) This would alert others that the driver has violated her operating profile.

148. Instead of the controller module generating the “alarm signals,”<sup>5</sup> it would be obvious to a POSITA for the vehicle interface module (*e.g.*, “slave control unit”) to generate the signals, as I discuss above at Claims 1[C]-1[D]. Since, the vehicle interface module would itself determine whether a violation of the operating profile occurred, a POSITA would understand that the vehicle interface module would subsequently generate an alarm. For example, the vehicle interface module would signal the controller that a violation had occurred, and the controller would generate an audible or visual announcement or alarm to the driver, and/or transmit the alarm signal to the remote facility. This would be a simple substitution of one

---

<sup>5</sup> The '427 broadly describes the “alarm signal” as a signal that “*can result* in an actual audible alarm, or it can be used to control/govern operational aspects of the vehicle.” ('427, 7:19-27.)

component (the vehicle interface module) for another (the controller module) to perform the same function (determining that a violation has occurred and causing an alarm). A POSITA would have a reasonable expectation of success in modifying Murphy in this manner.

149. Murphy's vehicle interface module already monitors vehicle operation and provides alerts based on this (e.g., if certain components are activated it can cause the system to alert the driver with a "driver interrogation sequence"), and a POSITA would have understood from this suggestion that the vehicle interface module could generate additional alerts based on the detection of certain conditions, e.g., if the driver violates her profile. Given that the vehicle interface module monitors vehicle operation, it would be obvious to try to have the vehicle interface determine occurrence of a violation and generate the alert signal.

**k) Dependent Claim 10: *The driver authentication and monitoring system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.***

150. Murphy renders obvious Claim 10.

151. Murphy discloses that its driver identification interfaces can include a "token or *smart card* (referred to collectively as a 'token')" for use with the TRAM. *See supra* Murphy, Claim 1[A]. The token may be "specific for the *person* who *presents* the token," have "*built into it a circuit* or pre-programmed information in

a storage medium that imposes selected restrictions on operation of the vehicle and/or that identifies the token holder,” and rely “upon digitized data stored in a flash *memory*, in a (re)programmable ROM or in similar information storage media.” (Murphy, 6:55-7:14; *see also id.*, 2:33-34, 14:46-65, Claim 38.) Murphy further teaches that the TRAM in the vehicle can receive “*insertion or presentation*” of the token. (*Id.*)

152. When Murphy’s token is a smart card with circuitry and memory that can be held and inserted into or presented at the TRAM, it is a “portable handheld device.” Smart cards are small devices, often the size of a credit card or the like, that can be held in the hand of a user. As Murphy discloses, they are devices that can contain circuitry and memory and are adapted for a particular purpose—namely, in the case of Murphy, storing and providing a data used for identification or authentication, as well as for storing and providing operating restrictions. Because they are portable and can be carried by a driver, and have circuitry and memory providing certain functionalities, the token is a portable handheld device.

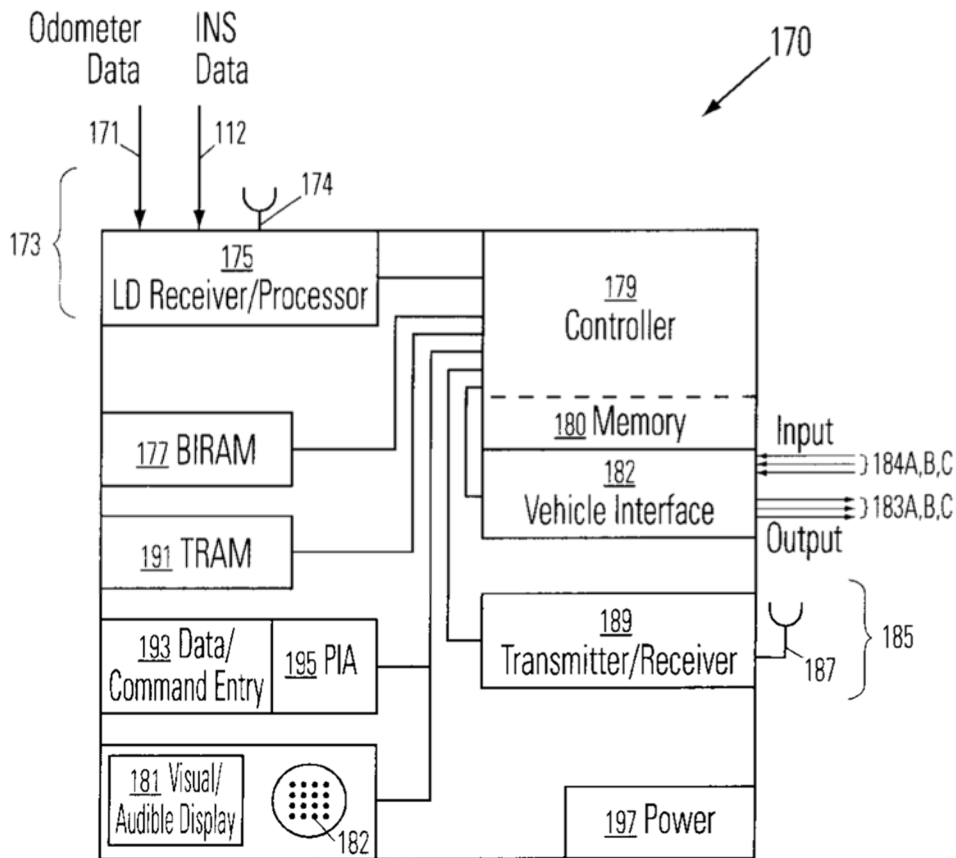
153. Further, as Murphy expressly discloses, its smart card can be “insert[ed] *or presented.*” (Murphy, 6:55-7:14; *see also id.*, 2:33-34, 14:46-65, Claim 38.) When the token is a smart card with circuitry and memory that can be presented to the TRAM, it is a “radio frequency identification (RFID) device.” It was well known in

the art at the time of the alleged invention that such contactless smart cards that were presented (as opposed to inserted) and thus were contactless communicated with a reader (like the TRAM) wirelessly via RFID. A POSITA would have thus understood that Murphy's disclosure that its smart card can be "presented" means that the token uses RFID technology. Moreover, the use of RFID with Murphy's smart card certainly would have been obvious as well. Again, RFID was a well-known method by which smart cards could be used to transmit or provide data for authenticating or identifying a person, without the user having to physically insert the card. Murphy specifically states that its smart card can be "presented" (as opposed to "inserted"), and a POSITA would have known that one such way that the smart card could be presented is via RFID.<sup>6</sup> Further, the use of RFID in the smart card would have obviated the need for the card to be inserted, making it faster and simpler for the driver to identify herself.

---

<sup>6</sup> RFID smart cards has been used and well-known in the industry as of 1998. *See, e.g.,* <https://scispace.com/pdf/applications-and-opportunities-for-radio-frequency-45ehip8oar.pdf> (Moscow subway system using RFID smartcards in 1998), <https://pcac.org/app/uploads/2014/09/In-your-Pocket-Smart-Cards.pdf> (Washington D.C. metro system implementing RFID smartcards in 1998); Adams, [0022], [0027]).

154. In addition, Murphy discloses that its *entire* in-vehicle system, including the driver identification interfaces, can be a “portable handheld device.” Specifically, Murphy teaches that “apparatus 170” shown below—which includes the “driver identification interfaces” (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA)—can be “installed in the vehicle dashboard or elsewhere in the vehicle” or “[a]lternatively... provided as a *stand-alone device* that communicates directly” with vehicle accessories. (Murphy, 15:1-8.) Claim 10 does not mean that only the “driver identification interface” can be portable; other aspects of the system can be portable as well. Thus, in the situation where Murphy’s in-vehicle system (*e.g.*, apparatus 170) is provided as a “stand-alone device,” the apparatus and, by extension, the driver identification interfaces would all be part of a “portable handheld device.” In other words, a person would be able to transport and carry the apparatus, including the circuitry therein, using her hands.



(Id., Fig. 6.)

- 1) **Dependent Claim 16:** *The method of authenticating and monitoring drivers in claim 15, wherein the motor vehicle includes a GPS module and the monitoring operation of the motor vehicle further comprises obtaining GPS data including motor vehicle speed and location.*

155. Murphy anticipates and renders obvious Claim 16.

156. Claim 16 is similar to Claim 11[B], which recites a “GPS module” which provides “location and speed information in association with movement of the motor vehicle.” As I discussed above at Claim 11[B], in Murphy, the motor

vehicle includes a “location determination” or “LD” module, which is a GPS that provides data on the speed and location of the motor vehicle. This speed and location data is used to monitor operation of the vehicle. *See supra* Ground 1, Claim 11[B].

**m) Dependent Claims 17/18: *The method of authenticating and monitoring drivers in claim [15/16], wherein the step of generating a signal includes providing [an audible alarm to the driver and a signal remotely/an alarm remotely] to an authorized user.***

157. Murphy anticipates and renders obvious Claims 17 and 18.

158. As I explained above with respect to claims 1[C], 15[D], 9, and 14, Murphy discloses both an audible alarm signal to a driver and a remote alarm signal to an authorized user. (Murphy, 5:13-60, Cl. 1; *see also* Abstract, 17:30-63, Cl. 20, 2:6-9, 4:15-27, 12:8-12, Fig. 6, 13:60-65, 14:23-45, Fig. 7, 15:37-50, 16:11-49.) For example, Murphy discloses a “display [or feedback] module” which can generate alerts in the vehicle to warn an authorized driver, as well as others in the vehicle (*e.g.*, other authorized drivers who may be present, like parents). (*Id.*, 5:53-54, 12:1-5, 15:42-54, Fig. 7.) Murphy’s system can also send an alert to an authorized user at a “remote facility” using a “telecommunication module.” (*Id.*, 14:23-45, Fig. 6, 16:12-49.) *See supra* Ground 1, Claims 1[C], 15[D], 9, and 14.

