

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EQUIPMENTSHARE.COM INC.,
Petitioner,

v.

AHERN RENTALS, INC.,
Patent Owner.

IPR2021-00834
Patent 9,193,330 B2

Before JAMES J. MAYBERRY, JASON W. MELVIN, and
BRENT M. DOUGAL, *Administrative Patent Judges*.

MAYBERRY, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Equipmentsshare.com Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–3, 7–13, and 17–20 (the “Challenged Claims”) of U.S. Patent No. 9,193,330 B2 (Ex. 1001, the “’330 patent”). The ’330 patent is owned by Ahern Rentals, Inc. (“Patent Owner”). Paper 11, 1.

For the reasons below, we conclude that Petitioner has not proven, by a preponderance of the evidence, the Challenged Claims unpatentable. *Cf.* 35 U.S.C. § 316(e) (“In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.”).

A. Background and Summary

Patent Owner filed a Preliminary Response to the Petition. Paper 15. With our authorization, Petitioner filed a Preliminary Reply and Patent Owner filed a Preliminary Sur-reply. Papers 16, 17. Upon review of the arguments and supporting evidence in these papers, we instituted an *inter partes* review of all claims and grounds asserted in the Petition. Paper 19 (“Institution Decision” or “Inst. Dec.”).

We held a conference call with the parties on February 23, 2022, and Patent Owner informed the Board it did not intend to file a Patent Owner Response, but was not abandoning the contest. Paper 25, 1. We advised Patent Owner that we would not consider any arguments it made in its Preliminary Response at the Final Written Decision stage, unless Patent Owner refiled the Preliminary Response. *Id.*

Patent Owner refiled its Preliminary Response “with limited edits” as its Patent Owner Response. Paper 26, 1 (“PO Resp.”). Petitioner filed a Reply to the Patent Owner Response. Paper 26 (“Pet. Reply”). Neither

party requested an oral hearing, and no hearing was conducted. *See* Paper 32.

B. Real Parties-in-Interest

Petitioner identifies Equipmentsshare.com, Inc. as the real party-in-interest. *See* Pet. 4. Patent Owner identifies Ahern Rentals, Inc. as the real party-in-interest. Paper 11, 1.

C. Related Matters

The parties identify the following litigation as related: *Ahern Rentals, Inc. v. Equipmentsshare.com Inc.*, No. 2:20-cv-333 (E.D. Tex., filed Oct. 15, 2020). Pet. 4; Paper 11, 1.

D. The '330 Patent

The '330 patent is titled “Method and a System for Controlling and Monitoring Operation of a Device” and relates to the same. *See* Ex. 1001, code (54), 1:16–17. According to the background of the '330 patent, there existed a need to use certain pieces of equipment for a limited time, without actually purchasing them. *See id.* at 1:21–23. Typically, companies purchase the sought-after equipment (e.g., passenger vehicles, earthmoving equipment, and construction equipment) with the intent to rent or charter such equipment to users. *See id.* at 1:23–27. The rental company often delivers the equipment a day or two prior to actual use by the customer, and may also remove the equipment a few days after the customer use is complete. *Id.* at 1:34–38. If the equipment registers additional operating hours beyond the duration of authorized use, disputes between the renter and the owner may arise. *Id.* at 1:43–45.

One embodiment of the '330 patent is a method of controlling and monitoring operation of a device, which includes communicating an authorization code through a management source to a processor of the

device, having a memory. Ex. 1001, 1:49–51. The management source may be a host computer or a cellular telephone, and the communication may be accomplished via cell modem. *Id.* at 1:63–66. The processor is configured for regulating operation of the device, and is operatively connected to a keyless start arrangement configured to activate the device. *Id.* at 1:51–54. The method also includes entering an access code using a selective input (e.g., a keypad or a cellular telephone), and the processor receiving the access code. *Id.* at 1:56–58, 2:9–10.

Figure 1 of the '330 patent is reproduced below:

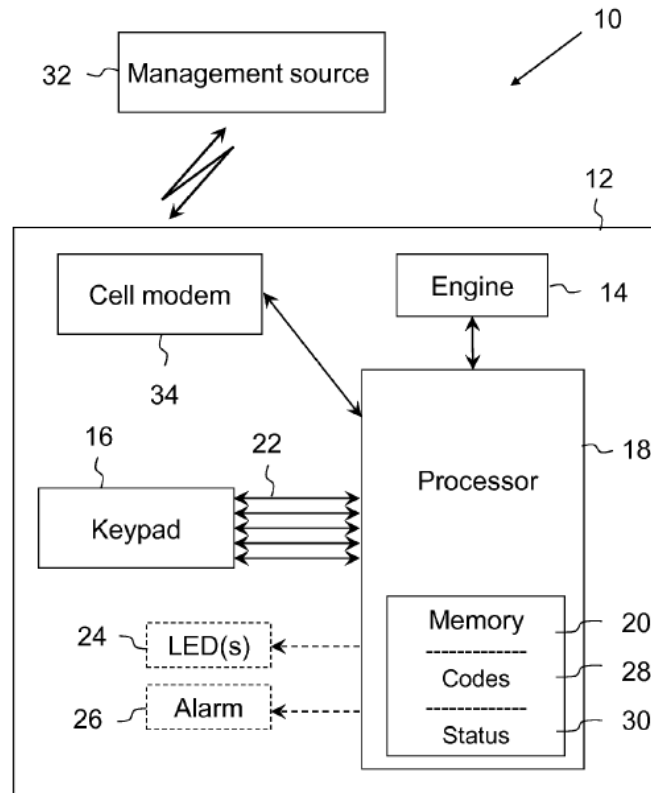


Fig. 1

Figure 1 is a schematic illustration of a system for controlling and monitoring operation of a device. Ex. 1001, 2:33–34. System 10 includes controlled equipment 12 having engine 14. *See id.* at 2:51–53. Controlled

equipment 12 may be a vehicle or a construction machine. *Id.* at 2:53–54. Controlled equipment 12 additionally includes a keyless start arrangement configured as a keyless ignition system of the controlled equipment 12. *Id.* at 2:54–56. The keyless ignition system includes keypad 16, operatively connected to electronically or mechanically interconnected devices, including a starter, coils, spark plugs, and sensors for starting engine 14. *Id.* at 2:57–61. In operation, during starting of engine 14, an access code selectively entered using keypad 16 activates the engine through operation of the starter, and facilitates function of the controlled equipment 12. *Id.* at 2:61–64. Controlled equipment 12 may additionally include accessories, for example, an excavator's bucket, a thumb, or a pulverizer. *Id.* at 2:64–67.

Controlled equipment 12 further includes processor 18 having memory 20, and is operatively connected to keypad 16 using connecting cable 22. Ex. 1001, 3:1–3. Memory 20 may be part of processor 18, or a separate element operatively connected to the processor. *Id.* at 3:3–5. Processor 18 is additionally connected to light emitting diodes (LEDs) 24 and to alarm system 26. *Id.* at 3:5–7. Alarm system 26 is configured to generate a visual or audible signal when triggered in an appropriate instance by processor 18. *Id.* at 3:7–10. Memory 20 includes storage of authorization codes 28 and a matrix of equipment status checks 30, for example, of a tamper evident status implicating unsuccessful attempts to enter a proper access code. *Id.* at 3:10–13.

Processor 18 is remotely configurable, and is adapted for regulating operation of controlled equipment 12, receiving the authorization code, storing the authorization code within memory 20, and receiving an access code entered via a selective input at keypad 16. Ex. 1001, 3:21–25. Processor 18 may also be adapted to authorize the operation of controlled

equipment 12 for a predetermined timeframe, i.e., duration, if the entered access code is proper, i.e., matches the authorization code. *Id.* at 3:29–32.

Controlled equipment 12 additionally includes cell modem 34 configured to communicate the authorization code from management source 32 to processor 18. Ex. 1001, 3:44–46. Processor 18 may be additionally adapted to detect unauthorized operation of controlled equipment 12 when operation of the controlled equipment occurs outside the predetermined timeframe. *Id.* at 3:46–49. Additionally, processor 18 may be adapted to communicate to management source 32 using cell modem 34 a signal indicative of the detected unauthorized operation. *Id.* at 3:50–52. Furthermore, management source 32 may also be adapted to remotely shut down the operation of controlled equipment 12 when such unauthorized operation is detected. *Id.* at 3:52–55.

Construction machine 56 may be additionally started by a controlling signal from host computer 45 or cellular telephone 54 directly, thereby providing wireless regulation of the operating construction machine 56 from any remote location. Ex. 1001, 4:48–52.

