Trials@uspto.gov
571-272-7822

Paper 34
Entered: September 28, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MOBILE TECH, INC.,
Petitioner,

v.

INVUE SECURITY PRODUCTS INC.,
Patent Owner.

Cases IPR2016-00898 and IPR2016-00899
Patent 9,269,247 B2

Before JUSTIN T. ARBES, STACEY G. WHITE, and DANIEL J. GALLIGAN, *Administrative Patent Judges*.

ARBES, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a)

I. BACKGROUND

Petitioner Mobile Tech, Inc. filed two Petitions requesting *inter partes* review of claims 1–37 of U.S. Patent No. 9,269,247 B2 (Ex. 1001,[1] "the '247 patent"), pursuant to 35 U.S.C. §§ 311–319, in Cases IPR2016-00898 and IPR2016-00899. On September 29, 2016, an *inter partes* review was instituted in each proceeding on certain grounds of unpatentability. Patent Owner InVue Security Products Inc. filed a Patent Owner Response and Petitioner filed a Reply in each proceeding, as listed in the following chart.

Case Number	Challenged Claims	Decision on Institution	Petition	Response	Reply
IPR2016-00898	1–24	Paper 10 ("-898 Dec. on Inst.")	Paper 5 ("-898 Pet.")	Paper 19 ("-898 PO Resp.")	Paper 23 ("-898 Reply")
IPR2016-00899	25–37	Paper 9 ("-899 Dec. on Inst.")	Paper 4 ("-899 Pet.")	Paper 16 ("-899 PO Resp.")	Paper 20 ("-899 Reply")

Patent Owner also filed a Motion to Exclude certain evidence submitted by Petitioner, Petitioner filed an Opposition, and Patent Owner filed a Reply in each proceeding, as listed in the following chart.

Case Number	Motion	Opposition	Reply
IPR2016-00898	Paper 27 ("-898 Mot.")	Paper 30 ("-898 Opp.")	Paper 31
IPR2016-00899	Paper 24	Paper 26	Paper 27

[1] Unless otherwise specified, we refer to papers and exhibits filed in Case IPR2016-00898.

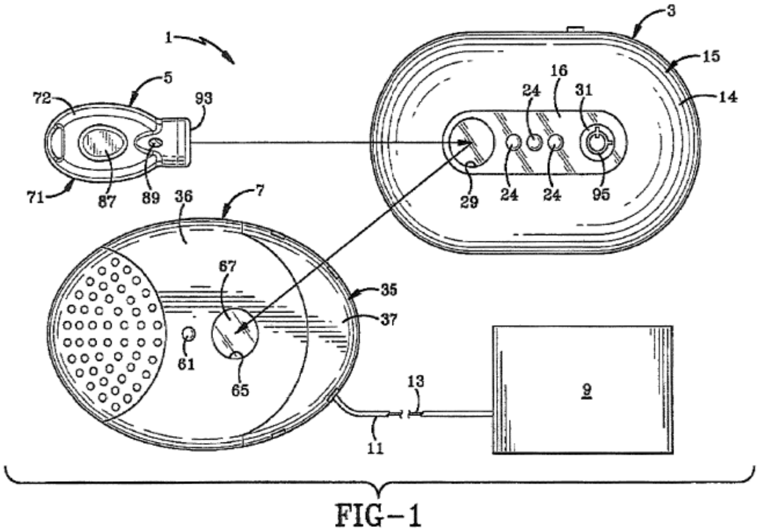
A combined oral hearing with Cases IPR2016-00892, IPR2016-00895, and IPR2016-00896 was held on June 14, 2017, and a transcript of the hearing is included in the record (Paper 33, "Tr.").

Cases IPR2016-00898 and IPR2016-00899 involve the same challenged patent and parties, and there is overlap in the asserted prior art and other evidence submitted by the parties. To administer the proceedings more efficiently, we exercise our authority under 35 U.S.C. § 315(d) to consolidate the two proceedings for purposes of issuing one final written decision.

We have jurisdiction under 35 U.S.C. § 6. This Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons that follow, we determine that Petitioner has shown, by a preponderance of the evidence, that claims 1–37 of the '247 patent are unpatentable.

A. The '247 Patent

The '247 patent describes a "programmable security system and method for protecting an item of merchandise." Ex. 1001, Abstract. Figure 1 of the '247 patent is reproduced below.



FIG–1

Figure 1 depicts security system 1 that includes programming station 3, programmable key 5, and alarm module 7 adapted to be attached to item of merchandise 9 by cable 11 with sense loop 13. *Id.* at col. 6, ll. 4–10. Programming station 3 randomly generates a unique security code (Security Disarm Code, or "SDC") that is transmitted via a wireless (e.g., infrared) link to programmable key 5, which in turn stores the SDC in key memory. *Id.* at col. 6, ll. 29–31, col. 7, ll. 25–30, col. 9, ll. 7–13. Once programmed with an SDC, programmable key 5 is taken to one or more alarm modules 7 and the SDC is communicated via circuitry to the respective alarm module, which stores the SDC in its memory. *Id.* at col. 9, ll. 26–35.

Cable 11 extends between alarm module 7 and item of merchandise 9. *Id.* at col. 7, ll. 54–56. If sense loop 13 (which contains electrical or fiber optic conductors) is compromised, such as by cutting cable 11 or by pulling the cable loose from alarm module 7 or item of merchandise 9, the alarm module emits an audible alarm. *Id.* at col. 7, ll. 52–64. To disarm alarm module 7, programmable key 5 is programmed with a valid SDC and circuits in the alarm module and the key communicate with one another to deactivate the alarm, thereby enabling cable 11 to be removed from the merchandise item. *Id.* at col. 10, ll. 47–59. Programmable key 5 then may be used to re-arm the alarm module. *Id.* at col. 10, ll. 59–63. "[T]o disarm and re-arm alarm module 7, the SDC memory 53 of the alarm module must read the same SDC that was randomly generated by the programming station 3 and programmed into the programmable key 5 and subsequently provided by the key to the alarm module." *Id.* at col. 10, l. 66–col. 11, l. 8.