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

159. Murphy anticipates and renders obvious Claims 19 and 20.

160. As I explained above with respect to Claim 15[D], Murphy's system can take a variety of "Control Action(s)" when a driver violates her operating profile. *See supra* Ground 1, Claim 15[D]; *see also supra* Ground 1, Claims 1[D], 9, and 14. As just one example, the "controller module" can generate a signal (*e.g.*, an alarm signal) to the vehicle interface module to alert it that the operating profile was violated and command it to take a control action. (Murphy, 15:36-54; *see also* 13:66-14:17, Figs. 6-7.) The vehicle interface module generates a control signal to limit vehicle functionality, such as by disabling the vehicle, disabling use of selected accessories, limiting the speed of the vehicle using a governor, or similar actions. (*Id.*, 5:13-54; *see also* 17:30-63, 6:1-18.)

**2. Ground 2: Murphy in view of Adams Renders Obvious Claim 10**

161. I have reviewed Adams which is U.S. Patent App. Pub. No. 2008/0046739. Adams was filed August 16, 2006, and published February 21, 2008, and I understand Adams is prior art under at least pre-AIA §102(e).

162. My review of the '427 Patent file history reveals that Adams was not considered during prosecution of the '427 Patent.

- a) **Dependent Claim 10: *The driver authentication and monitoring system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device, a radio frequency identification device; and a USB compatible device.***

163. Murphy in view of Adams renders obvious Claim 10.

164. Adams discloses a “smart card (SC)” and “smart card reader (SCR).” (Adams, [0001], [0022].) Similar to Murphy, Adams discloses that “smart cards” can be “contactless” and can “communicate with their smart card readers” wirelessly. (*Id.*, [0027].) Adams expressly discloses that such wireless communication can be using “*radio frequency identification (RFID).*” (*Id.*)

165. It would have been obvious to a POSITA to apply this teaching to Murphy to have its token use RFID and thus be a “radio frequency identification device” as recited in Claim 10. This would have been the simple combination of well-known prior art elements (RFID and contactless smart cards) according to known methods to yield predictable results. Indeed, both Murphy and Adams teach that smart cards were known in the art and can communicate with an interface (or smart card reader) wirelessly. (Adams, [0001], [0022]-[0030]; Murphy, 6:55-59, Abstract, 14:46-54.) Adams simply discloses that this wireless communication can be RFID. (Adams, [0027].) Applying this to Murphy, Murphy would operate in the

same fashion—for example, authenticating or identifying drivers as it did before—only now its token (or smart card) would use the well-known RFID protocol to communicate with the TRAM when “*present[ed]*” to the TRAM.

166. Furthermore, both references provide teachings that would have led a POSITA to the combination, as they disclose that smart cards are used for “authentication” and to control access and describe smart cards in a similar fashion (*e.g.*, as handheld devices with circuitry, memory, and security features). (Adams, [0001], [0023]; Murphy, 6:55-7:14, 2:33-34, 14:46-65, Claim 38.) A POSITA would have also been motivated to use RFID in Murphy’s token (or smart card), as taught by Adams, as such would have provided the token with a standardized, established protocol that could be easily implemented to effectively enable wireless communications between the token and TRAM and that would obviate the need for a driver to insert her token into the TRAM.

### **3. Ground 3: Murphy in View of Wu Renders Obvious Claims 7 and 12**

167. I have reviewed Wu which is U.S. Patent App. Pub. No. 2008/0114501. I understand that Wu was filed November 15, 2006, and published February 21, 2008, and I understand Wu is prior art under at least pre-AIA §102(a) and §102(e).

168. My review of the '427 Patent file history reveals that Wu was not considered during prosecution of the '427 Patent.

169. Wu discloses a remote start and vehicle control system that includes “a controller 20, a battery 40 ... an engine control module 60, ... a starter motor 80, a fuel pump 90, and an ignition circuit 100.” (Wu, [0020]-[0022], [0025]-[0027], Figs. 1-2.) Wu discloses that its controller, like that of Murphy, controls vehicle operations such as “starting” the vehicle and enabling or disabling the ignition. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039].) Wu further discloses controlling additional vehicle “accessories,” such as parking lights, air conditioners, heaters, and interior lights. (*Id.*, [0030], [0031].) Wu discloses that these control operations are performed by using a processor to send signals to “relays,” which then activate or disable the different vehicle systems and components. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.)

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

170. Murphy in view of Wu renders obvious Claims 7 and 12. Claims 7 and 12 merely add that the “slave control unit” includes certain well-known components—namely “a power regulator module; a starter relay module; a definable

relay module; a slave microcontroller; and an alarm synthesizer.” These are standard components that a POSITA would expect to be present in a motor vehicle. For example, it was well-known to include a “power regulator,” typically in the form of a voltage regulator, to provide the voltage level required for electronic components in the vehicle to function properly. These voltage regulators would, for example, regulate the voltage from a vehicle’s 12V battery or alternator to deliver a stable 5V supply to vehicle electronic components while protecting against voltage spikes. As another example, starter relays are standard electrical components that activate a starter motor, which in turn rotates a crank of the engine so that the engine itself can start. As a final example, an “alarm synthesizer” is simply a known component for electronically generating sounds. Additionally, the ’427 broadly describes that the “slave control unit” as a collection of disparate components broadly describes the “slave control unit” as a collection of components across the vehicle that are connected and respond to commands, such as from the “master control unit.” (’427, Fig. 6, Abstract, 8:15-55 (describing that the slave control unit can include a number of components).)

171. Murphy discloses, and it would have been obvious for its vehicle interface module to include, a “slave microcontroller.” For example, Murphy’s “vehicle interface module” is “connected to at least one vehicle component... for

use in controlling or restricting operation of the vehicle.” (Murphy, 13:53-14:17, Fig. 6, 15:32-54, Fig. 7.) When controlling these other components such as the “vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories,” the vehicle interface module will communicate instructions to them “according to serial data communications standards between *microcomputers in a vehicle*, as set forth in S.A.E. Documents J1708 and J1587.” (Murphy, 13:66-14:17.) Thus, and as I explained earlier, the vehicle interface module itself includes a “microcomputer” and further has “output terminals” connecting to the “microcomputers” of the components it controls. Because these “microcomputers” are part or connected to and take the actions instructed by the vehicle interface module, they are “slave microcontrollers.”

172. Murphy discloses, and it would have been obvious for its vehicle interface module to include, an “alarm synthesizer.” For example, Murphy’s system can include a “screen or monitor 181” and a “*loudspeaker* 182.” (Murphy, Fig. 6, 12:8-12, Fig. 7, 15:37-50.) When Murphy’s controller determines that a driver has violated or will soon violate an operating restriction in her profile, then it will use the display system (including the speaker) to synthesize, or electronically generate, an alarm. Murphy teaches that in this situation, the display system synthesizes an “audibly perceptible presentation to the driver,” such as “*audibl[e]*...

**announcement** that a violation has occurred and/or that the vehicle will become disabled...” (*Id.*, 15:47-50, 5:13-60; *see also* Claim 1, 17:30-63, 13:60-65.) *See supra* Ground 1, Claims 9/14. Moreover, a POSITA would have understood the “output terminals” of the vehicle interface module, which are used to control myriad components, could likewise be connected to the “alarm synthesizer,” because they can be connected to “different group of vehicle components.” (*Id.*, 13:66-14:17.) Likewise, Wu discloses that this same type of audible alert or announcement can be done with a synthesizer, including an “operational amplifier” and “resistor,” and a POSITA would have readily understood this to be a common and simple way to implement the audible alerts in Murphy for its intended purpose. (Wu, [0030].)

173. Murphy in view of Wu discloses, and it would have been obvious for its “slave control unit” to include a “power regulator module.” Murphy’s system includes a “power supply 197” that regulates power, as it “supplies power to operate one or more of the components of the apparatus 170” in the in-vehicle system. (Murphy, 13:66-14:4, 14:66-15:8.) Furthermore, Wu discloses it was “standard” to include a power (or voltage) regulating device in vehicle controllers, like Murphy’s, to “regulate the voltage level to 5V” or to voltage levels the system “requires.” (Wu, [0020], [0022], [0027]-[0028].) It would have been obvious to a POSITA to include a voltage regulator for the system in Murphy to perform its intended purpose, as

taught by Wu, including to ensure that the vehicle interface module receives the appropriate voltage that it “requires” to operate. (Wu, [0020], [0028])

174. Further, voltage fluctuations in vehicle systems may lead to erratic behavior or potential damage to electronic components if they were directly connected to, for example, the battery or alternator, and Wu’s disclosures teach that regulating power was a well-established practice in such systems. A POSITA would have understood this would merely require the use of a well-known, standard, component to perform its intended function. A POSITA would have been motivated to use a voltage regulator in order to ensure the voltage level required for the electronic controller in Murphy, and its associated modules, was delivered, such as 5V as is standard in automotive electronic components and systems. Again, a POSITA would have understood this to be simply the routine inclusion of a known, common vehicle component (a power or voltage regulator) for its intended purpose, and in fact would have expected Murphy’s in-vehicle systems to include such a standard component to apply the appropriate voltage to the controller and associated modules and to protect against voltage surges. (Wu, [0020], [0022], [0027]-[0028].)

175. Moreover, the vehicle interface module of Murphy is connected via its “output terminals” to a “vehicle power supply.” (Murphy, 5:29-60, *see also* 13:66-14:17, Fig. 6, 15:32-54, Fig. 7.) These “output terminals” also connect to various

vehicle components, which the vehicle interface controls, including vehicle accessories. (*Id.*) It would be obvious to include the “power regulator” within the vehicle interface module (“slave control unit”), because when the vehicle interface module controls components via its output terminals it must send them power at appropriate voltages. Given that Murphy discloses the power regulator is in its system, and that Wu further discloses to implement a power regulator for devices such as Murphy’s vehicle interface, it would be obvious to a POSITA to place the power regulator in the vehicle interface module. Such a modification would be applying well-known methods and would achieve a predictable result, namely, providing appropriate power supply to different components of the vehicle.