Figure 4 of the '330 patent is reproduced below:

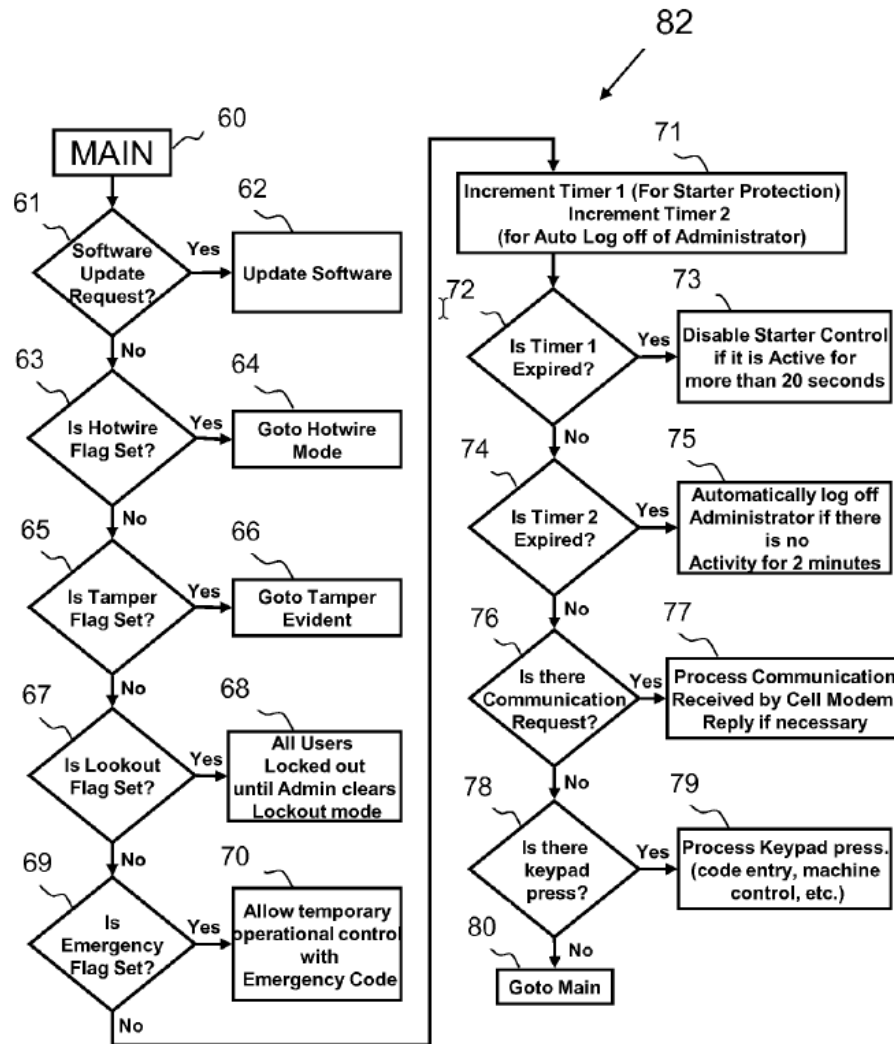


Figure 4 is a flow chart illustrating a logical sequence which may be employed within an algorithm implemented by the system for controlling and monitoring operation of the device shown in Figure 1. Ex. 1001, 2:41–44. At frame 65 of the algorithm, the algorithm checks whether the operator or any unauthorized individual has entered three or more consecutive incorrect access codes, thereby setting a Tamper Flag. *Id.* at 5:17–20. If so, the algorithm transits to a Tamper Evident Mode in frame 66, where LEDs 24, shown in Figure 1, start flashing, and a

notification regarding the unauthorized attempt is provided to host computer 45, as described with respect to Figure 3. *Id.* at 5:20–24.

If a correct access code was entered in frame 66, the Tamper Flag is cleared, LEDs stop flashing, and host computer 45 is notified regarding authorized access. Ex. 1001, 5:25–27. If the Tamper Flag is cleared, the algorithm continues to frame 67, where the software checks whether a Lockout Flag in frame 67 was set by an administrator at construction machine 56, or by an administrator at remote host computer 45. *Id.* at 5:27–31. If the Lockout Flag is set, then the algorithm transits to a Lockout Mode in frame 68, where all users are locked out and are no longer permitted to access and operate construction machine 56 until the Lockout Flag in frame 67 has been cleared by the administrator. *Id.* at 5:31–36.

If the Lockout Flag has not been set, the algorithm continues to frame 69, where the software checks whether an Emergency Flag was set by the administrator. Ex. 1001, 5:36–38. If the Emergency Flag in frame 69 was set by the administrator, then in the next frame 70 construction machine 56 allows for temporary operational control with Emergency Code, or the algorithm transits to frame 71. *Id.* at 5:38–42.

E. Illustrative Claim

Claims 1 and 11 are the independent claims challenged in the Petition. Claim 1, reproduced below, is illustrative of the subject matter:

1. A method of controlling and monitoring operation of a rental machine having a keyless start arrangement configured to activate the machine, the method comprising:

[a] communicating an authorization code via a remote management source to a processor having a memory,

[b] wherein the processor regulates operation of the machine and is operatively connected to the keyless start arrangement configured to activate the machine;

[c] storing the authorization code within the processor memory;

[d] detecting by the processor an entry of an access code made via a selective input;

[e] assessing whether the entered access code matches the authorization code;

[f] authorizing operation of the machine if the entered access code matches the authorization code;

[g] denying authorized operation of the machine if the entered access code does not match the authorization code; and

[h] locking out operation of the machine if the processor detects that the access code was disabled upon completion of the authorized operation of the machine and logging in the actual duration of time the machine was in use;

[i] wherein said authorizing operation of the machine includes starting the machine via the remote management source.

Ex. 1001, 6:10–34 (bracketed matter added). Independent claim 11 is a system claim, reciting structure configured to perform substantially the same steps as recited in claim 1. *See* Ex. 1001, 7:14–42.

F. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–3, 7–13, and 17–20 are unpatentable on the following seven grounds (Pet. 6):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3, 9–11, 13, 19, 20	103(a) ¹	Shibata ² , Kaman ³
7, 8, 17, 18	103(a)	Shibata, Kaman, Chase ⁴
2, 12	103(a)	Shibata, Kaman, Bernosky ⁵
1, 3, 7, 10, 11, 13, 17, 20	103(a)	Chase, Cheung ⁶ , Kaman
2, 12	103(a)	Chase, Cheung, Kaman, Bernosky
9, 19	103(a)	Chase, Cheung, Kaman, Ehrman ⁷
1–3, 7–13, 17–20	103(a)	Harvey ⁸ , Cheung, Kaman

In support of its challenges, Petitioner relies, *inter alia*, on the declaration of Christopher K. Wilson. Ex. 1006.

We provide a brief summary of the prior art relevant to this Final Written Decision, below. We also address Patent Owner’s criticism of Mr. Wilson’s declaration testimony.

¹ The Petition alleges art qualifying under pre-AIA 35 U.S.C. § 102(b) based on priority applications 12/657,130 (filed January 14, 2010), and 61/205,099 (filed January 15, 2009). See Pet. 9; see also Ex. 1001, 1:8–12 (providing priority claim). Patent Owner does not make any contrary representations. The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103. Because, on this record, the ’330 patent has an effective filing date before the effective date of the relevant amendment, the pre-AIA version of § 103 applies. However, our decision would not change regardless of the version of the Patent Act considered.

² US 2003/0137398 A1, pub. July 24, 2003 (Ex. 1007, “Shibata”).

³ US 5,660,246, iss. Aug. 26, 1997 (Ex. 1008, “Kaman”).

⁴ US 2003/0034873 A1, pub. Feb. 20, 2003 (Ex. 1009, “Chase”).

⁵ US 7,009,499 B2, iss. Mar. 7, 2006 (Ex. 1010, “Bernosky”).

⁶ US 4,438,752, iss. Mar. 27, 1984 (Ex. 1011, “Cheung”).

⁷ US 6,898,493 B2, iss. May 24, 2005 (Ex. 1012, “Ehrman”).

⁸ US 2009/0219135 A1, pub. Sept. 3, 2009 (Ex. 1014, “Harvey”).

1. *Shibata*

Shibata is titled “Security System of Construction Machinery” and relates “to a security system for a construction machine provided on a construction machine such as a hydraulic excavator, the security system for preventing theft of the construction machine by permitting operation of the construction machine only when a predetermined password is entered.”

Ex. 1007, code (54), ¶ 1.

Figure 5 of Shibata is reproduced below:

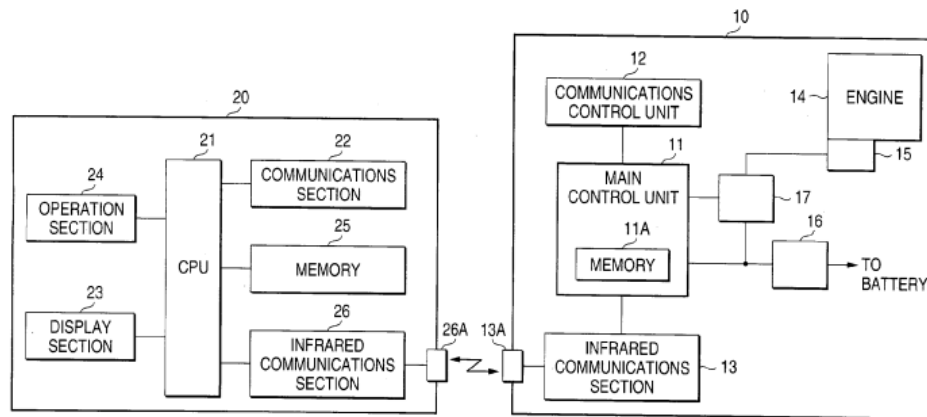


Figure 5 is a block diagram showing a configuration of a control system of a hydraulic excavator and a cell phone. Ex. 1007 ¶ 51. In a third embodiment (relied on by Petitioner), a personal identification number, which is different from a telephone number, is entered to memory 25 of cell phone 20. *Id.* ¶ 112. The operator of hydraulic excavator 10 sets infrared communications available between cell phone 20 owned by the operator, and then main control unit 11 of hydraulic excavator 10 operates engine key switch 16 when starting hydraulic excavator 10. *Id.* ¶ 114. This action causes the personal identification number stored in memory 25 of cell phone 20 to be fetched into main control unit 11 and compared with the personal identification number stored in memory 11a of main control unit 11. *Id.* If both personal identification numbers coincide with each

other, start of engine 14 is permitted. *Id.* Otherwise start of the engine 14 is inhibited. *Id.*

Figure 8 of Shibata is reproduced below:

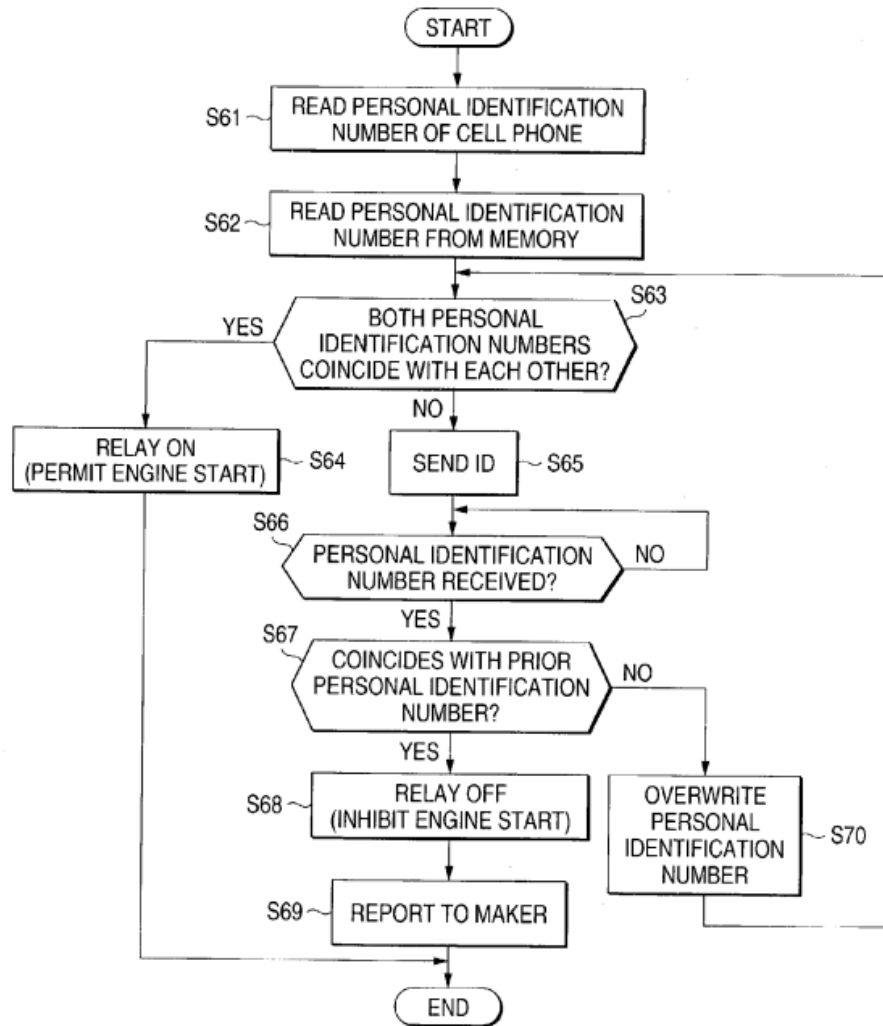


Figure 8 is a flowchart showing a control on a hydraulic excavator in Shibata's third embodiment. Ex. 1007 ¶ 55. Shibata's Step S63 assesses whether the personal identification number fetched from memory 25 of the cell phone coincides with the personal identification number stored in memory 11A of main control unit 11. *Id.* ¶ 123. In the case where these personal identification numbers coincide, start of the engine is permitted in Shibata's Step S64.

In the case where these personal identification numbers do not coincide, Shibata's method proceeds to Step S65 (and Step S66). *See* Ex. 1007, Fig. 8. Shibata discloses that this lack of matching corresponds to either a case where a person not authorized to use the excavator has made an attempt to start the engine or where the personal identification number has been changed (e.g., in the center server). *See id.* ¶¶ 118, 124. In order to determine which case applies, control unit 11 sends the ID number (stored in memory 11A in advance) of the hydraulic excavator 10 from communications control unit 12 to maker 40 and requests sending of the current personal identification number (Step S65). *Id.* ¶ 124. Main control unit 11, receiving a personal identification number sent from center server 41 (Step S66), checks whether the personal identification number received from center server 41 coincides with the personal identification number stored in memory 11A (Step S67). *See id.* ¶ 125. In case the personal identification number received from center server 41 coincides with the personal identification number stored in memory 11A, the personal identification number has not been changed and main control unit 11 inhibits start of engine 14 (Step S68). *Id.* In the event that the personal identification number received from center server 41 does not coincide with the personal identification number stored in memory 11A at Step S67, main control unit 11 determines that the personal identification number has been changed and proceeds to overwrite the personal identification number in memory 25 with the personal identification number fetched from cell phone 20, and proceeds to Steps S63 and S64 to permit start of the engine. *Id.* ¶ 126.

2. *Kaman*

Kaman is titled “Vehicle Access Controller” and relates to “methods of monitoring mobile vehicles and more particularly to methods of collecting operational information of mobile vehicles and securing such vehicles against unauthorized use.” Ex. 1008, code (54), 1:4–7. Kaman discloses access control device 28, which may be any device structured for determining indicia of identity of a prospective vehicle user (e.g., a keyboard, a magnetic card reader, a key card reader, a fingerprint scanner, or a retinal scanner). *Id.* at 6:65–7:2. Where access control device 28 is a keypad or cardreader, the indicia of identity may be an access code. *Id.* at 7:2–4. The central computer compares the indicia of identity with each file of authorized users and, if a match is found, responds with an access grant returned through the wireless data link. *Id.* at 7:16–19.

Kaman discloses that where an unauthorized access is determined (i.e., the vehicle was activated outside of normal working hours) or a card was lost, stolen, or expired, the central computer may download a new set of files identifying authorized users (thereby denying access to unauthorized users using indicia of identity of authorized users). Ex. 1008, 7:44–50. Kaman discloses that where a magnetic card (or keypad access code) is identified as having been lost or stolen, central computer 38 simply denies access. *Id.* at 7:54–56. Kaman discloses that central computer 38 may deny access by simply not responding to the access request transmitted by the vehicle controller 10, or may respond with a lock-out command to an existing vehicle security system. *Id.* at 7:56–60.

3. *Chase*

Chase is titled “Systems and Methods for Controlling Vehicle Access” and relates “generally to systems that provide for the shared-use of

vehicles [and more particularly] to a system that allows one of a plurality of drivers to automatically make a reservation for a car, then . . . controls the access and use of the car, and the return of the car, including billing.”

Ex. 1009, code (54), ¶ 2. Chase discloses that before the start of the reservation, the central resource management reservation system informs the appropriate vehicle-associated access control module of the details of the reservation including the chip card ID of the driver and the start and end time of the reservation. *Id.* ¶ 39. Chase discloses that at the time of the start of the reservation, the driver goes to the specific location and identifies himself by placing the proximity or chip card near the reader. *Id.* ¶ 40. If the driver’s ID matches the stored ID, then the vehicle-associated access control module unlocks the car door, disables the vehicle security system, enables ignition, and informs the server. *See id.* The proximity or chip card is used to lock the car the same way it was used to unlock the car. *Id.*

During the reservation period and beyond, until a different proximity or chip card ID is detected, the vehicle-associated access control module permits the driver’s proximity or chip card to be used to unlock and lock the car. *Id.*

If in step 502 the processor determines that a reservation has not begun, the status of the wireless connection via the wireless modem and antenna to the server is queried (step 506). Ex. 1009 ¶ 59; Fig. 5⁹. If the connection is enabled, the reservation data stored in Board Computer 101 is trusted and the card ID from the proximity card is compared with the stored reservations (step 507). *Id.* If the card ID matches, the processor records the beginning of the vehicle usage for this reservation (step 508). *Id.* The

⁹ Figure 5 includes steps numbered “1,” “2,” . . . “13.” *See* Ex. 1009, Fig. 5. These steps correspond to steps “501,” “502,” . . . “513,” described in Chase. *See id.* ¶¶ 58–60.

system then allows for vehicle usage, in step 504. *Id.* If the card ID does not match, access is refused. *Id.*

If the vehicle-associated access control module is equipped with a keyboard, user interface processor, and display, the driver may create a new reservation by entering desired information via the on-board keyboard.

Ex. 1009 ¶ 60. In certain embodiments, a driver is permitted access to the vehicle without a pre-authorized ID. *Id.* In such a case, the resource management reservation system performs an authorization before allowing vehicle use. *Id.*

4. Cheung

Cheung is titled “Vehicle Ignition System” and is directed to an additional security device within the ignition system which disables the system for illicit use independent of the possible short-circuiting of the ignition switch. Ex. 1011, code (54), 1:18–21.

Figure 1 of Cheung is reproduced below:

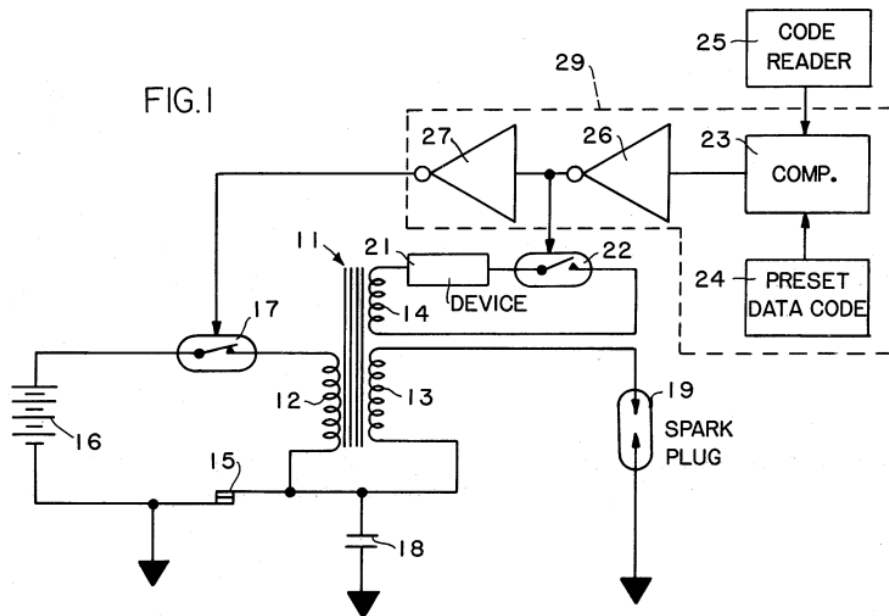


Figure 1 is a schematic drawing of a first embodiment of Cheung, for providing a secure ignition system. Ex. 1011, 1:43–44. The first terminal of the primary winding and one terminal of the conventional secondary winding 13 of the coil 11 are connected together through a capacitor 18 to earth. *Id.* at 1:64–68. The other terminal of the winding 13 provides the high voltage required for the vehicle engine, and in the drawing is shown being connected to a spark plug 19 in the engine. *Id.* at 1:67–2:2.