B. Illustrative Claim

Claims 1, 25, and 31 of the ’247 patent are independent. Claim 1 recites:

> 1. A programmable security system for protecting items of merchandise from theft, the programmable security system comprising:
>
> a programming station comprising a logic control circuit configured to generate a unique security code, and a memory for storing the unique security code;
>
> a plurality of programmable keys each configured to communicate with the programming station to receive and store the unique security code in a memory, each of the plurality of programmable keys having the unique security code stored in its memory; and
>
> a plurality of security devices each comprising an alarm and a memory for storing the unique security code, each of the plurality of security devices having the unique security code stored in its memory, each of the plurality of security devices configured to be attached to an item of merchandise, each of the plurality of security devices further configured to activate the alarm in response to the integrity of the security device being compromised;
>
> wherein each of the plurality of programmable keys is configured to arm or disarm each of the plurality of security devices upon a matching of the unique security code stored by the plurality of security devices with the unique security code stored by the plurality of programmable keys.

C. Prior Art

The pending grounds of unpatentability in the instant *inter partes* reviews are based on the following prior art:

> U.S. Patent No. 5,543,782, issued Aug. 6, 1996 (Ex. 1005, “Rothbaum”);

U.S. Patent No. 6,380,855 B1, issued Apr. 30, 2002 (Ex. 1006, "Ott");

U.S. Patent Application Publication No. 2004/0201449 A1, published Oct. 14, 2004 (Ex. 1003, "Denison");

U.S. Patent Application Publication No. 2005/0073413 A1, published Apr. 7, 2005 (Ex. 1004, "Sedon"); and

U.S. Patent Application Publication No. 2007/0159328 A1, filed Dec. 14, 2006, published July 12, 2007 (Ex. 1002, "Belden").

D. Pending Grounds of Unpatentability

The instant *inter partes* reviews involve the following grounds of unpatentability:

Reference(s)	Basis	Claim(s)
Belden	35 U.S.C. § 102(b)[2]	1, 3–34, 36, and 37
Belden and Sedon	35 U.S.C. § 103(a)	2 and 35
Rothbaum and Denison	35 U.S.C. § 103(a)	1 and 3–37
Rothbaum, Denison, and Ott	35 U.S.C. § 103(a)	2

II. ANALYSIS

A. Claim Interpretation

The Board interprets claims in an unexpired patent using the "broadest reasonable construction in light of the specification of the patent in which

[2] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. §§ 102, 103, and 112. Because the '247 patent has an effective filing date before the effective date of the applicable AIA amendments, we refer to the pre-AIA versions of 35 U.S.C. §§ 102, 103, and 112.

[they] appear[].” 37 C.F.R. § 42.100(b); *see also Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard). Under this standard, we interpret claim terms using “the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant’s specification.” *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997).
We presume that claim terms have their ordinary and customary meaning. *See Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1062 (Fed. Cir. 2016) (“Under a broadest reasonable interpretation, words of the claim must be given their plain meaning, unless such meaning is inconsistent with the specification and prosecution history.”); *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (“The ordinary and customary meaning is the meaning that the term would have to a person of ordinary skill in the art in question.” (internal quotation marks omitted)). A patentee, however, may rebut this presumption by acting as his own lexicographer, providing a definition of the term in the specification with “reasonable clarity, deliberateness, and precision.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

1. “Programmable Key”

In the Decision on Institution, the panel preliminarily determined that the claim term “programmable key” is not “limited to a programmable key that ‘deactivates itself upon the occurrence of a specific event,’ as argued by Petitioner.” *See* -898 Dec. on Inst. 7; -899 Dec. on Inst. 6–7. The parties do not dispute this interpretation, and we do not perceive any reason or evidence that compels any deviation from the interpretation. We adopt the previous analysis and need not further interpret the term for purposes of this Decision.

2. "Upon a Matching"

Claim 1 recites that "each of the plurality of programmable keys is configured to arm or disarm each of the plurality of security devices *upon a matching* of the unique security code stored by the plurality of security devices with the unique security code stored by the plurality of programmable keys" (emphasis added). Claim 25 recites "arming or disarming each of the plurality of security devices *upon a matching* of the unique security code stored by the plurality of security devices with the unique security code stored by the plurality of programmable keys" (emphasis added). Claim 31 recites "arming or disarming the security device *upon a matching* of the security code generated by the programming station with the security code stored by the security device" (emphasis added).

Patent Owner argues in its Responses that "upon a matching" should be interpreted to mean "on or after a match." -898 PO Resp. 4–12.[3] Petitioner argues that the phrase means "as a result of a determination of a match." -898 Reply 5–10. During the hearing, Patent Owner agreed to the "as a result of" portion of Petitioner's proposed interpretation but disagreed

[3] The parties make a number of similar arguments in their Petitions, Responses, and Replies. As to these arguments, we refer only to the papers filed in Case IPR2016-00898 for ease of reference.

as to the "determination of a match" aspect. Tr. 43:13–45:5, 50:18–21 ("[W]e do agree that there has to be a cause, causal connection. So we would also be happy with, you know, a definition of upon a match being a result of the matching."). Thus, the parties agree that the claim language requires a causal relationship between the matching of the security codes and the arming or disarming of the security devices (i.e., the arming or disarming is "as a result of" the matching). *See id.;* -898 Reply 6. The dispute we must resolve is whether the arming or disarming must be as a result of a "determination of a match." *See* Tr. 86:6–87:19.

We begin with the plain language of the claims. The term "matching" is used as a gerund (i.e., a verb acting as a noun) in claims 1, 25, and 31, and ordinarily means "[t]he action of match." Ex. 1020, 4, 6. Thus, the use of "upon a matching" suggests some action of a match, as opposed to, for example, "upon a match," which might be read to require simply the *existence* of a match. This supports Petitioner's view that the arming or disarming must be as a result of a "determination of a match" (a particular type of action).