176. Murphy in view of Wu discloses, and it would have been obvious for its slave control unit to include, a “starter relay module.” Murphy’s system includes an “ignition circuit,” and if a driver is authenticated after inserting and presenting “ident indicium” and is in compliance with her operating profile, then the system can “enabl[e]” (*e.g.*, activate) this “ignition circuit,” which then allows the engine to be started. (Murphy, Abstract, 6:55-59, 8:10-14.) Additionally, Wu discloses that a “starter relay” is controlled by a processor 22 in a controller 20 to start the engine of a vehicle. (Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.) When the controller receives a command or notification to start the vehicle, its

processor can send a signal to initiate a starter relay which will engage a starter motor, which causes the engine to start. (*Id.*, [0025], [0027], [0031].) A POSITA would have been motivated to include such a “starter relay” as taught by Wu in Murphy’s system, because it would provide a well-known and commonly-used mechanism for starting the engine. A POSITA would have understood such a “starter relay” could be included in the vehicle interface module of Murphy as part of Murphy’s circuitry that allows the engine to be started. (*Id.*) For example, Murphy discloses that the vehicle interface module (*e.g.*, “slave control unit”) includes “terminals” which connect to the “ignition” of the vehicle. (*Id.*, 13:66-14:11.) And, a POSITA would have had a reasonable expectation of success in using such a starter relay within the vehicle interface module, as Wu discloses that this is a standard component that would be used for its well-known purpose of engaging a “starter motor” to start the vehicle. (Wu, [0025], [0027], [0031].) Thus, such a modification into the slave control unit could easily receive a response back if the driver is authenticated and enable the activation of the engine. This would have, in fact, been simply the routine implementation of a standard starter relay that a POSITA would expect to be used in any vehicle system at the time of the invention to start the engine.

177. Murphy in view of Wu discloses, and it would have been obvious for its slave control unit to include, a “definable relay module.” Murphy discloses the

vehicle (or control action) interface module includes “interface output terminals” connected to other vehicle components, and the vehicle interface module can use these to cause the activation of specific circuitry or functionality such as “turn[ing] on at least one of the lights, exterior flashers or horn” for defined periods of time. (Murphy, 5:29-60, *see also* 13:66-14:17, Fig. 6, 15:32-54, Fig. 7.) Similarly, the vehicle interface module includes “interface input terminals” that are connected to certain “vehicle components (doors, ignition, alarm system, vehicle cargo, accessories, etc.) whose activation may indicate that someone is preparing to drive the vehicle.” (*Id.*) If this occurs, then it can “activate” certain system components and functionalities, such triggering the display system to turn on and provide a “driver interrogation sequence” to the driver. (*Id.*) Furthermore, Wu discloses that components such as the ignition system, lights, and accessories can be controlled by a processor sending a signal to a “defined relay” for such components. (Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.) For example, Wu notes that the timing for different relays can be based on voltage “pulses.” (*Id.*) A POSITA would have been motivated to use such definable “relays” for these and other components in Murphy, as taught by Wu. A POSITA would have understood using such “relays” would have merely been the implementation of known components for their intended purpose and would have allowed the processor in Murphy’s slave

control unit to selectively activate and deactivate the ignition, lights, fuel injector, and other accessories. As an example, Wu discloses that using a fuel injection relay and an ignition relay allows the engine to be enabled and disabled when desired. (Wu, [0025], [0031], [0039].) A POSITA would have understood using such relays from Wu would be one way to achieve Murphy's enabling and disabling of the vehicle engine, and the activation and deactivation of vehicle accessories. (Wu, [0025], [0031], [0039]; Murphy, 5:13-54; *see also* 17:30-63, 6:1-18.)

#### **B. Grounds Based on Arshad**

178. I have reviewed Arshad which is US2003/0189482. I understand that Arshad was filed April 3, 2003, and published October 9, 2003. I understand that Arshad is prior art under at least pre-AIA §102(b).

179. My review of the '427 Patent file history reveals that Arshad was not considered during prosecution of the '427 Patent.

180. Arshad discloses a system for "authoriz[ing]" fleet vehicle drivers and monitoring vehicle operation. (Arshad, Abstract, [0028].) A driver's "transponder" communicates with an in-vehicle system to identify the driver and transmit "operational limits," such as "maximum speed," authorized "geographical area," and "number of hours of authorized use." (*Id.*, [0019], [0033], [0043], [0057].) If these

are violated, Arshad’s system can “limit the speed” or disable the vehicle, “display a message,” or sound an “audio alarm.” (*Id.*, [0043]-[0045], [0063].)

**1. Ground 4: Arshad Renders Obvious Claims 1, 4-6, and 10**

**a) Independent Claim 1**

181. As viewed by a POSITA, Arshad renders obvious independent Claim 1.

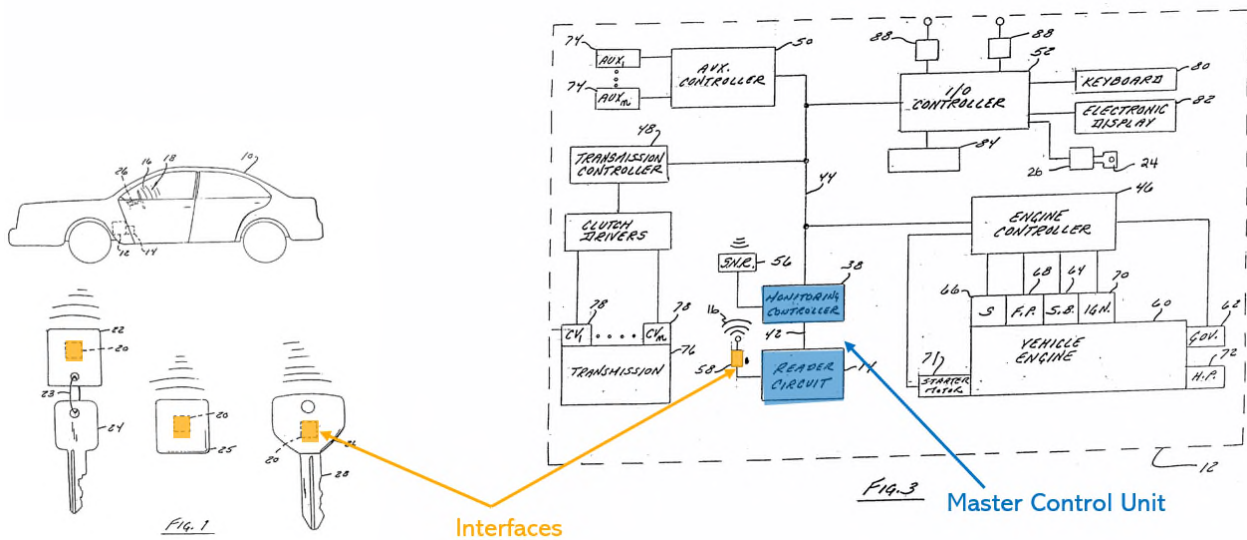
**(i) Claim 1[pre]: A driver authentication and monitoring system, comprising:**

182. Arshad discloses the preamble of Claim 1 to the extent the preamble limits the scope of the claim. Arshad’s system controls “access” to “[f]leet vehicles.” (Arshad, Abstract, [0005], [0008]-[0009]; *see also* Cl. 13, [0033] (referring to the “fleet management *system*”).) In Arshad, a driver’s “transponder 20” transmits data to an in-vehicle control system to “uniquely *identify* the person carrying the transponder.” (*Id.*, [0033], [0019], [0012], Cl. 7 (system is “mounted on the vehicle”).) After the driver is authenticated, a “*monitoring* controller 38” in the system monitors vehicle operation, “determines whether the operator is authorized” to take certain actions, and responds to unauthorized actions with “alert message[s]” or disablement of vehicle systems, among other things. (*Id.*, [0061], [0071]; *see also* [0028]-[0031], [0041]-[0045], [0072]-[0074].) *See also infra* Ground 4, Claims 1[A] *See infra* Ground 4, Claims 1[A].

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

183. Arshad discloses Claim 1[A].

184. Arshad’s system discloses a “master control unit” that comprises a “vehicle status and monitoring controller 38” coupled to a “reader circuit 14.” (Arshad, [0028]-[0029].) Controller 38 is “mounted on [a] vehicle” and coupled to other “microprocessor-based controllers,” and reader unit 14 is similarly in the vehicle. (*Id.*, [0019], [0028], [0010]-[0013].) Arshad discloses that controller 38 and reader circuit 14 operate to “authenticate” drivers via an interface comprising (i) “antenna 58” through which the reader circuit transmits and receives radio signals and (ii) “transponder 20” which is carried by the vehicle operator:



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

185. In order to authenticate drivers, Arshad’s controller 38 can issue “commands... to the control module” of reader circuit 14, including “to query for any transponder in range, and a specific query command to query for a specific transponder by its embedded identification number.” (*Id.*, [0031].) When a general query is issued, all nearby transponders will reply “with a response that includes their identification number.” (*Id.*, [0033].) Reader circuit 14 will then “single out and *identify* any transponder within range,” and the controller and reader circuit can then communicate with each transponder identified by sending “specific queries.” (*Id.*) For example, the controller may issue a specify query to cause “reader circuit 14 to generate and transmit radio signals through antenna 58 into the surrounding environment,” and any transponder close enough to be energized “internally checks to see if it has the identification number broadcast by antenna 58.” (*Id.*, [0032].) If a transponder has the broadcasted “identification number,” it “responds with an

affirmative message, and thereby establishes a communication session with controller 38.” (*Id.*)

186. Once “the reader circuit establishes the existence of a particular transponder or transponders” (*e.g.*, by authenticating through identification numbers), it communicates with the transponder in Arshad’s system to “download information” from the transponder’s memory “and thence to controller 38 for processing.” (*Id.*, [0033]-[0034].) *See infra* Ground 4, Claim 1[B].

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

187. Arshad discloses Claim 1[B].

188. Arshad discloses that different drivers have different associated operating profiles, as each driver may have a “*different* degree[] of vehicle access,” and may be authorized to use different “vehicle functions, operations, systems or sub-systems.” (*Id.*, [0008], [0020]; *see also* [0010]-[0012].) For example, a driver’s transponder may store “*operational limits*,” such as a “maximum speed,” “maximum load on the engine,” “total distance” of authorized travel, “geographical area in which the vehicle” can operate, “allowed times and dates of operation,” “total time” of allowed operation, or “subsystems” that the operator can use. (*Id.*, [0043],

[0057], [0026]; *see also* [0043]-[0044], [0074].) Arshad discloses that the operating profile, including the degrees of access and operational limits, can be “downloaded” from the transponder to controller 38 and that the controller 38 accesses the operating profile information from the transponder to determine, for example, whether a driver is “authorized” to use the vehicle or a vehicle subsystem, or is approaching or exceeding an operational limit. (*Id.*, [0031], [0034], [0043]-[0044], [0057], [0071]; *see also* [0011], [0019], [0040], [0059]-[0060], [0068], [0073]-[0074].)