Additional auxiliary winding 14 is connected across device 21 and switch 22. *Id.* at 2:3–4. Switches 17 and 22 are operable in response to electrical signals, and can comprise a triac, SCR, or any suitable semiconductor switch. *Id.* at 2:4–7. The electrical signal to actuate the switches is provided by comparator 23, which is fed with a signal from preset data coding device 24 and compares this with the output of code reader 25 into which the intending user of the vehicle inserts a code. *Id.* at 2:7–11. If the inserted code is correct, comparator 23 produces an electrical signal which is fed through inverter 26 to cause switch 22 to open and through further inverter 27 to cause switch 17 to close. *Id.* at 2:11–16. When comparator 23 produces the electrical signal, battery 16 energizes the primary winding of the coil, and additional auxiliary winding 14 produces no effect on coil 11 since switch 22 is open. *Id.* at 2:16–20. The power from winding 12 is therefore transferred to secondary winding 13 and spark plug 19. *Id.* at 2:20–22. However, when the correct code is not fed into reader 25, comparator 23 does not produce an electrical signal and switch 22 remains closed and switch 17 remains open. *Id.* at 2:22–26.

5. *Mr. Wilson's Declaration*

In Mr. Wilson's Declaration, he "consider[s] whether the references listed below, alone or in combination, disclose or suggest the features recited

in the” Challenged Claims. Ex. 1006 ¶ 1. Patent Owner argues that “the Board should find that Petitioner’s expert’s testimony is not ‘persuasive or helpful as it repeats the Petitioner’s arguments and offers little or no elaboration.’” PO Resp. 2 (quoting non-precedential decision in *InfoBionic, Inc. v. Braemer Mfg., LLC*, IPR2015-01704, Paper 11 at 6 (PTAB Feb. 16, 2016), and citing 37 C.F.R. § 42.65(a) and the non-precedential decision in *Kinetic Techs., Inc. v. Skyworks Sols., Inc.*, IPR2014-00529, Paper 8 at 15 (PTAB Sept. 23, 2014)). Patent Owner argues that “Petitioner’s expert’s report parrots Petitioner’s brief verbatim across practically all of the grounds. . . . The Board should afford Petitioner’s expert’s testimony no weight as it is not credible.” *Id.*

Petitioner replies that “[t]he Petition shares similarities with Mr. Wilson’s testimony because it is based, properly, on the knowledge and opinions expressed in Mr. Wilson’s expert declaration.” Pet. Reply 5.

We agree with Patent Owner that expert testimony that closely mirrors the language in a petition, without more, may provide little help to the Board as fact finder, because the expert fails to fill his or her role to help us “understand the evidence or [] determine a fact in issue.” See Fed. R. Evid. 702(a). Often, we are left with conclusory testimony with little or no supporting evidence. This type of testimony, however, is not necessarily deficient or entitled to no weight. As Petitioner notes, it may be the case that the expert’s testimony serves as the basis for language in a petition, and may include non-conclusory opinions.

As such, we evaluate the specific testimony of an expert to determine the amount of weight attributable to that testimony, based on the support provided for the testimony. So, some testimony may be entitled to greater weight than other testimony, based on the supporting evidence in the record.

II. ANALYSIS

A. *Legal Standards*

In *inter partes* reviews, a petitioner bears the burden of proving unpatentability of the challenged claims, and the burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail in this proceeding, Petitioner must support its challenge by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d) (2021). Accordingly, all of our findings and conclusions are based on a preponderance of the evidence standard.

Petitioner’s asserted grounds of unpatentability are based on obviousness under 35 U.S.C. § 103(a).

Section 103(a) forbids issuance of a patent when “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.”

KSR Int’l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007). “[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result.” *Id.* at 416 (citing *United States v. Adams*, 383 U.S. 39, 50–51 (1966)). The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and

(4) objective evidence of non-obviousness¹⁰. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

What prior art references teach or suggest, and whether a skilled artisan would have been motivated to combine the references, are questions of fact. *In re Kahn*, 441 F.3d 977, 985 (Fed. Cir. 2006). “[O]bviousness must be determined in light of all the facts, and . . . a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine” teachings from multiple references. *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006).

B. Level of Ordinary Skill in the Art

The level of skill in the art is “a prism or lens” through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). The person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors that may be considered in determining the level of ordinary skill in the art include, but are not limited to, the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* In a given case, one or more factors may predominate. *Id.*

Petitioner contends that a person of ordinary skill in the art at the relevant time would have had at least a bachelor’s degree in technology such as mechanical engineering, physics, electrical engineering, computer science

¹⁰ Neither party directs us to any objective evidence of non-obviousness in the record.

or a similar technical field, with at least three years of relevant product design experience, including design of remote control or remote monitoring systems, where an increase in experience could compensate for less education. Pet. 15 (citing Ex. 1006 ¶ 44).

Patent Owner states that it does not necessarily agree that three years of design experience including remote control or remote monitoring systems is a requirement to be a person of ordinary skill in the art but argues that the distinction is not determinative of the issues raised in the Petition. PO Resp. 6.

We adopt Petitioner’s proposed definition, basing our decision on our review of the ’330 patent, the prior art of record, and Mr. Wilson’s testimony. See Ex. 1006 ¶ 44. We agree with Patent Owner, however, that the level of experience is not determinative of the dispositive issues in this proceeding.

C. Claim Construction

We construe each claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). Under this standard, claim terms are generally given their plain and ordinary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*).

Petitioner proposes constructions of the term “lock out,” as variously used, i.e., “lock out,” “lock-out,” “locking out,” and “locking-out.” Pet. 16. Patent Owner does not disagree with Petitioner’s proposed constructions, and does not propose construction of any other terms. PO Resp. 6. We

construe “lock out” and address certain other terms as well that are central to the resolution of the Petition. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

1. “*lock out*”; “*lock-out*”; “*locking out*”; “*locking-out*”

Petitioner requests construction of the term “lock out” as “not allowing any user to access and/or operate the machine.” Pet. 16. Petitioner argues that this is the ordinary meaning of the term and is further consistent with the Specification, which discloses that all users are locked out in a Lockout Mode. *Id.* (citing Ex. 1001, 5:31–36).

Patent Owner agrees that the plain and ordinary meaning applies, but disagrees with Petitioner’s proposed construction of “not allowing any user to access and/or operate the machine.” PO Resp. 6. Patent Owner does not provide an alternate construction, but instead argues that the Petitioner fails to demonstrate unpatentability under its proposed construction. *See id.*

In our Institution Decision, we preliminarily construed the “locking out” terms to encompass locking out operation for all users. Inst. Dec. 22. We analyze the construction below.

We start with the words of the claim. *Phillips*, 415 F.3d at 1314 (“[T]he context in which a term is used in the [claim at issue] can be highly instructive.”). Claim 1 recites, in relevant part, the step of “locking out operation of the machine if the processor detects that the access code was disabled upon completion of the authorized operation of the machine.” Ex. 1001, 6:28–30. The words of this step make clear that what is locked out is *operation* of the machine, rather than access and operation as

Petitioner proposes. The words of the claim also make clear that this locking out takes place after completion of the authorized operation and disabling of the access code.

Also, this step is distinct from the step of “denying authorized operation of the machine if the entered access code does not match the authorization code” recited earlier in claim 1. *See id.* at 6:26–27. As such, “locking out” means more than just denying operation of the machine to any one user that has entered an invalid access code.

“[T]he specification ‘is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.’” *Phillips*, 415 F.3d at 1315. The Specification discusses locking out in the context of a Lockout Flag, which is part of the logical sequence of steps illustrated in Figure 4. *See Ex. 1001*, 2:41–44, 5:3–36. Specifically, the Specification describes that

the software checks whether a Lockout Flag in frame 67 was set by an administrator at the construction machine 56, or by an administrator at the remote host computer 45. If the Lockout Flag is set, then the algorithm transits to a Lockout Mode in the frame 68, where all users are locked out and are no longer permitted to access and operate construction machine 56 until the Lockout Flag in frame 67 has been cleared by the administrator.

Id. at 5:29–36. In this sole example, “locking out” prevents all users from operating the machine.

Neither party directs us to anything in the prosecution history that would inform our construction of the “locking out” terms.

In the parallel litigation, the district court construed the term to be limited to locking out operation (and not access), and locking one or more users (but not only all users). *See Ex. 3002*, 5–9. That is, the district court provides a construction of the term that is broader in scope than the

construction proposed by Petitioner, as it does not affect all users and does not restrict “access” to the machine. *See, e.g., id.* at 8 (“The plain and ordinary meaning of the term is therefore less restrictive than [Petitioner] contends.”).

When part of the record of an *inter partes* review proceeding, we must consider a district court’s constructions. *See* 37 C.F.R. § 42.100(b) (“Any prior claim construction determination concerning a term of the claim in a civil action . . . that is timely made of record in the *inter partes* review proceeding will be considered.”). We, however, maintain our construction from the Institution Decision, and particularly, the requirement that all users are locked out, as it closely aligns with Petitioner’s proposed construction, and is consistent with the language of the claims themselves and the Specification. We do not fully adopt Petitioner’s proposed construction, however, as we do not agree that “access” to the machine is locked out, based on the express language of the claim.

To summarize, we construe the “locking out” terms to locking out all users from operating the machine.