Turning to the Specification, only the Abstract uses the term "matching," and it largely repeats the phrasing of the claims. Ex. 1001, Abstract. The verb "match" also appears twice. Although this usage is "match" rather than "matching," both times the Specification uses the term to describe a determination of whether the security code stored in the programmable key is the same as what is stored in the programming station, and then performing some action based on the outcome of that determination. *Id.* at col. 3, ll. 32–37 ("enable the programming station to immediately 'time-out' the key . . . upon the programming station reading a

SDC stored in the key that does not match the SDC of the programming station"), col. 4, ll. 4–10 ("the logic control circuit of the programming station may be configured to permanently inactivate the SDC in a programmable key if the SDC programmed in the key does not match the SDC of the programming station"). These portions, therefore, are consistent with Petitioner's proposed interpretation requiring a determination of a match.

The Specification also describes, in connection with disarming and re-arming the security device, reading the security codes in the programmable key and security device to determine if they are the same. "In order to disarm alarm module 7, a programmable key 5 programmed with a valid SDC that is still within the active predetermined time period is placed into the key receiving port 65 of the alarm module, . . . and activation switch 85 is energized by depressing the flexible member 87 on the key." *Id.* at col. 10, ll. 47–52. Alarm module 7 and programmable key 5 then communicate with each other to deactivate the alarm, "thereby enabling cable 11 and any associated sensor to be removed from an item of merchandise 9 for sale of the merchandise to a customer." *Id.* at col. 10, ll. 52–59. "The programmable key 5 may then be used to re-arm the alarm module 7 by again presenting the key to the key receiving port 65 on the alarm module and depressing the flexible member 87 to energize the activation switch 85." *Id.* at col. 10, ll. 59–63.

Importantly, the Specification states that "in order to *disarm and re-arm* alarm module 7, the SDC memory 53 of the alarm module must *read the same SDC* that was randomly generated by the programming station 3 and programmed into the programmable key 5 and subsequently provided by the key to the alarm module." *Id.* at col. 10, l. 66–col. 11, l. 4 (emphases added). "If a SDC is sensed by alarm module 7 that is *different* than the one stored in SDC memory 53, controller 49 of alarm module 7 will sound alarm 51 to indicate that an invalid programmable key 5 has been used." *Id.* at col. 11, ll. 4–8 (emphasis added); *see also id.* at col. 4, ll. 48–61 ("disarming the security device upon verifying . . . the security code in the alarm module with the security code in the key"). Thus, for disarming and re-arming the security device, the Specification describes reading the security codes in the programmable key and security device and making a determination of whether they match.

Patent Owner acknowledges this disclosure from the Specification with respect to disarming and re-arming but argues that the Specification describes another way to arm "upon a matching." -898 PO Resp. 11–12. According to Patent Owner, programming the security code into the security device "*causes* a *matching* of the memories of the programmable key and the security device, thus meeting a condition precedent to arm the device." *Id.* at 7 (first emphasis added). Patent Owner argues that the security codes in the programmable key and security device match "after the programming/storing function occurs" and that "this matching of the SDC codes *must occur* in order to arm the security device," citing the testimony of the parties' declarants and Figure 13 of the '247 patent. *Id.* at 8–10. Petitioner responds that the programming cited by Patent Owner simply involves the security code being "copied from the key into the alarm module," without any "check . . . to see if the SDC in the alarm module and key 'read the same.'" -898 Reply 9–10. Thus, programming the security device with the security code does not involve "matching" as recited in the claims. *Id.*

We agree with Petitioner as to the initial programming of the security code into the security device. The Specification states that

> [o]nce programmed with the SDC, key 5 is taken to one or more alarm modules 7 (or other security devices) and key end 93 is inserted into key receiving port 65, as shown in FIG. 5. Activation switch 85 of key 5 is then actuated, thereby *programming* the SDC via the communication circuit 50 of alarm module 7 and communication circuit 79 of key 5 into security code (SDC) memory 53 of the logic control circuit 46 of the alarm module 7. SDC memory 53 permanently *stores* the randomly generated SDC in the alarm module 7, preferably for the remaining lifetime of the alarm module.

Ex. 1001, col. 9, ll. 26–35 (emphases added). This merely indicates that the security code is programmed (i.e., stored) into the security device, not that the security device is armed "upon a matching." *See id.*; -898 Reply 8. Indeed, claims 1, 25, and 31 separately recite "storing" the security code in the security device and "arming or disarming" the security device, indicating that the two actions are not the same. Further, in contrast to the portions of the Specification cited above regarding disarming and re-arming, which specifically refer to the security codes being "read" and being the "same," the portions cited by Patent Owner regarding initial programming include no such language. *See* -898 PO Resp. 7–10 (citing Ex. 1001, col. 3, l. 67–col. 4, l. 3, col. 4, ll. 45–47, col. 9, ll. 26–39, col. 11, ll. 27–29).

We also are not persuaded by Patent Owner's arguments (*id.* at 9–10) regarding Figure 13 of the '247 patent, which is reproduced below.