189. Further, Arshad discloses that controller 38 and reader circuit 14 receive a unique identification code to permit the driver to operate the vehicle within these operational limits. For example, each transponder stores an “*identification number*” in its memory to “*uniquely identify*” the driver carrying the transponder which can be sent to reader circuit 14 and controller 38. (*Id.*, [0032]-[0034].) *See also supra* Ground 4, Claim 1[A]. For example, reader circuit 14 receives this unique identification code after controller 38 “commands” it to “query” for transponders, which then send “a response that includes their identification number.” (*Id.*, [0031]-[0033].)

190. After a driver is authenticated using the transponder identification number, *see supra* Ground 4, Claim 1[A], Arshad’s controller 38 accesses the profile of operational limits and permits operation of the vehicle within these limits.

Specifically, the controller 38 will not allow the vehicle to operate “until [it] has received the data stored in transponder 20 and determined whether the operator is authorized to operate specific vehicle systems.” (Arshad, [0040]; *see also* [0034].) Further, Arshad’s controller 38 “compares” data from other controllers and sensors with “data it received from the transponder” to determine whether the driver has “attempted to exceed any of the operational limits that were indicated by the transponder data.” (*Id.*, [0043]-[0045], [0040]-[0042], [0057]-[0063], [0071]-[0074].) If any of the operational limits are exceeded, controller 38 takes appropriate actions such as shutting down or limiting vehicle subsystems or displaying a message indicating what limit has been exceeded. (*Id.*) *See also supra* Ground 4, Claim 1[A].

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

191. Arshad discloses Claim 1[C].

192. Arshad discloses a “slave control unit” installed in the vehicle and in communication with the “master control unit.” For example, in Arshad, “engine controller 46” is one of several “microprocessor-based controllers” that is “coupled together with” monitoring controller 38 over “communication bus 44”:

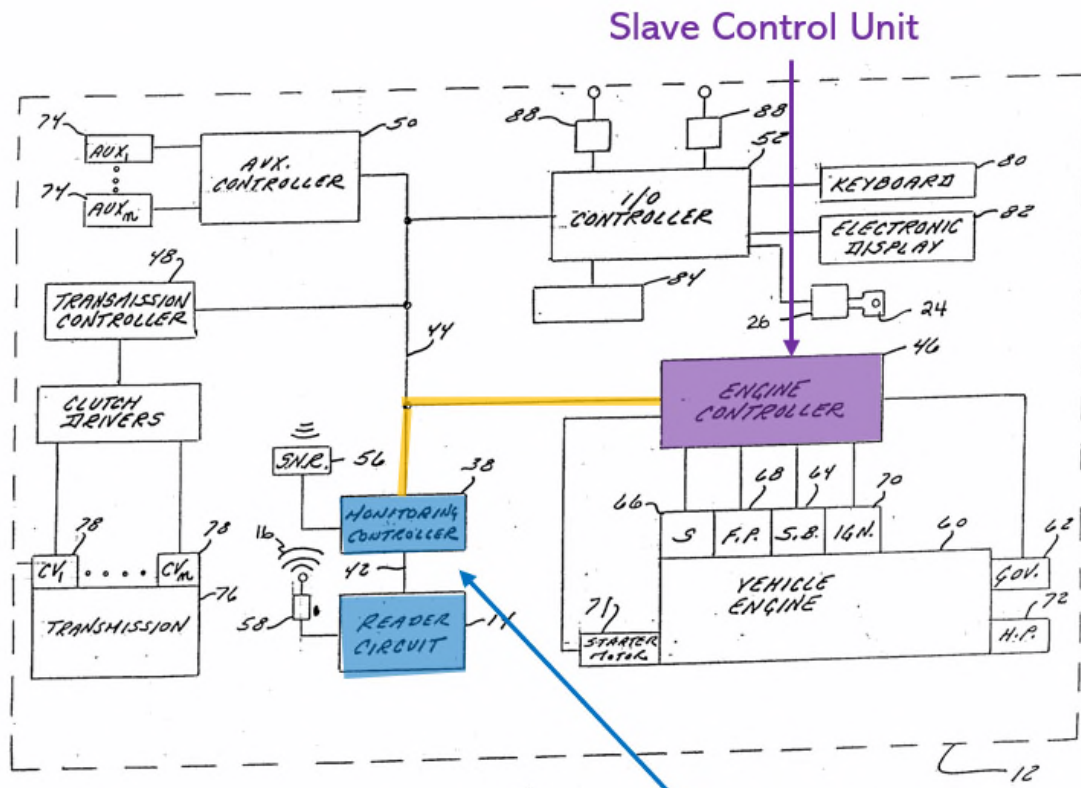
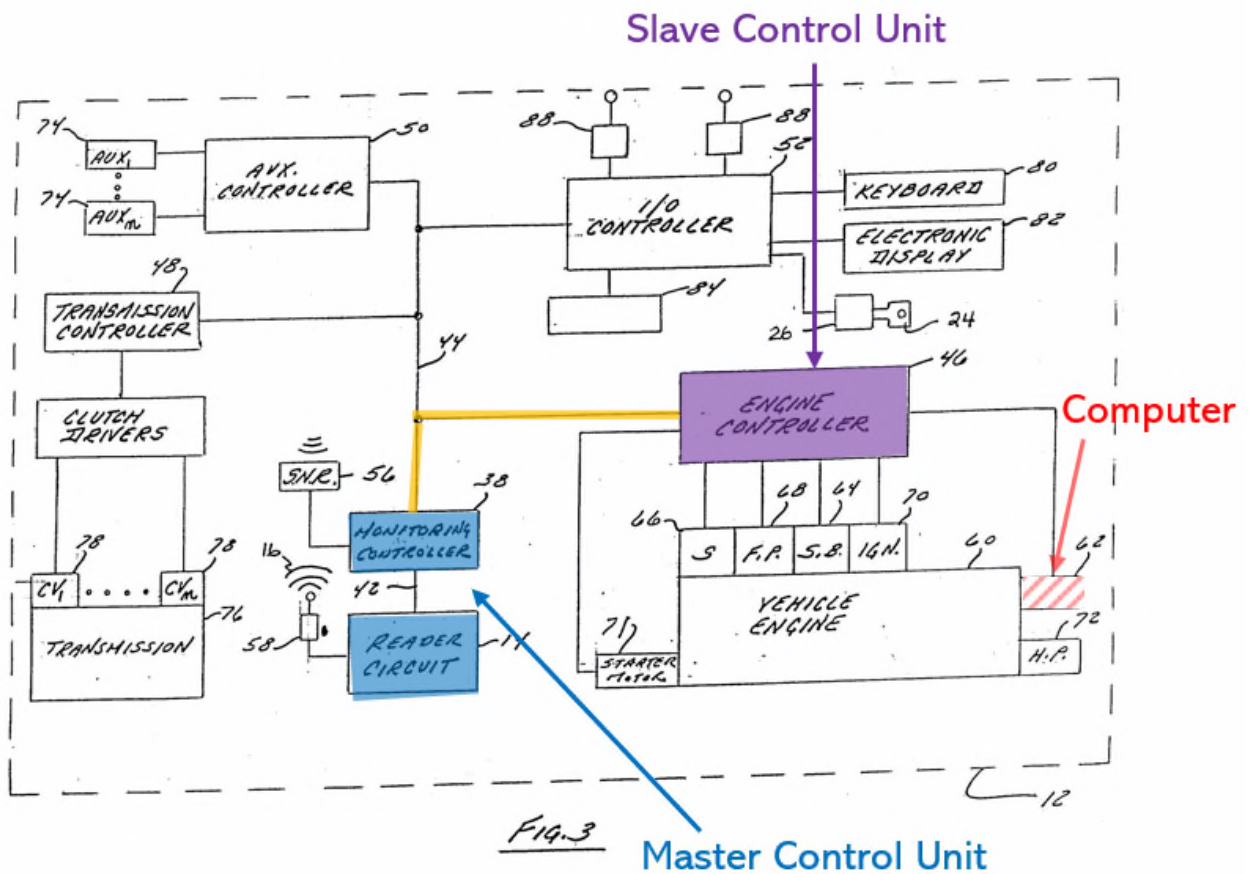


Fig. 3 Master Control Unit

(Arshad, Fig. 3 (annotated), [0028], [0041]-[0042].) Arshad discloses that “engine controller 46” is one of several “microprocessor-based controllers” in the vehicle that are “*coupled together with*” controller 38 via a data “bus 44.” (*Id.*, [0028].) Arshad disclose that monitoring controller 38 “*communicates with* the other controllers,” including the engine controller 46, by sending and receiving data “packets” over the bus. (*Id.*, [0041], [0043]-[0044], [0065], [0072], [0074].) For example, “monitoring controller 38” can transmit packets to the “engine controller 46” to shut down the fuel pump or ignition, or to limit vehicle or engine speed. (*Id.*, [0044].) As another example, “engine controller 46” can transmit “packets on bus

44” indicative of engine operation which are then received by controller 38. (*Id.*, [0072]-[0074].)

193. Furthermore, engine controller 46 (*e.g.*, “slave control unit”) is coupled to multiple “computers” associated with the vehicle, such as “electronic” “governor 62”:



(Arshad, Fig. 3 (annotated).) Engine controller sends signals to electronic governor that “indicates a commanded fuel flow rate or power output.” (Arshad, Fig. 3, [0046].) In response, electronic governor 62 generates and sends “an electronic signal” to fuel injectors or to open and close a “throttle valve.” (*Id.*) Further,

electronic governor 62 can “transmit a signal back to the engine controller 46” indicative of engine speed. (*Id.*) A “computer” is simply an electronic device or module for storing and/or processing data. Because governor 62 is an electronic device receiving and processing information, which can then take different actions as outputs, it is a “computer.”