2. “*wherein said authorizing operation of the machine includes starting the machine via the remote management source*” (claim 1) and “*wherein the remote management source is additionally configured to . . . start the machine if the entered access code matches the authorization code*” (claim 11)

The independent claims recite the phrases “wherein said authorizing operation of the machine includes starting the machine via the remote management source” (claim 1) and “wherein the remote management source is additionally configured to . . . start the machine if the entered access code matches the authorization code” (claim 11). Ex. 1001, 6:33–34, 7:30–35. In the Institution Decision the Board, *sua sponte*, adopted a construction of

these phrases “to require that the remote management source actually starts the machine or be configured to start the machine, and not merely be capable of enabling the machine to start.” Inst. Dec. 23; *cf. Praxair Distrib., Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024, 1034 (Fed. Cir. 2018) (rejecting argument that Board violated patent owner’s “procedural rights by adopting a claim construction that neither party proposed”). We based our construction on the actual words of the claim. *See id.*; *Phillips*, 415 F.3d at 1314 (“[T]he context in which a term is used in the [claim at issue] can be highly instructive.”).

We maintain our construction, which neither party challenges. *See* PO Resp. 6; Pet. Reply 8. Again, as we concluded in our Institution Decision, the express language of the claims requires “*starting the machine* via the remote management source” or “the remote management source . . . configured to . . . *start the machine.*” Ex. 1001, 6:33–34, 7:30–35. Nothing in the express language of these phrases indicates that merely enabling the machine to be started by a user would be encompassed in this action.

Our construction is also consistent with the Specification. In one disclosed embodiment, the Specification describes that “construction machine 56 may be additionally started by a controlling signal from the host computer 45 or cellular telephone 54 directly, thereby providing wireless regulation of the operating construction machine 56 from any remote location.” Ex. 1001, 4:48–52; *see also id.* at 4:14–17 (describing that, in a rental company embodiment, host computer 45 is the “management source”). Consistent with our construction, construction machine 56 is started remotely, from a host computer that is the remote management source.

Our construction is also consistent with the prosecution history. In an interview with the examiner, the applicant characterized the subject matter of these limitations as “starting the machine remotely.” *See* Ex. 1002, 65; *see also id.* at 78 (describing the telephonic interview with the examiner, and stating that “an agreement was reached that the presently cited references do not disclose or suggest dependent claim limitation[] ‘authorizing operation of the machine includes starting the machine via the remote management source.’”).

The district court provided a similar construction for these phrases: “wherein said authorizing operation of the machine includes the remote management source starting the machine.” Ex. 3002, 20–21.

For the above reasons, we construe the phrases “wherein said authorizing operation of the machine includes starting the machine via the remote management source” (claim 1) and “wherein the remote management source is additionally configured to . . . start the machine if the entered access code matches the authorization code” (claim 11) to require the remote management source to actually start the engine of the machine if the entered access code matches the authorization code, rather than merely allowing the machine to be started.

3. *The “authorizing operation,” “denying authorized operation,” and locking out operation” steps of claim 1*

Claim 1 recites, in relevant part,

“authorizing operation of the machine if the entered access code matches the authorization code” [(“authorizing operation” step)];

“denying authorized operation of the machine if the entered access code does not match the authorization code” [(“denying authorized operation” step)]; and

“locking out operation of the machine if the processor detects that the access code was disabled upon completion of the authorized operation of the machine and logging in the actual duration of time the machine was in use” [(“locking out operation” step)].

Ex. 1001, 6:24–32

In our Institution Decision, we invited the parties to brief whether these conditional steps must be satisfied by the prior art. In particular, we noted that in *Ex parte Schulhauser*, Appeal No. 2013-007847 (PTAB Apr. 28, 2016) (precedential), the Board held that where a method claim includes several conditional steps, the associated action in a conditional step does not need to be performed if the condition precedent recited in each step is not met. *See Schulhauser*, at 6–10; *see also Microsoft Corp. v. Uniloc 2017 LLC*, IPR2019-01116, Paper 22 at 49–52 (PTAB Oct. 26, 2020) (applying *Schulhauser* under the *Phillips* standard and concluding that “*Schulhauser*, on its face, does not limit its application to circumstances where the broadest reasonable interpretation rule applies”) (Final Written Decision).

Patent Owner did not address these terms. PO Resp. 6. “Petitioner believes the claim is properly interpreted to require the presence of all three limitations.” Pet. Reply 10. Petitioner explains that “[a] logical reading of the claim is that the first two phrases provide alternatives depending on whether the entered access code matches, or does not match, an authorization code.” *Id.* at 10. Petitioner adds that “[t]he phrase requires the possibility of a third option – that the entered access code may have been disabled – in which case the first two possibilities (matching or not matching an authorization code) are, in essence, superseded by locking out operation of the machine.” *Id.* at 10–11.

On the complete trial record, we evaluate claim 1 as requiring the “authorizing operation,” “denying authorized operation,” and “locking out operation” steps. We agree with Petitioner’s characterization of the claim language, where the “locking out” step is distinct from the “authorizing operation” and “denying authorized operation” steps. The “locking out” step looks to whether an access code was disabled because of the completion of an authorized operation. This step is not dependent on the actions of the “authorizing operation” and “denying authorized operation” steps, which are based on whether an entered access code matches a stored authorization code.

D. Ground 1: Obviousness of Claims 1, 3, 9–11, 13, 19, and 20 over Shibata and Kaman

Petitioner contends that claims 1, 3, 9–11, 13, 19, and 20 would have been obvious over Shibata and Kaman. Pet. 17–36.

1. Independent Claim 1

Claim 1 recites, in relevant part, the step of “locking out operation of the machine if the processor detects that the access code was disabled upon completion of the authorized operation of the machine and logging in the actual duration of time the machine was in use.” Ex. 1001, 6:28–32 (the “locking out operation” step of claim 1).

Petitioner contends that Shibata teaches that, as part of its authorization process, Shibata’s processor reports that a disabled access code is used. Pet. 25 (referencing Ex. 1007 ¶¶ 124–125). Petitioner contends that a person having ordinary skill in the art “would understand that the unauthorized operator nevertheless had a cell phone compatible with Shibata’s system because it communicated with, and sent its PIN to, the control unit 11.” *Id.* Petitioner argues that the unauthorized operator was,

therefore, either trying to access the machine prior to or after a reservation period. And, in this later case, the user's PIN was disabled upon completion of the authorized operation. *Id.* (referencing Ex. 1006 ¶ 66).

We understand that Petitioner contends that Shibata teaches the “locking out operation” step of claim 1 by disabling a user's PIN upon completion of authorized operation—a “simple denial of authorization.” Pet. 25. We find, on the complete record, that Petitioner does not demonstrate, by a preponderance of the evidence, that Shibata's denial of operation meets the “locking out operation” step. Even if we accept Petitioner's premise that authorization was denied because authorized operations have been completed, Petitioner does not provide persuasive arguments and evidence to support a finding that operations are “locked out,” such that no other user may operate the machine. Indeed, as Petitioner characterizes this teaching, it is a simple denial of authorization, not a locking out of operations to all users. As Patent Owner argues, denying authorization is encompassed by another step of claim 1. *See* PO Resp. 11–12; Ex. 1001, 6:26–27 (reciting the step of “denying authorized operation of the machine if the entered access code does not match the authorization code”).

Alternatively, Petitioner contends that Kaman discloses an embodiment in which its central computer 38 may respond with a lock-out command to an existing vehicle security system. Pet. 26 (referencing Ex. 1008, 7:54–60). Petitioner contends that, like Shibata, Kaman's system is for securing vehicles such as “heavy equipment” against unauthorized use. *Id.* (referencing Ex. 1008, 1:5–8, 20–22). Petitioner contends that Kaman discloses an embodiment in which its central computer 38, analogous to Shibata's server 41, sends a lock-out command to a vehicle's system to lock-

out operation of a vehicle when someone attempts unauthorized use, and the “central computer 38 . . . may respond with a lock-out command to an existing vehicle security system.” *Id.* (referencing Ex. 1008, 7:54–60).

Petitioner contends that a person of ordinary skill would have found it obvious to include Kaman’s lock-out feature in Shibata’s third embodiment at or after Step 69 (“Report to Maker [40, 41]”) where the machine’s control unit 11 informs server 41 of the attempted unauthorized access. *Id.* Petitioner contends that a person of ordinary skill would have been motivated, and would have had a reasonable expectation of success, to include a response from the server 41 that locks-out operation of the machine 40 because of the unauthorized access that is presently being attempted when the location or type of machine has a high risk of theft. Pet. 26 (referencing Ex. 1006 ¶ 68).

Mr. Wilson’s testimony largely mirrors Petitioner’s contentions within the Petition. Mr. Wilson testifies that a person having ordinary skill in the art would have been motivated to lock out operation of the machine, such as by removing all access codes from the machine, because of an unauthorized access attempt. Ex. 1006 ¶ 68. Mr. Wilson declares that this motivation may result from the machine being in a high theft area or if there has been “password ‘leakage’ as suggested by Shibata, or if a threshold number or rate of unauthorized access attempts are reported.” *Id.* (referencing Ex. 1007 ¶¶ 2, 8).

Patent Owner argues that this embodiment of Kaman addresses the situation where a key card has been lost or stolen and argues that “it does not make sense” for Kaman to lock out users other than the user who lost the key card. PO Resp. 12. Patent Owner argues that the purpose of Kaman is to detect the indicia of identity of a specific user, and Petitioner does not

argue that Kaman discloses that users share a password or access card. *Id.* 12–13 (referencing Ex. 1008, 2:14–29, 6:64–7:6).