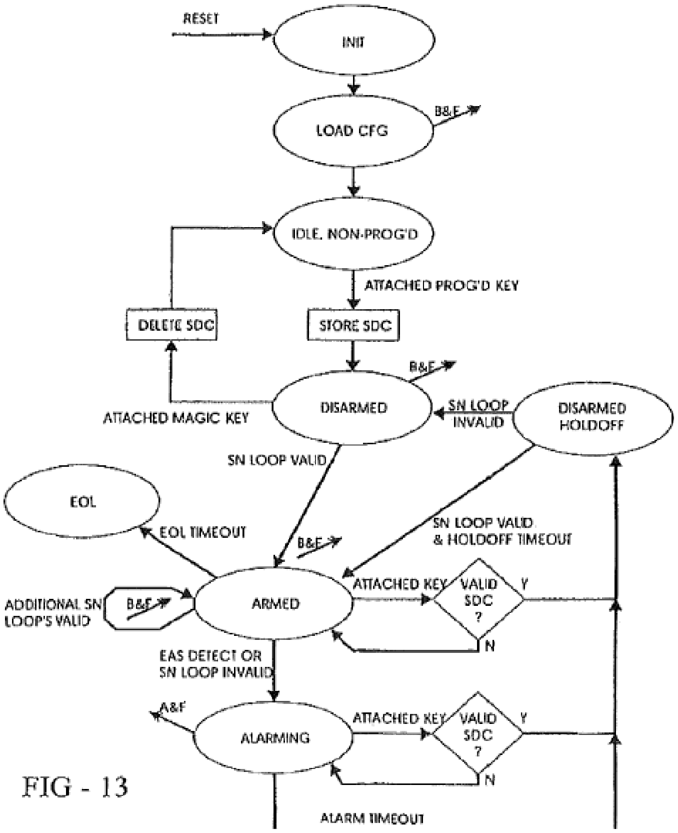


FIG - 13

Figure 13 "illustrates in flow chart form the manner of operation of the logic control circuit 46 of alarm module 7," the sequence of events and actions of which are "readily understood and appreciated by those skilled in the art." Ex. 1001, col. 11, ll. 52–57. Patent Owner contends that "[t]he security device goes from a 'DISARMED' state to an 'ARMED' state *only* upon a matching occurring between the SDC in the programmable key and the code in the security device." -898 PO Resp. 9–10. The point at which the security codes in the programmable key and security device become the same, however, is earlier—when the security code is first programmed into the security device in the "STORE SDC" step. Ex. 1001, Fig. 13. After doing so, the security device moves to the "DISARMED" state, and only moves to the "ARMED" state when the sense loop connected to the item of merchandise is determined to be valid ("SN LOOP VALID"). *Id.*, Fig. 13, col. 3, l. 63–col. 4, l. 3; col. 7, l. 50–col. 8, l. 4. Thus, Figure 13 does not support Patent Owner's position regarding the "upon a matching" claim language.

Finally, we note that the parties also disagree as to whether the "upon a matching" language requires the arming or disarming to take place "immediately" as a result of the matching. *See, e.g.*, -898 PO Resp. 18–19; -898 Reply 6 & n.1; Tr. 44:7–16, 59:9–60:17, 69:19–70:10, 112:11–115:4. Petitioner submits dictionary definitions of "on," including "[o]n the occasion of (an action)," "immediately after (and because of or in reaction to)," and "as a result of." Ex. 1020, 3; *see* -898 Reply 6 n.1 (also arguing that "upon" means "on"). However, unlike the disclosure of the Specification cited above, which supports Petitioner's view that the arming or disarming must be "as a result of" a determination of a match, we see no language in the claims or written description pertaining to the timing of when the arming or disarming must occur. Thus, we are not persuaded to read into the claims a requirement that the arming or disarming take place "immediately" after a matching. The only requirement supported by the claim language and Specification is arming or disarming as a result of a determination of a match.

Reading the Specification of the '247 patent as a whole, we are persuaded that Petitioner's proposed interpretation of "upon a matching" is the broadest reasonable interpretation in light of the Specification. Accordingly, we interpret "upon a matching" to mean as a result of a determination of a match.

3. "Configured to Communicate" and "Providing the [Unique] Security Code"

Claim 1 recites "a plurality of programmable keys each *configured to communicate* with the programming station to receive and store the unique security code in a memory, each of the plurality of programmable keys having the unique security code stored in its memory" (emphasis added). Claim 25 recites "*providing* the unique security code to each of a plurality of programmable keys, each of the plurality of programmable keys having a memory and the unique security code stored in its memory" (emphasis added). Claim 31 recites "*providing* the security code to a programmable key" (emphasis added).[4]

Petitioner argues that the phrases "configured to communicate" and "providing the [unique] security code," as used in the challenged claims of the '247 patent, "encompass[] both wireless and wired forms of communication." *See* -898 Pet. 7; -899 Pet. 7. Petitioner bases this argument on the Specification's disclosure that "[a]nother aspect of the present invention is to provide various forms of data communication between the various elements of the security system," including, "[i]n one preferred embodiment, . . . by wireless communication," and, "[i]n another preferred embodiment, . . . through electrical contacts." Ex. 1001, col. 3, ll. 6–21. Petitioner proposes this interpretation to argue that the application that published as Belden does not describe communication through electrical contacts and, therefore, does not provide written description support for the

[4] Claim 13, which depends from claim 1, recites that the programmable keys are configured to "wirelessly communicate" with the programming station. Claims 26 and 32, which depend from claims 25 and 31, respectively, recite that the providing comprises "wirelessly communicating" the security code.

claimed subject matter reciting “configured to communicate” and “providing the [unique] security code.” *See* -898 Pet. 17–19; -899 Pet. 17–20. In particular, Petitioner contends that the continuation-in-part application to which the ’247 patent claims priority “broadened the meaning of the term[s] ‘communicate’ [and ‘providing’] within the claims to encompass the genus of both wireless and non-wireless communication” by reciting other forms of communication, such as communication “through electrical contacts.” -898 Pet. 18–19 (citing Ex. 1001, col. 3, ll. 6–21); *see* -899 Pet. 19–20.

We do not agree that the recital of various “forms of data communication” (Ex. 1001, col. 3, ll. 6–21) in the ’247 patent broadened the meanings of the phrases “configured to communicate” and “providing the [unique] security code.” Rather, the “forms” of communication in the cited portion of the ’247 patent merely represent examples of the media or means by which the communication occurs in various preferred embodiments. *Id.* (listing at least seven examples, including “wireless communication, such as infrared (IR), radio frequency (RF) or similar wireless communication system[s],” “through electrical contacts,” and “induction, for example electromagnetic induction, magnetic induction, electrostatic induction, etc.”). Thus, Petitioner does not persuade us that we need to interpret the phrases “configured to communicate” and “providing the [unique] security code” expressly to encompass both wireless and wired communications.

4. "Unique Security Code" (Claims 1 and 25), "Security Code Generated by the Programming Station and Being Unique Thereto" (Claim 31), and "Unique to a Particular Retail Establishment or Retail Store" (Claim 21)

Independent claims 1 and 25 recite a "unique security code." Independent claim 31 recites "the security code generated by the programming station and being unique thereto." Claim 21, which depends from claim 1, recites that "the unique security code is unique to a particular retail establishment or retail store." In the Decision on Institution, the panel determined that "a randomly generated security code is within the broadest reasonable interpretation of 'unique security code,'" as recited in claims 1 and 25 and similarly recited in claim 31. *See* -898 Dec. on Inst. 7–8; -899 Dec. on Inst. 7. The parties do not dispute this interpretation as to claims 1 and 25, and we do not perceive any reason or evidence that compels any deviation from the interpretation as to claims 1 and 25.