194. Similarly, engine controller 46 is coupled to “transmission controller 48,” “auxiliary controller 50,” and “input/output controller 52” through bus 44. (Arshad, Fig. 3, [0041], [0051]-[0054], [0063]-[0072].) Each has “a microprocessor 90,” RAM, ROM, and a “communication processor 96 configured to handle all communications over bus 44 with other controllers.” (*Id.*, [0075]-[0080], Fig. 4.) For example, ““transmission controller 48” controls the “shifting of the vehicle’s transmission 76” and is configured to “select the particular clutches necessary to engage the transmission in a particular gear ratio and sequentially energizes the clutch control valves 78 such that appropriate gears and shafts are engaged.” (*Id.*, [0052]-[0053].) Because transmission controller 48 is an electronic device that receives and process information and can then select particular clutches accordingly, it is a “computer.” Additionally, auxiliary controller 50 controls the “operation of various hydraulically powered subsystems of the vehicle” and regulates the “flow of fluid to and from the lift arm cylinders and bucket cylinders (as the case may be)

that raises, lower, and tilt the bucket.” (*Id.*, [0051], [0054].) Because auxiliary controller 50 is an electronic device that controls flows of fluid within the vehicle system by receiving and processing information related to the hydraulically powered subsystems and then taking certain actions as outputs, it is a “computer.” Moreover, input/output controller 52 “drives and responds to operator interface devices including keyboard 80, display 82, audio annunciator 84, and key switch 26.” (*Id.*, [0051], [0054].) Because it is an electronic device that receives information and responds to the interface devices as outputs, it is a “computer.” Thus, these controllers comprise “computers” “associated with the motor vehicle.”

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

195. Arshad renders obvious Claim 1[D].

196. *First*, Arshad’s engine controller 46 (*e.g.*, slave control unit) is configured to monitor vehicle operation and generate signals to monitoring controller 38 (*e.g.*, master control unit). Engine controller 46 “is ***configured to monitor***” vehicle operation, such as “elapsed engine hour[s],” “engine speed,”

“engine load,” “oil pressure,” “oil temperature,” and “coolant temperature.” (Arshad, [0042]-[0043], [0046]-[0047], [0050], [0065], [0072], [0074].) For example, it “*transmits*” such data (*e.g.*, signals) “on bus 44,” and “[c]ontroller 38 *receives* this information.” (*Id.*, [0072], [0042]-[0043], [0065].)

197. Arshad’s monitoring controller 38 (*e.g.*, master control unit) receives information from other controllers and sensors regarding vehicle operation, such as geographic location and auxiliary system use. (Arshad, [0042], [0058]-[0059], [0064]-[0074].) For example, it “compares the elapsed engine hour data” from the “engine controller” with “authorized hours received from the transponder” to determine whether operational limits were “exceeded.” (*Id.*, [0043]-[0045], [0065], [0072].) In addition, it compares “engine RPM” and “engine load” data from the engine controller against operational limits on engine speed and load and determines whether these have been exceeded. (*Id.*, [0043]-[0045], [0065], [0074].)

198. With regard to engine controller 46 generating a signal to monitoring controller 38 “if the at least one driver violates the operating profile, thereby providing feedback to the master control unit about usage of the vehicle,” engine controller 46 receives operational limits from monitoring controller 38, with engine controller 46 then comparing engine operating conditions to the limits. (*Id.*, [0074].) If engine controller 46 determines a violation occurred based on the comparison of

engine speed and load to the limits, it “can be configured to maintain these speed and load limits by itself, without input from controller 38.” (*Id.*) However, it would have been obvious to a POSITA that engine controller 46 could also, upon its comparison showing engine limits were violated, send a signal to the monitoring controller 38 regarding the violation, thereby providing such additional feedback about vehicle operation to monitoring controller 38. (*Id.*, [0065], [0069]- [0072], [0074].)

199. Arshad’s engine controller 46 already provides engine operation information to monitoring controller 38 (and other controllers), and a POSITA would have understood engine controller 46 could likewise provide information such as determined engine operation violations. (*Id.*) This would have simply been providing additional information (engine violations) that is similar to the information already provided (engine operating information) in the same manner by transmitting it over bus 44. (Arshad, [0064]-[0074].) In fact, engine operation violations are the type of data Arshad teaches monitoring controller 38 would consider, as Arshad discloses “[c]ontroller 38” constantly monitors data from other controllers, including data “indicative” of “events” or “error conditions experienced” by the controllers. (*Id.*, [0042], [0069]-[0074].) For example, some of these signals indicate the vehicle is being improperly used, such as going too fast, operating the engine at too high of

a speed, or exceeded geographical (e.g., “This vehicle cannot be used outside of Michigan.”), or operating hours limits (e.g., “Only 15 minutes left to operate the vehicle.”). (*Id.*)

200. A POSITA would have been motivated to have engine controller 46 send data regarding violations of engine limits to monitoring controller 38, so that it can receive this feedback and take into account all vehicle operation information when issuing commands to monitor driving safety. For example, where the operating time limit is exceeded, or where the driver forces the engine to exceed its operational load or RPM limits, engine controller 46 can alert monitoring controller 38 of this occurrence and then wait for a command on what action to take. (*Id.*, [0043]-[0045], [0072], [0074].) Having engine controller 46 send such a signal to monitoring controller 38 would also be consistent with Arshad’s approach of keeping all controllers in “constant communication with each other” (*id.*, [0064]), and allowing monitoring controller to determine the “priority” of the limit being exceeded before determining which actions the system should take. (*Id.*, [0043]-[0045].) While its engine controller 46 is able to automatically take certain actions (*id.*, [0074]), Arshad acknowledges it may not always want to do so. (*Id.*, [0045] (for example, if a vehicle is traveling 60 mph down a highway, controller 38 may decide not send a packet to engine controller 46 instructing it to stop the engine immediately or slow

significantly, but would instead instruct I/O controller 52 to display a warning message.)

201. *Second*, engine controller 46 (*e.g.*, slave control unit) cooperates with at least one “computer” to control vehicle operation based on commands received from monitoring controller 38 (*e.g.*, master control unit). For example, in response to information from engine controller 46 that an engine limit was exceeded, monitoring controller 38 can transmit a packet instructing engine controller 46 to “shut down the fuel pump, the ignition system, or to limit the speed of the vehicle or the engine,” as well as “transmit a packet to I/O controller 52 commanding it to display a message indicating what limit has been exceeded.” (Arshad, [0044]-[0045], [0058]-[0063], [0071]-[0074].) In response to such commands, engine controller 46 cooperates with “computers” to control vehicle operation, such as by “sending a signal” to electronic governor 62, which then instructs the “fuel injectors” to regulate “fuel flow rate or power output” to “limit the speed of the vehicle,” “stop[]” the engine, or limit the engine’s RPM and load. (*Id.*, [0044]-[0046], [0074].) The governor may alternatively “open or close” a “throttle valve.” (*Id.*, [0046].) *See also supra* Ground 4, Claim 1[C] (discussions on “computers”).

202. Similarly, engine controller 46 engine controller 46 cooperates with I/O controller 52 (another computer) to control vehicle operation based on commands

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

**b) Dependent Claim 4: *The driver authentication and monitoring system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.***

203. Arshad renders obvious Claim 4.

204. Arshad discloses a “satellite navigation receiver 56” (*e.g.*, “GPS module”) which is “coupled to” monitoring controller 38:

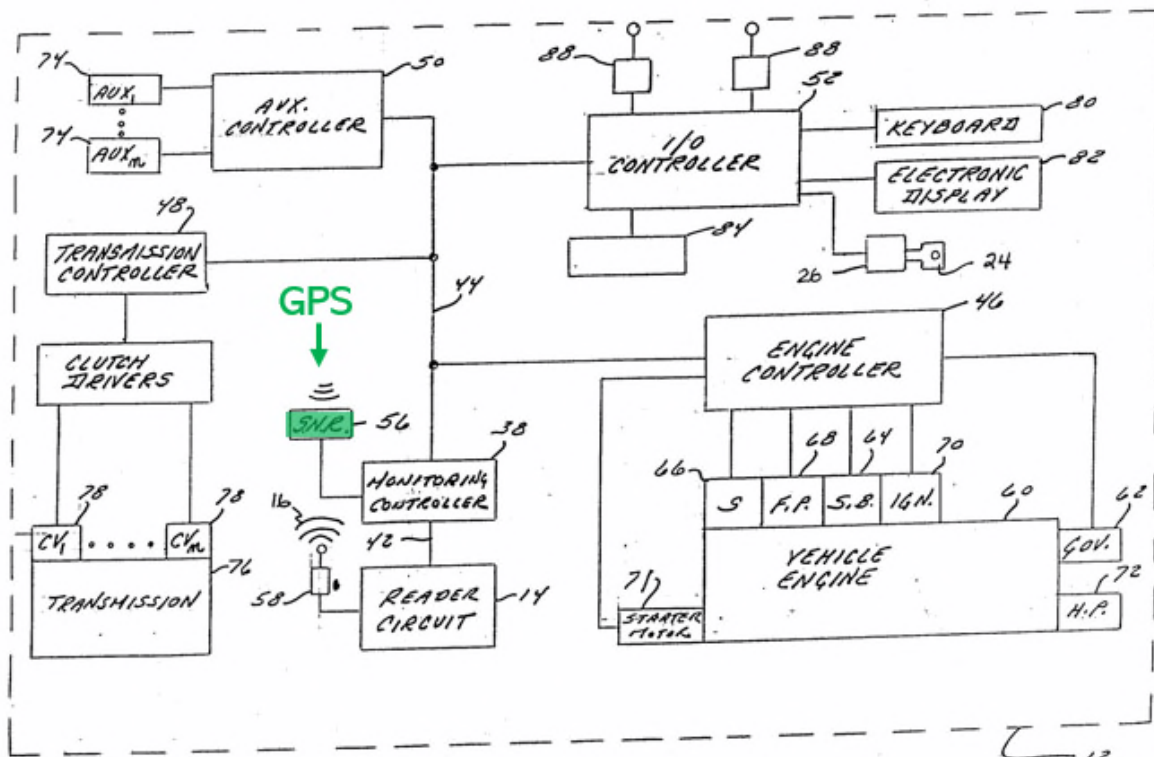


Fig. 3

(Arshad, Fig. 3 (annotated), [0029].) The satellite navigation receiver “is configured to receive radio transmissions from satellites and to convert them into data indicative of the vehicle's current location such as latitude and longitude.” (*Id.*, [0029], [0073] (disclosing that controller 38 is configured to receive “data indicative of the vehicle’s current position from receiver 58 [sic],” compare it to the authorized geographic area of operation received from the transponder, and generate a message to display a warning if the limit is approached or exceeded.)) As such, a POSITA would understand it is a “GPS receiver,” as it receives global positioning signals from satellites and uses them to determine latitude and longitude location information.