Patent Owner argues that Petitioner does not “argue that Shibata or Kaman disclose locking out all users.” PO Resp. 13. Patent Owner argues that Petitioner’s motivation to combine Kaman’s teachings with Shibata—the “unauthorized access”—is user specific. *Id.* Patent Owner concludes that “neither the cited references nor Petitioner provides a reason to lock out all users, as is required by Petitioner’s construction.” *Id.*

Patent Owner also argues that Mr. Wilson testifies that “perhaps” a person having ordinary skill in the art would remove all access codes, and that support for this opinion “is found nowhere in Kaman or Shibata, nor supported by other evidence.” PO Resp. 13. With respect to Mr. Wilson’s testimony regarding password leakage, number of unauthorized access attempts, or for a machine located in a high risk of theft area as motivating facts, Patent Owner argues that these factors are inconsistent with Shibata. *Id.* at 13–14. Patent Owner argues that this alleged motivation to combine Shibata and Kaman is “nonsense,” as “Shibata requires that a user download dedicated software onto their cell phone.” *Id.* at 14 (referencing Ex. 1007 ¶ 115).

Patent Owner adds that Petitioner argues that a person having ordinary skill in the art “would understand that the unauthorized operator nevertheless had a cell phone comparable with Shibata’s system because it communicated with, and sent its PIN to, the control unit 11.” PO Resp. 14 (quoting Pet. 25). That is, Petitioner argues that the unauthorized user is an otherwise authorized user who is trying to access the machine before or after the authorized time. *Id.* Patent Owner argues that theft is not an issue in Shibata’s system. *Id.*

Patent Owner also argues that Petitioner's reasoning for combining the teachings of Shibata and Kaman is contrary to Shibata's express disclosure. PO Resp. 14. Patent Owner argues that Shibata's system of using a PIN stored in a cell phone avoids the risk of password leakage or the loss of a magnetic card, such as in Kaman. *Id.* (referencing Ex. 1007 ¶¶ 1, 2, 8–12, 33, 36, 82, 108, 115, 134). Patent Owner concludes that:

There is, therefore, no reason for a [person having ordinary skill in the art] to combine Shibata with Kaman's passcode and magnetic card system because (i) Shibata relies on cell phones with dedicated software specific to that system, instead of passcodes and magnetic cards and (ii) purportedly unauthorized use in Shibata (an expired but previously recognized PIN) is distinct from the alleged unauthorized use in Kaman (theft of a magnetic card or keypad access code, which is not possible in Shibata's system).

Id. at 15. Patent Owner adds that “rather than implementing a lock out procedure, the Shibata system dealt with a password security concern by requiring a PIN from the maker be stored on a cell phone.” *Id.*

As an initial matter, we agree that neither Shibata nor Kaman discloses locking out all users if the processor detects that the access code was disabled upon completion of the authorized operation of the machine as required by claim 1. As Petitioner recognizes, Shibata simply denies authorization to the user with that access code. *See* Pet. 25; *see also* Ex. 1007 ¶ 125 (“[M]ain control unit 11 determines that unmatched between [PINs] in Step S63 is due to the fact that a person not authorized to use the hydraulic excavator has made an attempt to start the engine 14. Then the main control unit 11 inhibits start of the engine 14 (Step S68) . . .”). Kaman is directed at verifying an indicium of identity to determine if a

specific user is an authorized user. *See, e.g.*, Ex. 1008, code 57, 7:7–60 (describing processes for authorizing a user).

We recognize that Kaman uses the term “lock-out command.” *See* Ex. 1008, 7:59. This term is used, however, with respect to a single user, not all users. As Kaman describes, when a magnetic card or access code (exemplary indicia of identity) is identified as lost or stolen, then central computer 38 may either not respond to an access request using the lost or stolen indicium, or respond to the access request with a lock-out command. *Id.* at 7:52–60. That is, when access is controlled by a remote, central computer, that computer can lock out a specific user who attempts access with lost or stolen indicia of identity. We discern nothing in this disclosure, nor does Petitioner persuasively explain, that Kaman’s use of the term “lock-out” would lock out all users, as required by Petitioner’s construction. *See* PO Resp. 12–13 (“[I]t does not make sense that Kaman would lock out all users following the loss or theft of a single magnetic card or keypad access code; no, at most only that specific card or code would be ‘locked out’ while others remained active.”).

Similarly, when access is controlled locally with Kaman’s system, the central computer periodically checks the list of users from vehicle access controller 10. “Where an unauthorized access is determined (i.e., the vehicle was activated outside of normal working hours) or a card was lost, stolen, or expired, the central computer may download a new set of files identifying authorized users (thereby denying access to unauthorized users using indicia of identity of authorized users).” Ex. 1008, 7:45–51. In this case, authorized users may still access the machine. As such, to the extent that Petitioner argues that Kaman teaches locking out all users, we find, on review of the complete record, that Petitioner fails to prove, by a

preponderance of the evidence, that all users are locked out by Kaman's "lock-out" command.

To the extent that Petitioner argues that a person having ordinary skill in the art would have had reason to modify the combined teachings of Shibata and Kaman to lock-out all users, we analyze Petitioner's reasons for modifying Shibata with Kaman. *See, e.g.*, Ex. 1006 ¶ 68 (testifying that a person having ordinary skill in the art could have, "perhaps simply remove[d] all access codes from the machine"). We have weighed the evidence in the complete record, as informed by the parties' arguments, and find that Petitioner has not demonstrated, by a preponderance of the evidence, that a person having ordinary skill in the art would have had reason to modify Shibata with Kaman to lock out all users.

The primary reason that Petitioner provides for the proposed modification is "when . . . the location or type of machine 10 has a high risk of theft." Pet. 26. We agree with Patent Owner, however, that Shibata's system of restricting access to a user with a cell phone containing specialized software to access the machine ameliorates any risk of theft from an unauthorized user. *See* PO Resp. 14. As Shibata discloses, its security system "prevents possible theft of a construction machine." Ex. 1007, code 57. Shibata explains that its invention overcomes the deficiencies of security systems that address the problem of "frequent theft of a construction machine." *Id.* ¶¶ 2–11. Indeed, as Petitioner recognizes, a person having ordinary skill in the art would have understood from Shibata's teaching that an "unauthorized operator nevertheless had a cell phone compatible with Shibata's system because it communicated with, and sent its PIN to, the control unit 11." Pet. 25. As such, "the (unauthorized) operator either was attempting access before their reserved date/time, or was previously

authorized to use the vehicle but their reservation period had ended such that the authorized PIN stored in server 41 (if any) identified a different operator.” *Id.* In other words, Shibata’s unauthorized users were those who were otherwise authorized but attempting to operate the machine outside their authorized time. Even if a skilled artisan were concerned with preventing theft, Petitioner has not shown the claimed approach (locking out all users) was taught by the prior art. And in light of the prior art’s deficiency, Petitioner has not adequately justified modifying the prior art’s approach to include locking out all users.

We also give little weight to Mr. Wilson’s testimony. With respect to his testimony that, perhaps, a person having ordinary skill in the art would have “simply remove[d] all access codes from the machine,” we note first that this specific modification does not appear in the Petition. *Compare* Pet. 25–36, *with* Ex. 1006 ¶ 68. Also, this testimony is directed to what a person having ordinary skill in the art could have done (“perhaps”), not what a person having ordinary skill in the art would have been motivated to do. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have* made but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”). Also, this evidence is entitled to little weight as Mr. Wilson does not provide support for this modification, particularly in light of Kaman’s teachings of removing unauthorized users but maintaining a list of authorized users when unauthorized access is detected. *See* Ex. 1008, 7:45–51; *see also* 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

With respect to Mr. Wilson’s reliance on “password leakage” as a motivating factor, we agree with Patent Owner that Shibata already addresses this concern by locking out the otherwise-authorized user rather than locking out all users. See Ex. 1006 ¶ 68 (testifying that “there may have been password ‘leakage’ as suggested by Shibata”); PO Resp. 14. Shibata discloses that its security system “is not cumbersome or confusing to an operator but convenient *as well as prevents leakage of a password* and ensures a higher level of security.” Ex. 1007 ¶ 134 (emphasis added).

In its Reply, Petitioner argues that Patent Owner “merely repeats, *verbatim*, the same attorney arguments included in PO’s Preliminary Response which the Board considered prior to its [Institution] Decision.” Pet. Reply 15. Petitioner argues that Patent Owner “has submitted no additional evidence, so the only evidence-supported finding is that these claim limitations would have been obvious based on the combination of Shibata and Kaman as set forth in the Petition.” *Id.* at 16. We find this argument unpersuasive. Tellingly, Petitioner quotes our Institution Decision saying that “Petitioner has shown a reasonable likelihood that a person of ordinary skill would have sought to incorporate Kaman’s theft control system [in Shibata’s system] to guard against theft,” and that “it is a reasonable position in view of the prior art that a person of ordinary skill in dealing with rental issues would have combined the devices of Shibata and Kaman to arrive at the claimed limitation.” *Id.* at 16. These statements reflect the standard that applies at the institution stage—whether the information in the Petition shows there is a reasonable likelihood that a challenged claim is unpatentable. See 35 U.S.C. § 314(a). At the final written decision stage, the burden is higher—Petitioner must demonstrate unpatentability by a preponderance of the evidence. See 35 U.S.C. § 316(e)

(“In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.”). Here, we have reviewed Petitioner’s argument and supporting evidence anew, against the burden required at this stage of the proceeding, and find that Petitioner’s argument is not supported by a preponderance of the evidence.

Accordingly, based on weighing the evidence of record, including the disclosures in the prior art references and Mr. Wilson’s testimony, we find that Petitioner fails to demonstrate, by a preponderance of the evidence, that a person having ordinary skill in the art would have had reason to modify Shibata with Kaman’s teachings to arrive at a security system that locks out operation of the machine for all users if the processor detects that the access code was disabled upon completion of the authorized operation of the machine as required by claim 1.

For these reasons, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claim 1 is unpatentable under 35 U.S.C. § 103(a) over Shibata and Kaman.