With respect to claims 21 and 31, Petitioner contends that the phrases encompass a randomly generated security code, just like claims 1 and 25, relying primarily on the Specification of the '247 patent. -899 Pet. 6–7, 53; -899 Reply 19–21. Patent Owner responds that the "unique" phrase in claim 31 should be given its "[p]lain meaning affording adequate weight to [the] requirement of 'unique' in the context of . . . the programming station." -899 PO Resp. 4. According to Patent Owner, "[a]lthough some randomly generated codes are unique, not *all* randomly generated codes are unique." *Id.* In support of its position, Patent Owner cites portions of the Specification, claim 33, and the testimony of Petitioner's declarant, Thaine Allison III. *Id.* at 4–6. Patent Owner makes similar arguments with respect to claim 21. -898 PO Resp. 40–43.

We are persuaded that, given its broadest reasonable interpretation in light of the Specification, the "unique" phrases in claims 21 and 31 encompass a randomly generated security code. In multiple places, the Specification characterizes a randomly generated security code as "unique." *See* Ex. 1001, col. 9, ll. 7–13 ("Actuation of activation switch 85 causes logic control circuit 18 of programming station 3 to randomly generate a unique security code (i.e. SDC) . . . ."), col. 9, ll. 19–23 ("In accordance with one of the objectives and features of the present invention, the SDC initially provided by programming station 3 is randomly generated and is unique to that programming station and always remains with that programming station for subsequent use."), col. 12, ll. 33–39 ("the programmable key . . . is programmed with a randomly generated SDC unique to that particular retail store, and the SDC is initially randomly generated by a programming station used only by that particular retail store"), col. 15, ll. 26–28 ("the logic control circuit further comprises an electronic random number generator producing a unique SDC"). Thus, while there may be other ways to generate security codes, one way to generate a security code unique to the programming station and/or retail store, according to the Specification of the '247 patent, is to randomly generate the security code. *See id.* at col. 15, ll. 20–26 (stating that the security code "may be a predetermined (i.e. 'factory preset') security code, but preferably is a random security code").

This is confirmed by claim 33, which depends from claim 31 and recites "randomly generating the security code in the programming station." *See also id.*, claims 20, 28 (also reciting random generation of security codes). Contrary to Patent Owner's arguments, the language of claim 33 indicates that parent claim 31 encompasses within its scope the random generation of a security code in the programming station (as well as potentially other methods of generation), not that claim 31 requires something "more" than random generation. *See* -899 PO Resp. 5–6.

We also are not persuaded by Patent Owner's arguments regarding Mr. Allison's testimony and the potential sample size for generating a security code that is unique to the programming station. *See id.* at 6 (citing Ex. 2010, 178:24–179:23; Ex. 2013 ¶ 47). Mr. Allison was testifying in the cited excerpt to uniqueness "[i]n an absolute sense," not in the context of the '247 patent. *See* Ex. 2010, 179:19–23; -899 Reply 20–21. As Petitioner correctly points out, no number (even in a sample size of one to one billion, for example) is "unique in an absolute sense," and the term "unique" must be interpreted in light of the Specification. *See* -899 Reply 20.

Finally, we note that Patent Owner's proposed interpretation is vague and unclear in scope. Patent Owner contends that "adequate weight" must be given to how "unique" is used "in the claimed context," but does not explain in any detail how much weight should be given or provide any logical basis for determining whether a security code is or is not unique to a programming station or retail store. *See* -899 PO Resp. 4, 6. For this reason as well, we are not persuaded by Patent Owner's arguments.

Accordingly, we interpret "unique security code" in claims 1 and 25, "security code generated by the programming station and being unique thereto" in claim 31, and "unique to a particular retail establishment or retail store" in claim 21 as encompassing (but not being limited to) a randomly generated security code. We need not further interpret the claim language for purposes of this Decision.

B. Level of Ordinary Skill in the Art

> 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) (quoting 35 U.S.C. § 103(a)).

Petitioner's declarant, Mr. Allison, testifies that a person of ordinary skill in the art

> would have had a four year technical degree (*e.g.* B.S. engineering) with a minimum of three years of experience in using, provisioning, designing or creating, or supervising the design or creation, of such theft prevention devices, and other related security devices. Extended experience in the industry could substitute for a technical degree. A [person of ordinary skill in the art] would have known how to research the technical literature in fields relating to theft prevention, including in retail and other environments, as well as security in general. Also, a [person of ordinary skill in the art] may have worked as part of a multidisciplinary team and drawn upon not only his or her own skills, but also taken advantage of certain specialized skills of others in the team, e.g., to solve a given problem. For example, designers, engineers (*e.g.*, mechanical or electrical), and computer scientists or other computer programmers may have been part of a team.

Ex. 1015 ¶ 21. Patent Owner provides a slightly different skill level:

> [A person of ordinary skill in the art] would have the equivalent of a four-year degree in electrical engineering, computer engineering, computer science, or the equivalent and would also have approximately two to five years of professional experience and be trained in electronics including microcontrollers, and embedded programming for microcontrollers.

-898 PO Resp. 12 (citing Ex. 2001 ¶ 34). Patent Owner's declarants, Harry Direen, Ph.D., P.E., and Christopher J. Fawcett, testify that a person of ordinary skill in the art would have been

> an engineer (with a B.S. in electrical engineering, computer engineering, computer science, or the equivalent) with 2 to 5 years of experience and trained in electronics including microcontrollers, and embedded programming for microcontrollers. He/she would have been familiar with flowcharts and turning flowcharts and system operational descriptions into working software/firmware. He/she would have been familiar with asynchronous serial communications which were very common in systems that use microcontrollers. He/she would have been adept at turning design concepts into working products.

Ex. 2001 ¶ 34; Ex. 2013 ¶ 39.