205. The system in Arshad further includes a memory module, as “each controller (including controller 38) of FIG. 3 has a microprocessor 90, **RAM memory 92 and ROM memory 94.**” (*Id.*, [0075]; *see also* [0078]-[0079].) In addition, “transponder 20” contains an “internal digital **memory.**” (*Id.*, [0023], [0025]-[0027], [0033]-[0034], [0060], Fig. 2.)

206. Arshad’s system also includes numerous “function indicator modules.” For example, Arshad’s “engine controller 46” is coupled to “sensors 66 that are themselves coupled to the engine to generate signals indicative of oil pressure (oil pressure sensor), oil temperature (oil temperature sensor), coolant water temperature (coolant temperature sensor), engine speed (sensor 64) and engine load.” (*Id.*, [0047], [0050], [0065], Figs. 2-4.)

207. Furthermore, Arshad discloses that its system includes a “display 82” that can “**indicate[]**” any “**alarm conditions**” controllers determine exist based on information from sensors, such as “oil pressure too low,” “coolant water temperature too high,” or “approach[ing] the authorized engine RPM.” (*Id.*, [0056], [0074].) Further, Arshad’s controllers 38, 46, 48, 50, and 52 monitor vehicle operation and determine “**fault or error conditions,**” such as “low fuel” or “electrical output too low,” which are recorded in the transponder’s memory. (*Id.*, [0027].)

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

- c) **Dependent Claim 5: *The driver authentication and monitoring system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.***

209. Arshad renders obvious Claim 5.

210. Arshad discloses that the operating profile, including the "operational limits" for the particular driver, includes "numeric or digital values that are remotely downloaded into the transponder" and "stored in the memory of microcontroller 30" within the transponder. (Arshad, [0026]-0027], Fig. 2; *see also* [0023].)

211. Furthermore, Arshad discloses that "transponder 20" downloads the "operational limits" for the driver into "controller 38" when the driver is authenticated, thereby enabling controlled operation of the vehicle. (Arshad, [0031], [0034], [0040]-[0043].) Arshad discloses, for example, that controller 38 includes "RAM *memory 92*," which "is used to store working variables" used by the controller. (Arshad, [0075], [0078]-[0079].) *See also supra* Ground 4, Claims 1[A]-[B], 4. A POSITA would understand that RAM memory 92, which Arshad discloses

as the only memory associated with controller 38, stores information related to vehicle control operation, including the “working variables” for the controller. (Arshad, [0075], [0078]-[0079].) A POSITA would understand that the “working variables” include operational limits for controller 38 to control the operation of the vehicle.

- d) **Dependent Claim 6:** *The driver authentication and monitoring system of claim 4, wherein the GPS module provides location information to at least the master control unit in association with a physical location of the vehicle.*

212. Arshad renders obvious Claim 6. *See supra* Ground 4, Claim 4. I also note that, as I explained in Claim 11[B] below, the GPS location information is provided by the GPS module to the controller (*e.g.*, master control unit). *See infra* Ground 5, Claim 11[B].

- e) **Dependent Claim 10:** *The driver authentication and monitoring system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.*

213. Arshad renders obvious Claim 10.

214. Arshad discloses its driver identification interface includes “a radio (RF) transponder 20” and radio frequency antenna 58. (Arshad, Abstract, [0019], [0022]; *see also* [0010]-[0013], [0030]-[0033].) Arshad’s transponder is a radio frequency identification device, “preferably one of Texas Instruments RFID

products,” that transmits “radio signals” which can be “receiv[ed]” by “antenna 58” of “reader circuit 14.” (*Id.*, [0023]-[0025], [0030]-[0034].) *See also supra* Ground 4, Claims 1[A]-[B].

215. The “transponder 20” in Arshad is also a portable handheld device, because it can be carried by an vehicle operator. Arshad teaches the “transponder” includes a microcontroller, integrated circuit package, antenna, capacitors, and memory, and that it can be “molded into a thin credit card-sized sheath” and “easily carried” in a “wallet, shirt pocket or pants pocket,” or incorporated into the ignition key. (*Id.*, [0020]-[0023], Figs. 1-2.)

**2. Ground 5: Arshad in View of Petrik Renders Obvious Claims 2-4, 8-9, 11, and 13-20**

216. As viewed by a POSITA, Arshad in view of Petrik renders obvious Claims 2-4, 8-9, 11, and 13-20.

217. I have reviewed Petrik which is US2007/0168125. I understand that Petrik was filed August 9, 2005 and published July 19, 2007. I understand Petrik is prior art under at least pre-AIA 35 U.S.C. §§ 102(a) and (e).

218. My review of the ‘427 Patent file history reveals that Petrik was not considered during prosecution of the ‘427 Patent.

219. Petrik discloses an in-vehicle monitoring unit that incorporates GPS based 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].)

**a) Independent Claim 11**

220. As viewed by a POSITA, Arshad in view of Petrik renders obvious independent Claim 11.

**(i) Claim 11[pre]: A driver authentication and monitoring system, comprising:**

221. Arshad discloses the preamble of Claim 11 to the extent the preamble limits the scope of the claim. *See supra* Ground 4, Claim 1[pre].

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

222. Arshad discloses Claim 11[A].

223. Arshad discloses a “master control unit” (*e.g.*, reader circuit 14 and monitoring controller 38) for “authenticating at least one driver via [a] driver identification [interface].” *See supra* Ground 4, Claim 1[A]. Moreover, the reader circuit and monitoring controller “associate[s]” an “operating profile with the at least one driver.” *See supra* Ground 4, Claim 1[B].

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

224. Arshad in view of Petrik renders obvious Claim 11[B].

225. Arshad discloses a “satellite navigation receiver 56” (*e.g.*, “GPS module”) which is “coupled to” monitoring controller 38 and provides it with “data indicative of the vehicle’s current location.” (Arshad, [0029], [0073], Fig. 3.) *See also supra* Ground 4, Claim 4. A POSITA would understand that satellite navigation receiver 56 can receive GPS signals from satellites and can calculate their own

position and speed of the vehicle from the received signals.

226. Additionally, it would have been obvious for such GPS module to provide additional speed information. Petrik, in the same field of Arshad, discloses a “GPS based vehicle monitoring, management and cruise control” system with an “in-vehicle monitoring unit” for identifying drivers, monitoring vehicle operation, and taking actions such as issuing alerts and using an engine controller to slow or stop a vehicle if the driver deviates from operational limits. (Petrik, [0016]-[0026], [0030], Fig. 1.) Drivers are issued “smart cards,” which, similar to the “transponders” in Arshad, are read by a reader to confirm driver identity and allow vehicle operation within “vehicle and driver related operational parameters” such as an intended “route plan,” required “rest times,” and speed limits. (Petrik, [0001], [0009], [0017]-[0018], [0025]-[0028].) An in-vehicle unit is connected to an engine management system, which is programmed to take instructions from it and perform actions such as slowing down or stopping the vehicle if limits are exceeded. (*Id.*, [0020], [0025]-[0026], [0030].)

227. Petrik discloses using a “GPS receiver module” to provide location and speed information, and its system “keeps a constant log of the date, time, location, distance travelled and speed of the vehicle both in the units’ memory and in the smart card.” (*Id.*, [0001], [0025]-[0026], [0009], [0040].) The GPS speed and location

information is used by Petrik's in-vehicle monitoring unit to prevent the vehicle from exceeding speed limits and to determine if a driver has deviated from a permissible route (*e.g.*, filed route). (*Id.*, [0025]-[0028], [0030].)

228. It would have been obvious to modify Arshad to, as taught by Petrik, use a GPS module to provide both location and speed information to monitoring controller 38. A POSITA would have been motivated to use a GPS to determine both location and speed, as taught by Petrik, in order to have an accurate source of location, speed, and time information that could not be manipulated by the driver, and that could be stored in logs to keep a record of vehicle operation. (Petrik, [0001], [0009], [0012], [0025]-[0028].) A POSITA would have had a reasonable expectation of success in implementing a GPS module to provide both speed and location information, as Arshad already includes a satellite receiver for determining location information, and a POSITA would have understood that using a GPS module to determine both location and speed information would simply be the use of a known component for its intended function to better monitor driving behaviors. Additionally, a POSITA would have understood that using GPS speed and location information, as taught by Petrik, would provide the speed and location information necessary for the monitoring controller 38 to determine if a driver has violated speed or geographic operational limits.

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

229. Arshad in view of Petrik renders obvious Claim 11[C].

230. Arshad discloses that “microcontroller 30” within the “transponder 20” can “receive[] data from the vehicle” and “store[] this data in its internal memory,” thus disclosing a data logging device which records vehicle operation data (e.g., distance travelled, time vehicle started/stopped) indicating use of the vehicle by the driver. (Arshad, [0025]-[0027].) *See supra* Ground 4, Claim 11[C].

231. In a similar field as Arshad, 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 teaches that “the GPS keeps a constant log of the date, time, location, distance travelled and speed of the vehicle both in the [in-vehicle] units' memory and in the smart card.” (Petrik, [0025]-[0029]; *see also* [0009], [0012], [0018].) It would have been obvious to a POSITA to modify Arshad to record GPS speed and location information in its transponder 20 as well as a memory in controller 38. A POSITA would have understood that, as taught by Petrik, this would provide an irrefutable log of operational and infraction data that could not be manipulated by the driver. *See also*

*supra* Ground 5, Claim 11[B].

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

232. Arshad discloses Claim 11[D]. *See supra* Ground 4, Claim 1[C].

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

233. Arshad discloses Claim 11[E]. *See supra* Ground 4, Claim 1[D].

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

234. Arshad discloses Claim 11[F]. *See supra* Ground 4, Claims 1[B]-1[D].

**b) Independent Claim 15**

235. As viewed by a POSITA, Arshad in view of Petrik renders obvious independent Claim 15.

**(i) Claim 15[pre]: *A method of authenticating and monitoring drivers, comprising:***

236. Arshad discloses the preamble of Claim 15 to the extent the preamble limits the scope of the claim, because it discloses a method for driving authentication and monitoring. *See supra* Ground 4, Claim 1[pre].

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

237. Arshad discloses Claim 15[A], because it discloses a driver authentication and monitoring system in a vehicle. *See supra* Ground 4, Claims 1[pre], 1[A].