2. Independent Claim 11

Independent claim 11 contains similar language and requirements as independent claim 1. For the “lock out operations” subject matter of claim 11, Petitioner relies on its contentions with respect to the lock out operations step of claim 1. See Pet. 35. Accordingly, for the reasons discussed above in connection with our analysis of claim 1, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claim 11 is unpatentable under 35 U.S.C. § 103(a) over Shibata and Kaman.

3. *Analysis of Claims 3, 9, 10, 13, 19, and 20*

Dependent claims 3, 9, and 10 depend directly from claim 1, and claims 13, 19, and 20 depend directly from claim 11. For the reasons discussed above in connection with our analysis of independent claims 1 and 11, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claims 3, 9, 10, 13, 19, and 20 are unpatentable under 35 U.S.C. § 103(a) over Shibata and Kaman.

E. Grounds 2 and 3: Obviousness of Dependent Claims 7, 8, 17, and 18 over Shibata, Kaman, and Chase and Dependent Claims 2 and 12 over Shibata, Kaman, and Bernosky

Petitioner contends that dependent claims 7, 8, 17, and 18 would have been obvious over Shibata, Kaman, and Chase (Ground 2), and dependent claims 2 and 12 would have been obvious over Shibata, Kaman, and Bernosky (Ground 3). Pet. 36–42. Under these grounds, Petitioner does not rely on either Chase or Bernosky to remedy the deficiency in the combination of Shibata and Kaman we identify above in our analysis of independent claims 1 and 11, from which these dependent claims depend. *See id.*; *see, e.g., id.* at 39–40 (relying on the analysis of the “locking out operation” step of claim 1 for claim 8, which also recites “locking out operation”).

Accordingly, for the reasons discussed above in connection with our analysis of independent claims 1 and 11, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claims 7, 8, 17, and 18 are unpatentable under 35 U.S.C. § 103(a) over Shibata, Kaman, and Chase and that claims 2 and 12 are unpatentable under 35 U.S.C. § 103(a) over Shibata, Kaman, and Bernosky.

F. Ground 4: Obviousness of Claims 1, 3, 7, 10, 11, 13, 17, and 20 over Chase, Cheung, and Kaman

Petitioner contends that claims 1, 3, 7, 10, 11, 13, 17, and 20 would have been obvious over Chase, Cheung, and Kaman (Ground 3). Pet. 6, 42–70.

1. Independent Claim 1

Claim 1 recites, in relevant part, “wherein said authorizing operation of the machine includes starting the machine via the remote management source.” Ex. 1001, 6:33–34 (the “starting” step of claim 1).

Petitioner contends that if Chase’s driver arrives at the vehicle before his or her reservation starts, the vehicle’s processor communicates to the management server before authorizing the driver to operate the vehicle. Pet. 60–61 (citing Ex. 1009 ¶¶ 59–60). The server can then authorize the vehicle to be started. *Id.* at 61. In this scenario, Petitioner relies on Cheung to start the vehicle: “e.g., Cheung’s transformer fires the spark plug.” *See id.* at 61 (citing Ex. 1006 ¶ 142).

Petitioner appears to be referring back to its assertions with respect to Cheung for the “processor regulating operations” limitation of claim 1¹¹, in which Petitioner contends that Cheung’s comparator 23 produces an electrical signal that causes switch 22 to open and switch 17 to close, resulting in power to spark plug 19 and ignition of the vehicle’s engine. Pet. 50–51 (citing Ex. 1011, 2:3–26, 3:20–23, Fig. 1; Ex. 1006 ¶ 125).

¹¹ The “processor regulating operation” limitation of claim 1 recites, “wherein the processor regulates operation of the machine and is operatively connected to the keyless start arrangement configured to activate the machine.” Ex. 1001, 6:15–17.

The cited portions of Cheung disclose sending power to secondary winding 13 and spark plug 19 (Ex. 1011, 2:6–26) and further disclose that “[a]though the conventional firing system for an internal combustion engine has been shown with mechanical contacts 15, the invention can clearly be applied to other ignition systems, including electronic systems” (*id.* at 3:20–23). Cheung elsewhere discloses that “[o]ne terminal of the primary winding 12 is connected through a pair of contacts 15 of the distributor to the earthed terminal of the battery 16.” *Id.* at 1:55–58. Thus, Cheung discloses that other ignition systems may be used and that current may be sent to contacts 15 of the distributor in addition to spark plug 19.

Although Cheung discloses sending energy to spark plug 19 and to contacts 15 of the distributor, the complete record does not support a finding, by a preponderance of the evidence, that Cheung discloses *starting* the engine, based only on powering the spark plug and contacts of the distributor. These conditions by themselves are not sufficient to start the engine. These conditions may *allow* the engine to start, but they do not, themselves, cause the engine to start. A starter motor must initiate the engine to start. *See, e.g.*, Ex. 1007 ¶ 102 (describing the typical operation of an engine, such as engine 14, where, for example, “[w]hen the relay 17 is ON, the starter motor 15 is driven through operation of the key switch 16, thus starting the engine 14”); Ex. 1001, 2:57–60 (“The keyless ignition system includes a keypad 16, shown in F[igure] 1, operatively connected to such various electronically and/or mechanically interconnected devices as a *starter*, coils, sparkplugs, and sensors (not shown) *for starting engine 14.*” (emphasis added)), 2:61–64 (“In operation, during starting of engine 14, an access code selectively entered via keypad 16 *activates the engine through*

operation of the starter, and facilitates function of the controlled equipment 12.” (emphasis added)).

Mr. Wilson’s declaration closely tracks the Petition and does not provide an additional basis to conclude that the engine would start when Cheung sends energy to spark plug 19 and to contacts 15 of the distributor. See Ex. 1006 ¶¶ 125, 142. Mr. Wilson testifies that the result of a user entering a correct code into Cheung’s system is “power to the spark plug 19 and ignition of the vehicle’s engine (although other ignition systems can be used).” Ex. 1006 ¶ 125 (citing Ex. 1011, 2:3–26; 3:20–23); see *id.* ¶ 142 (stating that “Cheung’s transformer fires the spark plug”). We give this testimony little weight, as it is not supported by Cheung. As we have already discussed, we discern nowhere in Cheung, including the citations provided by Mr. Wilson, that Cheung discloses that its system “ignit[es] . . . the vehicle’s engine” or “fires the spark plug,” that is, starts the engine. Cheung’s disclosure states only that power is transferred to winding 13 and spark plug 19, allowing it to be started. See Ex. 1011, 2:20–22. Mr. Wilson fails to explain adequately why the description in Cheung discloses actually starting the machine.

In its Reply, Petitioner argues that Cheung is directed to a vehicle ignition system. Pet. Reply 17. Petitioner argues that “Cheung . . . discloses that the singular act of powering the ignition coil ‘energize[s] the vehicle engine.’” *Id.* at 18 (referencing Ex. 1011, 1:5–9). Petitioner argues that Cheung describes that, in its system, “[i]nstead of closing [the] switch [that energizes the ignition coil] using a physical key, one embodiment in Cheung closes the switch using a ‘code reader 25 into which the intending user of the vehicle inserts a code.’” *Id.* (referencing Ex. 1011, 2:11–12). Petitioner adds that, “[i]f the code (access code) is correct (matches an authorization

code) then . . . switch 22 opens, switch 17 closes, and ‘power from the winding 12 is therefore transferred to the secondary winding 13 and the spark plug 19.’” *Id.* (referencing Ex. 1011, 2:20–22, Fig. 1).

Petitioner concludes:

In short, although there might be things that Cheung does not discuss that may be necessary to start the engine, such as fuel availability, it is clear that Cheung’s disclosure intends for the vehicle engine to actually start upon closure of switch 17 and the opening of switch 22, i.e., upon ignition of the spark plug 19 and electrification of contacts 15 of the distributor.

Pet. Reply 18.

Upon review of the complete trial record, we find Petitioner’s contention with respect to Cheung disclosing the subject matter of the “processor regulating operations” limitation of claim 1 unpersuasive. We do find that Petitioner characterizes Cheung correctly to a point. We agree that Cheung discloses that, if a user enters the correct access code, Cheung’s system opens switch 22, closes switch 17, and “power from the winding 12 is therefore transferred to the secondary winding 13 and the spark plug 19.” See Ex. 1011, 2:11–21. These operations deliver high voltage necessary to the distributor, which is ultimately used to create an electric spark in the spark plugs to ignite the fuel-air mixture within a cylinder of the engine. We reproduce Cheung’s Figure 1, below.

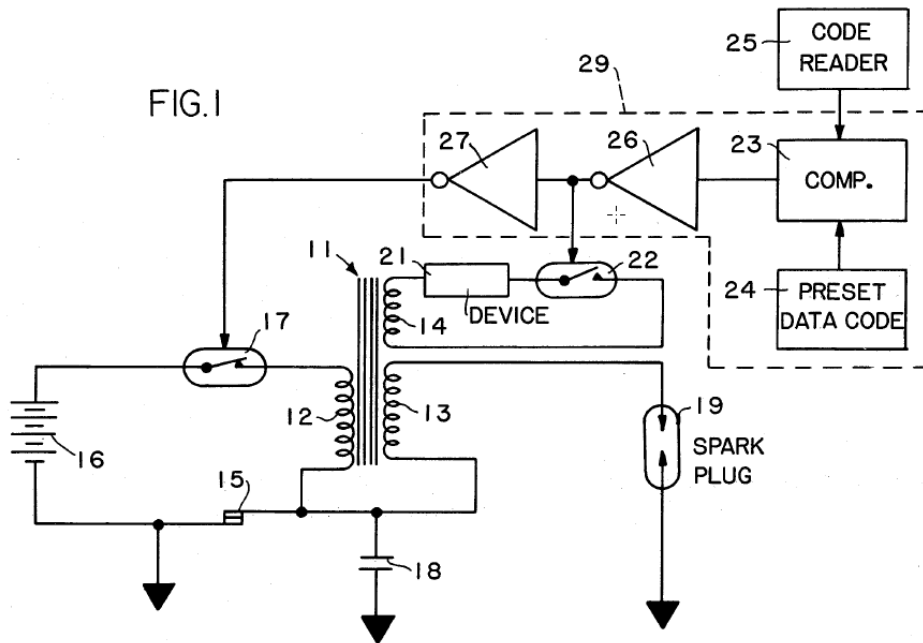


Figure 1 depicts a schematic drawing of Cheung's "secure ignition system." Ex. 1011, 1:43–44. What is missing from Cheung's disclosure, and Petitioner's explanation (and Mr. Wilson's testimony), is the step of energizing a starter motor, which would begin the process of the spark plug igniting the air-fuel mixture. In other words, Cheung's secure ignition system *allows* the engine to start, once certain security steps have been successfully performed, but we discern no disclosure that describes Cheung's system of actually starting the engine, as required by the "processor regulating operations" limitation of claim 1.