Neither party explains in detail why its proposed level of ordinary skill in the art should be adopted nor how the different levels affect the parties' analyses. Although there are slight differences between the proposed levels of ordinary skill in the art, the parties' declarants agree that an ordinarily skilled artisan would have had a four-year technical degree or the equivalent and some amount of professional experience. Based on the evidence of record, including the testimony of the parties' declarants, the subject matter at issue, and the prior art of record, we determine that a person of ordinary skill in the art would have had a four-year technical degree or equivalent experience with a minimum of two years of professional technical experience in the field of theft prevention devices or related security devices. We apply this level of ordinary skill in the art for purposes of this Decision.

C. Obviousness Ground Based on Rothbaum and Denison (Claims 1 and 3–37)

Petitioner contends that claims 1 and 3–37 would have been obvious based on the combination of Rothbaum and Denison.[5] *See* -898 Pet. 33–57; -899 Pet. 34–58. Petitioner explains how the cited prior art references teach the claimed subject matter, provides reasoning as to why one of ordinary skill in the art would have been motivated to combine their respective teachings, and relies upon the testimony of Mr. Allison to support its positions. *Id.*

1. Whether Rothbaum and Denison are Analogous Art

As an initial matter, to be considered for obviousness, a reference must be analogous art. *See In re Bigio,* 381 F.3d 1320, 1325 (Fed. Cir. 2004) ("References within the statutory terms of 35 U.S.C. § 102 qualify as prior art for an obviousness determination only when analogous to the claimed invention."). A prior art reference qualifies as analogous art (1) if it is from the same field of endeavor as the claimed invention, regardless of the problem addressed, or (2) if the reference is not within the field of the inventor's endeavor, it is nonetheless reasonably pertinent to the particular problem with which the inventor is involved. *Id.*

Petitioner argues that "Denison and Rothbaum are in the field of security devices for the protection of merchandise." -898 Pet. 35 (citing Ex. 1015 ¶¶ 156–157). The '247 patent describes the "Field of the Invention" as follows:

[5] Rothbaum and Denison were not of record during prosecution of the '247 patent.

> The invention relates to security systems and methods for protecting merchandise from theft, and in particular, to a security system and method including a programmable key that is programmed with a security code from a programming station and is subsequently used to program and/or operate an alarm module attached to an item of merchandise.

Ex. 1001, col. 1, ll. 24–29. Therefore, the ’247 patent itself describes the relevant field of endeavor as “protecting merchandise from theft.” Further, claims 1, 25, and 31 are directed to a programmable security system and methods “for protecting items of merchandise from theft.”

We find that Rothbaum and Denison are analogous to the claimed invention because both references are in the same field of endeavor as the claimed invention, namely protecting merchandise from theft. In particular, Rothbaum is directed to “security systems, and more specifically to electronic security systems used in retail stores, offices, hotels and other establishments to prevent the theft of merchandise.” Ex. 1005, col. 1, ll. 6–9.[6] Similarly, Denison’s disclosure of electronically-locking vending machines is directed to protecting merchandise from theft. *See* Ex. 1003 ¶ 9 (“The use of the field-programmable electronic locks for vending machines provides an effective way to reduce theft and fraud in terms of unauthorized access to the machines.”).[7] Therefore, both references qualify as prior art to the challenged claims.

[6] During oral argument, counsel for Patent Owner acknowledged that Rothbaum is analogous art to the ’247 patent. Tr. 94:21–22.

[7] In its Responses, Patent Owner argues that “[v]ending machines are not analogous to retail merchandise systems (using alarms) as [Petitioner] alleges.” *See* -898 PO Resp. 28; -899 PO Resp. 31. During oral argument, counsel for Patent Owner stated that “Denison is only somewhat analogous to retail store security” and later clarified that Patent Owner’s argument is

2. Claim 1

Petitioner relies on Rothbaum for teaching certain limitations of claim 1 and relies on Denison for teaching other limitations. *See* -898 Pet. 33–44. Below we address Petitioner's contentions as to each reference and then address Petitioner's contentions and Patent Owner's arguments with respect to the combination of the teachings of Rothbaum and Denison.

a. Claim Limitations Taught by Rothbaum

Claim 1 is directed to "[a] programmable security system for protecting items of merchandise from theft." Petitioner contends Rothbaum teaches a security system for protecting merchandise, as illustrated in Figure 1 of Rothbaum. -898 Pet. 33, 40.

that Petitioner has not set forth a sufficient rationale to combine the teachings of Rothbaum and Denison, not that Denison is not analogous art to the '247 patent. Tr. 95:11–97:2.

Figure 1 of Rothbaum is reproduced below.

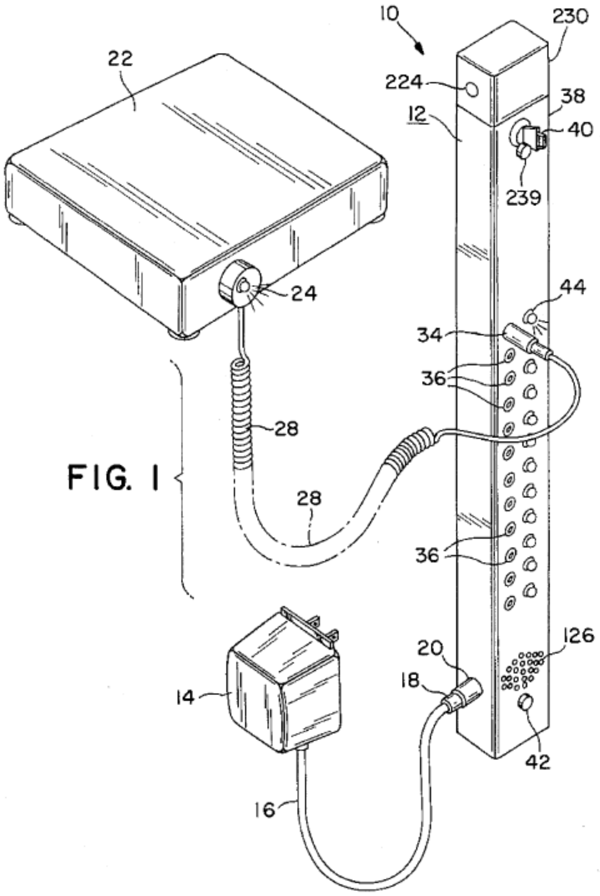


FIG. 1

In Figure 1, “a twelve jack security system 10 is shown which can protect twelve items of merchandise.” Ex. 1005, col. 5, ll. 10–11. We are persuaded by Petitioner’s argument and find that Rothbaum discloses a security system for protecting items of merchandise from theft. *See, e.g.*, *id.* at col. 5, ll. 10–11, Fig. 1; *see also id.* at col. 1, ll. 6–9 (“The present invention generally relates to security systems, and more specifically to electronic security systems used in retail stores, offices, hotels and other establishments to prevent the theft of merchandise.”).