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

238. Arshad discloses and renders obvious Claim 15[B].

239. In Arshad, the system can be programmed with an operating profile associated with a high risk driver. *See supra* Ground 4, Claim 1[B]. The '427 discloses that high-risk drivers may be fleet or rental drivers ('427, 2:34-38), and Arshad discloses its system can be used with “fleets” of vehicles, including rental

vehicles. (Arshad, [0005]-[0009], [0033], [0045].)

240. Arshad discloses that “operational limits” are programmed into the transponder, as they are “*remotely downloaded into* the transponder.” (Arshad, [0026], [0043], [0057]-[0059].) *See supra* Ground 4, Claim 1[B]. These operating limits are maintained in the memory of the transponder. (*Id.*) Further, the operational limits are programmed into the monitoring control unit, as they are downloaded from the memory of the transponder to the controller 38 “for processing.” (*Id.*, [0034], [0043], [0057], [0071]-[0073]; *see also* [0074] (indicating the operational limits may be downloaded to the engine controller 46 as well.)) Moreover, these operational limits are maintained by data logging devices, namely the memories, contained in monitoring controller 38 and other controllers within the system. (*Id.*, [0034], [0043], [0057], [0075]-[0080].)

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

241. Arshad discloses Claim 15[C].

242. Arshad discloses authenticating high-risk or high profile drivers and enables their operation of a motor vehicle within their respective operating profiles. *See supra* Ground 4, Claims 1[A]-[B]. By “high profile drivers,” the ’427 refers to

drivers who are “high-risk” and thus have operating “profile” restrictions. (See Response to Non-Final Office Action of November 15, 2018 (U.S. App. No. 15/898,322, later U.S. Patent No. 10,259,465) (in a nearly identical claim, changing “high profile” to “high risk” in response to an antecedent basis rejection).) In other words, “high profile” drivers are those who pose a greater risk than a typical driver, and thus have a need for a strict operating profile. (See ’427, Abstract, 1:63-2:5 (discussing high risk drivers).)

243. Further, Arshad discloses “monitoring” operation of the vehicle to determine if the driver violates the operational parameters of their profile. *See supra* Ground 4, Claims 1[C]-[D]. For example, Arshad’s “monitoring controller 38” compares data it receives from controllers and sensors with operational limit data received from the transponder “to determine whether the operator has attempted to exceed any of the operational limits” and if the limits are exceeded. (*Id.*, [0042]-[0044], [0058]-[0059], [0065], [0071]-[0074] (disclosing that the engine controller 46 can also monitor operation of the engine and determine if operational limits are approached or exceeded).)

- (v) **Claim 15[D]: *generating a signal if said high profile driver violates the operating profile while operating the motor vehicle; and***

244. Arshad discloses and renders obvious Claim 15[D].

245. Arshad discloses generating a signal if the high-risk driver violates the operating profile. For example, if operational limits are approached or exceeded, controller 38 generates a signal to one of the other “microprocessor-based controllers” “directing” it to take responsive action. (Arshad, [0028], [0043]-[0044]; *see also* [0045]-[0046], [0057]-[0059], [0061]-[0063], [0071]-[0074].) Controller 38 can signal engine controller 46 to slow or stop the engine. (*Id.*, [0044]-[0046]; *see also* [0074].) Controller 38 can also signal I/O controller 52 to generate an “audio alarm” or a visual “alphanumeric message.” (*Id.*, [0044]-[0045], [0057]-[0059], [0061]-[0063], [0071]-[0073].) Additionally, if a driver attempts to use a hydraulic subsystem they are not authorized to access, controller 38 “will *not* forward the operator request” to “auxiliary controller 50,” thereby preventing the subsystem from operating. (*Id.*, [0071].) *See also supra* Ground 4, Claims 1[C]-[D].

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

246. Arshad in view of Petrik renders obvious Claim 15[E].

247. Similar to Arshad, Petrik discloses an in-vehicle unit that is in communication with a “base station” and a “Transport Management Command Centre” through SATELITE/GPRS/GSM two-way communications. (Petrik, [0016]-[0018], [0030], [0069], Fig. 1, Cls. 48-51.) Petrik’s in-vehicle unit and the remote Command Centre monitor operation of the vehicle, including whether the

vehicle is adhering to a “route plan” of where the driver is allowed to operate. (Petrik, [0030], [0010].) If the driver of the vehicle is not adhering to the route plan, or if the driver is determined to be out of control or hostile, an alarm signal can be generated and sent from the in-vehicle unit to the Command Centre, and the Command Centre can send the in-vehicle unit a “disable” command. (*Id.*) This command from the remote Command Centre can control operation of the vehicle remotely, as it can be passed from the in-vehicle unit to the engine management system to “lock up” and stop the vehicle.

248. It would have been obvious for a POSITA to modify Arshad to include providing a Command Centre in communication with Arshad’s “control system 12” to allow for remotely controlling operation of the vehicle, as taught by Petrik. A POSITA would have been motivated to modify Arshad’s control system 12 to include providing for remote commands to control operation of the vehicle, as taught by Petrik, in order to increase driving safety and give real-time instructions based on information at the command facility such as traffic jams, accidents, road closures, and adverse weather. (Petrik, [0030], Cls. 48-53, 58-60.)

249. A POSITA would have had a reasonable expectation of success in implementing such remote commands to, for example, disable the engine, in Arshad’s system. Furthermore, Arshad discloses its engine controller 46 can slow or

stop the engine based on commands received from monitoring controller 38 (Arshad, [0044]-[0045], [0074]), and Petrik merely adds that a command sent from an in-vehicle control unit (like Arshad's monitoring controller 38) to an engine control unit (like Arshad's engine controller 46) can originate from a remote facility. (Petrik, [0030], Cls. 58-60.) This would have simply required the addition of a known component—a two-way communications module like Petrik's SATELITE/GPRS/GSM module—for its intended purpose to achieve better monitoring and safety purposes. Arshad's system was ready for such modification, as it already includes multiple controllers that communicate with each other over a data bus and adding the two-way communication module would simply be the addition of another controller on this same communication bus. Thus, Arshad's system would continue operating as expected, but with an additional safety backup to allow a remote facility to take control of the vehicle if, for example, the driver continuously violates the operational limits or is out of control and causing hazardous situations. This would have further allowed greater control and flexibility from the remote facility over the overall fleet of vehicles and drivers, as the remote facility would receive information regarding each driver's operation of the vehicles.

- c) **Dependent Claim 2:** *The driver authentication and monitoring system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.*

250. Arshad in view of Petrik renders obvious Claim 2.

251. Arshad discloses a program module, which comprises “numeric or digital values” indicative of operational limits that can be “remotely downloaded into the transponder.” (Arshad, [0026].) These limits reflect the “different degrees of access” authorized by fleet management for different vehicle operators. (*Id.*, [0008]-[0013].)

252. Similar to Arshad, Petrik discloses a fleet management system identifies drivers and allows operation of fleet vehicles only within operation parameters, such as speed limits, geographic route plans, and operation time limits. *See supra* Ground 5, Claim 11[B]. Petrik’s system includes a “Command Centre with an up to date database of road conditions” and other parameters associated with a vehicle, such as “accidents, road closures, detours, adverse weather,” “geographic speed zones,” “state border crossings,” and “driver hours of service records.” (Petrik, [0010]-[0011], [0024], [0030], Cl. 49.) An authorized user (*e.g.*, dispatcher) at a dispatch has access to the Command Centre database via a SATELITE/GPRS/GSM

link, and can use the Command Centre database to program the operating profile of the driver. (*Id.*, [0024], [0030], Cls. 49-51.) For example, the dispatcher at the Transport Management Command Centre can check its up to date national database to see if any obstacles, such as accidents, road closures, detours, adverse weather etc. exist along the intended route, and notifies the vehicle via the SATELITE/GPRS/GSM. (*Id.*, [0010]-[0011], [0024], [0030], Cls. 49-51.) As another example, the dispatcher can also program speed limits for the driver based on the speed zone information in the Command Centre database. (*Id.*, [0018]-[0019], Cls. 49-51.)

253. It would have been obvious to a POSITA to modify Arshad's system to include providing a facility with a remote database of operating parameters accessible by an authorized user (such as a fleet manager) via a network utilizing a remote computer, as taught by Petrik. A POSITA would have understood that such a modification can be performed, for example, by providing authorized fleet managers computer access to the remote facility database over a network communication link. (Petrik, [0010], [0018], [0024], [0030], Cls. 48-51.) This would have allowed fleet managers and dispatchers to access the remote, central database and review the information stored on the database when programming the "numeric or digital values" indicative of the operational limits, before they are downloaded to

the transponder remotely over the network. (Arshad, [0026].)

254. A POSITA would have understood that, by accessing the remote database, the fleet manager could check driver records, current detours or road closures, and adverse weather, before setting, for example, operating time and geographic limits for the driver to achieve better safety and flexibility monitoring. (Petrik, [0010], [0018], [0024], [0030], Cls. 48-51; Arshad, [0026].) Arshad's system was ready for this improvement, and a POSITA would have had a reasonable expectation of success because it would have involved simply using known components including computer, networked communications, and a central database available over the network, to achieve their intended functions, as taught by Petrik. Additionally, this would have facilitated Arshad's goals of managing fleets of vehicles and authorizing different degrees of vehicle operation to different drivers. (Arshad, [0008]-[0013].).

**d) Dependent Claim 3: *The driver authentication and monitoring system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the master control unit for the at least one driver.***

255. Arshad in view of Petrik renders obvious Claim 3.

256. Arshad discloses that its driver identification interface (e.g., transponder 20 and reader antenna 58) loads driver operational limits to the reader circuit and monitoring controller 38. *See supra* Ground 4, Claims 1[A]-[B].

Furthermore, as I discussed in Claim 2 above, Arshad in view of Petrik renders obvious loading the operational limits using the transponder and a remote computer. *See supra* Ground 5, Claim 2. For example, a POSITA would have understood that an authorized user at a remote computer could access a central database, program a profile, and then “remotely download” values indicative of the operating limits to the transponder. *Id.*

- e) **Dependent Claim 4: *The driver authentication and monitoring system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.***

257. Arshad in view of Petrik renders obvious Claim 4.

258. Arshad discloses a satellite navigation module, a memory module, and a function indicator module. *See supra* Ground 4, Claim 4. Moreover, Petrik discloses a GPS module, and it would have been obvious to include such a GPS module in Arshad’s system to obtain location and speed information. *See supra* Ground 5, Claim 11[B]. A POSITA would have understood that such a modification merely involves adding a known component into Arshad’s system for its intended purpose.