Alternatively, Petitioner contends that, in Chase, a user may create a new reservation, and Chase's server is responsible for confirming reservations. Pet. 61 (referencing Ex. 1009 ¶¶ 56, 60). For this scenario, Petitioner relies on Chase's starter module 106 to start the vehicle. *See id.* at 61–62 (referencing Ex. 1009 ¶ 50; Ex. 1006 ¶ 143). Petitioner contends that, "[b]ecause Chase's server is responsible for confirming reservations" a person having ordinary skill in the art "would understand this new

reservation requires Chase's processor to communicate the driver's reservation request to the server before confirming that the vehicle is available for use." *Id.* (referencing Ex. 1009 ¶ 50; Ex. 1006 ¶ 143).

Paragraph 50 of Chase discloses that "[i]f the ID matches an appropriate reservation, the board computer unlocks the car door via the door locks module 107 and *enables* the ignition via the starter module 106." Ex. 1009 ¶ 50 (emphasis added). Thus, starter module 106 is permissive as it *enables* the ignition but does not necessarily *start* the vehicle, as Petitioner contends. This paragraph also discloses that a code can be entered and compared before enabling the ignition. *Id.* This disclosure is consistent with the understanding that Chase's system *enables* the vehicle to start but does not disclose *starting* the vehicle. Chase elsewhere discloses that processor 1001 is able to enable and disable the vehicle ignition using ignition disable 1009. *Id.* ¶ 66; *see also id.* ¶ 59 (disclosing that, if the card ID matches, the processor sends a signal to the door unlock mechanism and *enables* the ignition using the Ignition Disable), ¶ 60 (allowing vehicle use). This type of control is also permissive. Accordingly, we find Petitioner's alternative contention relying on Chase unpersuasive.

To the extent that Petitioner argues that Chase discloses that, upon verifying a user's PIN, the "board computer enables ignition" by way of a "Hardwire to starter," we find that this evidence does not demonstrate that Chase's management server starts the vehicle. *See* Pet. 49–50 (referencing Ex. 1009, p. 21 (table, row 8); Ex. 1006 ¶ 123). Again, this disclosure indicates that Chase's system *enables* ignition. *See* Ex. 1009, p.21 (table, row 11). Neither Petitioner nor Mr. Wilson provides sufficient argument or evidence to demonstrate that Chase alone discloses actually starting the

engine, as required by the “processor regulating operations” limitation of claim 1.

Even if we were to agree with Petitioner that Cheung’s system actually starts the engine we conclude, on review of the complete evidence, that Petitioner fails to provide a persuasive reason to modify Cheung to allow Chase’s management server to start the vehicle. The only motivation provided in the Petition is that a person having ordinary skill in the art “would have been motivated, with reasonable expectations of success, to use Cheung’s keyless start arrangement in Chase’s system to avoid requiring keys or transferring keys among users, while providing security against theft.” Pet. 51 (referencing Ex. 1006 ¶ 126). As Petitioner explains, with “Cheung’s keyless start arrangement,” *a user* enters an access code into a code reader *at the vehicle site*. *Id.* at 50. Petitioner provides no persuasive reason to further modify the combination of Chase and Cheung to have Chase’s remote management server start the vehicle. *See* Pet. 60–62 (discussing the “starting” step of claim 1, and not providing any additional motivation to modify Chase with Cheung’s teachings such that Chase’s server starts the vehicle). Indeed, with respect to Chase’s server, Petitioner contends that it allows *a user* to start the vehicle. *See* Pet. 61 (“[T]he driver’s authorized operation of the vehicle includes starting the vehicle (e.g., Cheung’s transformer fires the spark plug) only after involvement of the remote management source (i.e., via Chase’s server).”), 62 (“[T]his new reservation requires Chase’s processor to communicate the driver’s reservation request to the server before confirming that the vehicle is available for use (and before authorizing the user to use “starter module 106” to start the vehicle.”).

Accordingly, on the complete trial record, we conclude that Petitioner has not proven, by a preponderance of the evidence, that claim 1 is unpatentable under 35 U.S.C. § 103(a) over Chase, Kaman, and Cheung.

2. *Independent Claim 11*

Claim 11 recites, in relevant part, “wherein the remote management source is additionally configured to: . . . start the machine if the entered access code matches the authorization code.” Ex. 1001, 7:30–35 (the “starting” limitation of claim 11). Petitioner relies on its same contentions in support of its unpatentability position for the “starting” step of claim 11 as it does for the “starting” step of claim 1. See Pet. 68–69. Accordingly, for the reasons discussed above in connection with our analysis of claim 1 for Ground 4, we conclude that Petitioner has not proven, by a preponderance of the evidence, that claim 11 is unpatentable under 35 U.S.C. § 103(a) over Chase, Kaman, and Cheung.

3. *Dependent Claims 3, 7, 10, 13, 17, and 20*

Dependent claims 3, 7, and 10 depend directly from claim 1, and claims 13, 19, and 20 depend directly from claim 11. For the reasons discussed above in connection with our analysis of independent claims 1 and 11 under this ground, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claims 3, 7, 10, 13, 19, and 20 are unpatentable under 35 U.S.C. § 103(a) over Chase, Kaman, and Cheung.

G. *Grounds 5 and 6: Obviousness of Claims 2 and 12 over Chase, Cheung, Kaman, and Bernosky, and Obviousness of Claims 9 and 19 over Chase, Cheung, Kaman, and Ehrman*

Petitioner contends that dependent claims 2 and 12 would have been obvious over Chase, Kaman, Cheung, and Bernosky (Ground 5), and claims 9 and 19 would have been obvious over Chase, Kaman, Cheung, and

Ehrman (Ground 6). Pet. 70–72. Under these grounds, Petitioner does not rely on either Bernosky or Ehrman to remedy the deficiency in Cheung we identify above in our analysis of independent claims 1 and 11, from which these dependent claims directly depend. *See id.*

Accordingly, for the reasons discussed above in connection with our analysis of independent claims 1 and 11 over Chase, Kaman, and Cheung, we conclude that Petitioner fails to demonstrate, by a preponderance of the evidence, that claims 2 and 12 are unpatentable under 35 U.S.C. § 103(a) over Chase, Kaman, Cheung, and Bernosky, and that claims 9 and 19 are unpatentable under 35 U.S.C. § 103(a) over Chase, Kaman, Cheung, and Ehrman.

H. Ground 7: Obviousness of Claims 1–3, 7–13, and 17–20 over Harvey, Cheung, and Kaman

Petitioner contends that claims 1–3, 7–13, and 17–20 would have been obvious over Harvey, Cheung, and Kaman (Ground 7). Pet. 6, 73–86.

As with Ground 4, analyzed above, Petitioner relies on Cheung for teaching the subject matter of the “starting” step of claim 1 and the “starting” limitation of claim 11. Pet. 81, 85. Accordingly, for the reasons discussed above in connection with our analysis of claim 1 for Ground 4, we conclude that Petitioner has not proven, by a preponderance of the evidence, that independent claims 1 and 11 are unpatentable under 35 U.S.C. § 103(a) over Harvey, Cheung, and Kaman. Also, for these same reasons, we conclude that Petitioner has not proven, by a preponderance of the evidence, that dependent claims 2, 3, 7–10, 12, 13, and 17–20, which depend, directly or indirectly from either claim 1 or 11, are unpatentable under 35 U.S.C. § 103(a) over Harvey, Cheung, and Kaman.

III. CONCLUSION

For the reasons above, we conclude that Petitioner has not demonstrated, by a preponderance of the evidence, that any of the Challenged Claims are unpatentable.

In summary:

Claims	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 3, 9, 10, 11, 13, 19, 20	103(a)	Shibata, Kaman		1, 3, 9, 10, 11, 13, 19, 20
7, 8, 17, 18	103(a)	Shibata, Kaman, Chase		7, 8, 17, 18
2, 12	103(a)	Shibata, Kaman, Bernosky		2, 12
1, 3, 7, 10, 11, 13, 17, 20	103(a)	Chase, Cheung, Kaman		1, 3, 7, 10, 11, 13, 17, 20
2, 12	103(a)	Chase, Cheung, Kaman, Bernosky		2, 12
9, 19	103(a)	Chase, Cheung, Kaman, Ehrman		9, 19
1–3, 7–13, 17– 20	103(a)	Harvey, Cheung, Kaman		1–3, 7–13, 17– 20
Overall Outcome				1–3, 7–13, 17–20

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–3, 7–13, and 17–20 of U.S. Patent No. 9,193,330 B2 are determined not to have been proven unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2021-00834
Patent 9,193,330 B2

FOR PETITIONER:

Edward H. Sikorski
Matthew Satchwell
James M. Heintz
DLA Piper LLP
ed.sikorski@dlapiper.com
matthew.satchwell@dlapiper.com
jim.heintz@dlapiper.com

FOR PATENT OWNER:

Theodore Stevenson, III
Matthew Howell
ALSTON & BIRD
ted.stevenson@alston.com
matthew.howell@alston.com