Petitioner argues that Rothbaum’s disclosure of strip or housing 12 connecting to article of merchandise 22 via item cord 28 is a “security device[] . . . configured to be attached to an item of merchandise,” as recited in claim 1. -898 Pet. 33, 37–38, 42 (citing, *inter alia*, Ex. 1005, col. 5, l. 62–col. 6, l. 4, Fig. 1). We are persuaded by Petitioner's argument and find that Rothbaum teaches this limitation of claim 1 based on Rothbaum's disclosure in Figure 1 that item cord 28 connects strip 12 to sensor 24 on article of merchandise 22. *See* Ex. 1005, col. 5, l. 62–col. 6, l. 2 ("Hard goods sensor 24, including a sensor housing 23, is attached to the article 22 . . . . Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12."); Ex. 1015 ¶ 144.

Petitioner also argues that Rothbaum's security device has an "alarm" (i.e., horn 126) and is "configured to activate the alarm in response to the integrity of the security device being compromised," as recited in claim 1. -898 Pet. 33, 37–38, 42 (citing, *inter alia*, Ex. 1005, col. 6, ll. 15–22, col. 8, ll. 22–28, col. 12, ll. 10–18). We are persuaded by Petitioner's argument and find that Rothbaum teaches a security device having an "alarm" and being "configured to activate the alarm in response to the integrity of the security device being compromised" based on the following disclosure of Rothbaum:

> As can be seen in FIG. 12, tamper switch 225 is normally open. The tamper switch is activated by the battery compartment screw 224 as can be seen in FIG. 1. If an unauthorized person attempts to tamper with the battery 226, by opening the battery compartment cover 220, they must loosen screw 224. As screw 224 is removed, tension on the activator of switch 225 is moved thus closing switch 225. When switch 225 closes, transistor 122 is turned on thus activating horn 126.

Ex. 1005, col. 12, ll. 10–18. The integrity of Rothbaum's security device is compromised when the battery compartment is opened. *See* Ex. 1015, 71–72.

Petitioner further argues that Rothbaum teaches a key for disarming the security device after a security breach occurs. -898 Pet. 33 (citing Ex. 1005, col. 6, ll. 15–22, col. 8, ll. 22–28). We are persuaded by Petitioner's argument and find that Rothbaum teaches a key for disarming the security device after a breach occurs because Rothbaum discloses that, "once a breach of security condition is detected, the alarm horn 126 will sound [u]ntil key switch 38 is turned from the ON position to the SET position." Ex. 1005, col. 8, ll. 23–25.

Petitioner notes that "Rothbaum does not disclose that [its] 'key' is 'programmable' or used with a 'programming station,'" as recited in claim 1. -898 Pet. 33. Petitioner relies on Denison for these limitations. *See id.* at 33–34.

b. Claim Limitations Taught by Denison

Petitioner contends "Denison discloses a security system having both a 'programmable key' and 'programming station.'" -898 Pet. 33. Denison discloses the use of electronic locks for vending machines. Ex. 1003, Abstract, ¶¶ 2, 6.

Figure 17 of Denison is reproduced below.

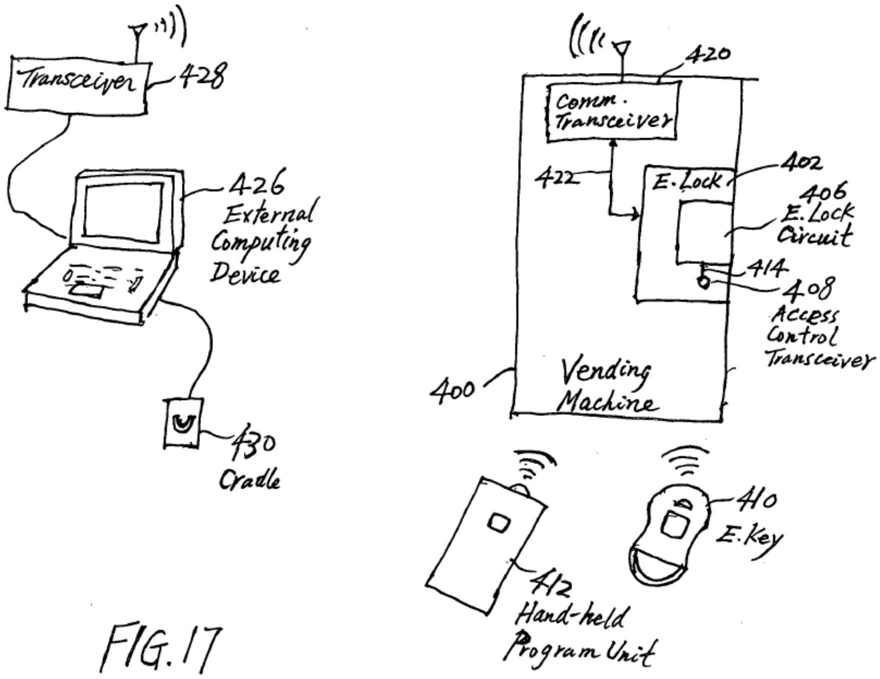


FIG. 17

Figure 17 depicts "a system in which one or more programming schemes may be implemented for field-programming the electronic lock 402 of the vending machine 400 without having to open the vending machine to access a program switch." *Id.* ¶ 77.

i. Programming Station

Petitioner argues that Denison's external computing device is "a programming station comprising a logic control circuit configured to generate a unique security code, and a memory for storing the unique security code," as recited in claim 1. -898 Pet. 33–34, 38, 40 (citing Ex. 1003 ¶¶ 43, 79, 84, 86). In particular, Petitioner contends that an access code stored within Denison's key code is a "unique security code" as claimed, and that the "access code is randomly generated by the 'external computing device' (*i.e.*, 'programming station'), which has a memory for storing the code." *Id.* (citing Ex. 1003 ¶¶ 43, 79, 84).