- f) **Dependent Claims 8/13: *The driver authentication and monitoring system of claim [2/11], wherein [the/the 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.***

259. Arshad in view of Petrik renders obvious Claims 8 and 13.

260. For example, Arshad’s “operating limits” include (i) “maximum speed” (*i.e.*, maximum allowable vehicle speed), (ii) “geographical area in which the vehicle” can operate and “total distance of authorized travel” (*i.e.*, allowable vehicle locations), and (iii) “allowed times and dates of operation,” “number of hours of authorized use,” and “predetermined number of hours” the engine can be operated (*i.e.*, allowable hours of operation). (Arshad, [0011]-[0013], [0026], [0043]-[0045], [0057], [0059], [0072]-[0074].) *See also supra* Ground 4, Claim 1[B].

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

261. Arshad in view of Petrik renders obvious Claims 9 and 14.

262. In Arshad, the in-vehicle system monitors whether a driver is operating the vehicle in accordance with her operating profile, and, if she violates her profile, the system can “display a message” that provides an alert “indicating what limit has been exceeded.” *See supra* Ground 1, Claim 1[D].

263. Similar to Arshad, Petrik discloses an “in-vehicle monitoring unit” that generates an alarm signal which “notifies” *authorized personnel at a remote facility* (e.g., “Transportation Management Command Centre”), via a “SATELLITE/GPRS/GSM” communication link, when a driver violates her operating profile, such as by “divert[ing] inappropriately from the ‘filed’ route plan.” (Petrik, [0030], Cl. 58-60.) The people, such as dispatchers at the Transportation Management Command Centre, are authorized personnel because they are administrators who can program or modify the operating profiles for the drivers.

264. It would have been obvious to a POSITA to modify Arshad to have its system (e.g., the engine controller) generate and send “alarm signals” to remote authorized personnel via a communications link, as taught by Petrik, for the reasons discussed in Claim 15. *See supra* Ground 5, Claim 15[E]. For example, a POSITA would have understood in view of Petrik that, after determining whether there is a violation, Arshad’s engine controller could generate an “alarm signal” that causes the system to transmit an alert to authorized persons at a remote facility. The ’456 broadly explains the “alarm signal” as a signal that “*can result* in an actual audible alarm, or it can be used to control/govern operational aspects of the vehicle.” (’456, 7:21-29.) The addition of a communications link to alert remote personnel in Arshad, as taught by Petrik, would have been the mere addition of basic, well-known

components that could be driven by the system already existing in Arshad.

265. Arshad's system was ready-for-improvement in this regard, and Arshad suggest the modification, as its system (including its engine controller) already monitors vehicle operation and discloses generating alerts based on this. A POSITA would have understood from this that such alerts in Arshad (*e.g.*, alerting that there has been a profile violation) could likewise be transmitted to authorized personnel at a remote facility, as taught by Petrik, to enhance the driving monitoring. A POSITA would have also been motivated (and it would have been obvious to try) to have the engine controller generate such an alert, since, for example, it is already monitoring the operation of vehicle components and can determine whether a driver has violated her profile based on this. By having Arshad's engine controller and system send such an alert to authorized personnel at a remote facility as taught in Petrik, Arshad would be able to better "manage access to vehicles used in fleets" (a stated purpose of it), as remote personnel would now be able to better monitor driver operation and better ensure that drivers comply with their profiles.

**h) Dependent Claim 16: *The method of authenticating and monitoring drivers in claim 15, wherein the motor vehicle includes a GPS module and the monitoring operation of the motor vehicle further comprises obtaining GPS data including motor vehicle speed and location.***

266. Arshad in view of Petrik renders obvious Claim 16. *See supra* Ground

5, Claim 11[B].

- i) **Dependent Claims 17/18:** *The method of authenticating and monitoring drivers in claim [15/16], wherein the step of generating a signal includes providing [an audible alarm to the driver and a signal remotely/an alarm remotely] to an authorized user.*

267. Arshad in view of Petrik renders obvious Claims 17 and 18.

268. Arshad discloses generating an audible alarm by energizing an annunciator to generate a “sound to get the operator's attention.” (Arshad, [0063], [0071]-[0072].) For the reasons that I discussed in Claims 9 and 14, Arshad in view of Petrik further renders obvious providing an alarm signal remotely to an authorized user. *See supra* Ground 5, Claims 9 and 14.

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

269. Arshad in view of Petrik renders obvious Claims 19 and 20.

270. In Arshad, the system takes numerous actions in response operating profile violations, such as generating a signal to slow or stop the vehicle. *See supra*, Ground 5, Claim 15[D]; *see also supra* Ground 4, Claims 1[D]. For example, “controller 38” can generate a signal (*e.g.*, an alarm signal) to alert “engine controller 46” that the operating profile was violated and “direct[]” it to control the engine. (Arshad, [0043]-[0044], [0074].) The “engine controller 46,” in turn, generates a

“control[]” signal to the “governor 62” to limit vehicle functionality, such as by “limit[ing] the speed of the vehicle,” “stopping” the engine, or limiting the engine’s RPM and load. (*Id.*, [0044]-[0046], [0074].) Furthermore, Arshad discloses “transmit[ing] a packet that shuts down a particular vehicle subsystem” if a driver violates her operating profile. (*Id.*, [0044]-[0445], [0057], [0060]-[0063], [0071]; *see also* [0011], [0013], [0020], [0026], [0040], [0045], [0051], [0067].)

**3. Ground 6: Arshad (Alone or as Modified by Petrik) in View of Wu Renders Obvious Claims 7 and 12**

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

271. Arshad (alone or as modified by Petrik) in view of Wu, renders obvious Claims 7 and 12. As discussed in Claims 7 and 12 above, they include well-known components—“a power regulator module; a starter relay module; a definable relay module; a slave microcontroller; and an alarm synthesizer.” *See supra* Ground 3, Claims 7 and 12. They are disclosed or would have been obvious based on Arshad alone, or, at minimum, based on Arshad in view of Wu.

272. Arshad discloses and renders obvious that its “engine controller 46” (*e.g.*, slave control unit) includes a power regulator module. Arshad’s “engine

controller 46” includes a “driver circuit 102” that “controls the application of power” to “actuators” such as the “fuel pump, governor and ignition system.” (Arshad, [0077]; *see also* [0044], [0048]-[0049], [0064].) Moreover, because it is an electronic component which controls other electronic components, a POSITA would have understood Arshad’s engine controller 46 to have a “power regulator” to ensure receipt of a stable supply of the required voltage, including as taught by Wu. (Wu, [0020], [0022], [0027]-[0028].)

273. Furthermore, Arshad’s engine controller includes a starter relay module. Arshad’s “engine controller 46” (*e.g.*, “slave control unit”) “is coupled to the engine starting motor 71 to turn the starting motor on or off under computer control.” (Arshad, [0049]-[0050].) The coupling would involve a starter relay to energize the starting motor. In a similar field, Wu discloses that such “starter relays” are commonly used to energize starter motors (Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2), and a POSITA would have understood that the coupling in Arshad’s system provides a well-known, commonly-used mechanism for activating and deactivating the starting motor.

274. In addition, Arshad’s engine controller also includes a definable relay module. “Engine controller 46” is “coupled to ignition system 70 of the engine” and can “energize or de-energize the ignition under computer control.” (Arshad, [0049]-

[0050]; *see also* [0044.]) Such coupling would involve a relay module to activate or deactivate the ignition system. In a similar field, Wu discloses that ignition systems can be energized and de-energized using an ignition circuit enabling means comprising a processor (like in Arshad's engine controller) and a relay. (Wu, [0020]-[0021], [0025], [0031], [0039], Figs. 1-2.) A POSITA would have been motivated to use such a processor and ignition relay, as taught by Wu, to implement the computerized control of the ignition system with Arshad's engine controller. This would have merely been the implementation of known components (*e.g.*, ignition relay) in a similar system for their intended purpose to achieve the same results (energizing or de-energizing the ignition). (*Id.*)

275. Moreover, Arshad discloses that its engine controller includes a slave microcontroller. The "engine controller 46" (*e.g.*, "slave control unit") is a "microprocessor-based controller" that includes a microprocessor, RAM and ROM, sensor circuit, driver circuits, and a communication processor. (Arshad, [0028], [0075]-[0080], Fig. 3.) Because engine controller 46 receives instructions from the monitoring controller 38 (*e.g.*, part of the master control unit), it is a slave microprocessor-based controller. Arshad's engine controller 46 includes a "driver circuit 102" that "controls the application of power" to "actuators" such as the "fuel

pump, governor and ignition system.” (Arshad, [0077]; *see also* [0044], [0048]-[0049], [0064].) Thus, its engine controller includes a slave microcontroller.

276. Further, Arshad renders obvious its engine controller including an alarm synthesizer. Arshad discloses its I/O controller can “energize annunciator 84” (e.g., an “alarm synthesizer”) to “generate a sound to get the operator’s attention” when operational limits are exceeded. (Arshad, [0054], [0063], [0071]-[0072].) For example, if “engine controller 46” senses that “the vehicle is approaching the time limit of engine operation,” a signal can be sent to the I/O controller which then activates the annunciator. (*Id.*, [0072].) A POSITA would be motivated to provide the annunciator with the engine controller, such that the engine controller could activate the annunciator to issue an audible alarm upon the engine controller determining allowed engine operational hours have been or will be exceeded. Engine controller includes driver circuitry like the I/O controller does, and it would have been obvious to use this driver circuitry to operate an annunciator immediately when the engine controller determines an operational limit of the engine is or will be exceeded. (Arshad, [0072], [0074].) Similarly, Wu discloses generating such audible alerts with a synthesizer, including an “operational amplifier” and “resistor,” and a POSITA would have understood this to be a common and simple way to implement

the audible alerts in Arshad to provide better driving safety monitoring. (Wu, [0030].)

## **VI. CONCLUSION**

277. For the reasons stated above, I believe that Claims 1-20 of the '427 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: April 25, 2025

## APPENDIX A

### Materials Considered

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