We find that Denison's external computing device is "a programming station comprising a logic control circuit configured to generate a unique security code, and a memory for storing the unique security code," as recited in claim 1. This finding is supported by Denison, which discloses:

> The external computing device 426 has in its *memory* a timebase, *access code or codes for electronic locks on vending machines*, and access control parameters for the electronic locks. In addition, the external computing device 426 may have a database 436 containing available access codes and control parameters that can be programmed into electronic locks in vending machines. The database 436 may alternatively or additionally contain *programs for computing new access codes and generating control parameters for electronic locks and keys*.

Ex. 1003 ¶ 79 (emphases added). Denison further discloses that "external computing device 426 may . . . have programs that implement[] mathematical algorithms for computing the access codes and control parameters. Such calculations may generate the access codes randomly or based on a function that includes the time as a variable." *Id.* ¶ 84. As such, Denison discloses that external computing device 426 is configured to generate an access code and has a memory to store the access code.

We also are persuaded by Petitioner's argument and find that Denison's access code is a "unique security code," as claimed, because it is randomly generated. *See* -898 Pet. 38–40 (citing Ex. 1003 ¶¶ 43 ("[A] key code 68 stored in an electronic key includes seven (7) digits. The first digit of the key code is used to indicate the type of the key. . . . The next 6 digits in the key code are the access code (000,000 to 999,999)."), 79, 84); *supra*

Section II.A.4. Finally, according to Petitioner and Mr. Allison, a person of ordinary skill in the art would have understood that "a microprocessor of the external computing device generates [the] random number" used as the access code and that "such a microprocessor is a 'logic control circuit.'" -898 Pet. 38; Ex. 1015, 67–68. We agree, given Denison's express disclosure that the external computing device executes "programs" implementing "mathematical algorithms" to compute access codes and functions to provide the access code to an electronic key. *See* Ex. 1003 ¶ 84.

ii. Programmable Key

Petitioner argues that Denison's electronic key is a "programmable key[]" that has "the unique security code stored in its memory" and is "configured to communicate with the programming station to receive and store the unique security code in a memory," as recited in claim 1. -898 Pet. 33–35, 38–41 (citing Ex. 1003 ¶¶ 6, 41–43, 60, 85, Figs. 1, 17). Petitioner argues that the electronic key in Denison communicates with the external computing device to receive the access code (i.e., "unique security code") and store it in memory. *Id.*

We are persuaded by Petitioner's contentions and find that Denison teaches the "programmable key" limitations of claim 1. This finding is supported by Denison, which discloses:

> [T]he external computing device 426 may optionally be used to program an electronic key 410 that can be used to visit and access the vending machine 400 through the access control transceiver 408. To that end, the electronic key 410 is connected to the cradle 430, and the access code that has been programmed into the lock is transmitted via the cradle into the key, together with any other appropriate access control

> parameters for the key. The key 410 can then be used to access the vending machine by communicating with the electronic lock circuit 406 via the access control transceiver 406 based on the newly programmed access code(s) and control parameters.

Ex. 1003 ¶ 85. Denison also discloses that "electronic key 26 includes . . . a nonvolatile memory 82," which "is for storing a key code 88." *Id.* ¶ 41; *see also id.* ¶ 42 ("Each electronic key 26 has a key code 88 stored therein . . . ."). Denison teaches a "plurality" of programmable keys, each having the same unique security code, as recited in claim 1. *Id.* ¶¶ 42 ("Each electronic key 26 has a key code 88 stored therein, and the same key code is stored in the memory 52 of the electronic lock in each vending machine to be operated with the electronic key."), 58 ("many keys with the same key code will be expected to communicate with many locks on different vending machines containing that key code"), 59 ("there may be many keys containing the same key code, and there may be many vending machines that have 'learned' the same key code"); *see* -898 Pet. 38.

Petitioner further argues that Denison teaches "each of the plurality of programmable keys [being] configured to arm or disarm each of the plurality of security devices upon a matching of the unique security code stored by the plurality of security devices with the unique security code stored by the plurality of programmable keys," as recited in claim 1. -898 Pet. 38–40, 43–44 (citing Ex. 1003 ¶¶ 36, 41–42, 58; Ex. 1015, 73). In particular, Petitioner contends that Denison "discloses unlocking / disarming the electronic lock of the vending machine (*i.e.*, 'security device') when the 'key code' in the key's memory matches that in the lock's memory." *Id.* at 38 (citing Ex. 1003 ¶¶ 36, 41–42). Thus, Petitioner argues that Denison teaches one of the two recited alternatives—disarming. We are persuaded by

Petitioner's argument and find that Denison teaches that its electronic key is configured to *disarm* the security device upon a matching (i.e., as a result of a determination of a match) of the unique security code stored in the memory of the security device with the security code stored in the memory of the programmable key. *See supra* Section II.A.2. This finding is supported by Denison, which discloses:

> During each access attempt, the key code in the electronic key is transferred from the key to the electronic lock using a secured communication method. The electronic lock can be unlocked if the key code it receives from the electronic key matches the key code stored in the memory of the lock.

Ex. 1003 ¶ 42.

iii. Plurality of Security Devices

Petitioner also relies on the combined teachings of Rothbaum and Denison for the recitation in claim 1 of a "plurality" of security devices, each having the unique security code stored in memory. -898 Pet. 33–34, 38–39, 42–43. Petitioner argues that

> a [person of ordinary skill in the art] would have understood that in retail, there is a need to display and secure many items of merchandise, which would require a plurality of "security systems," such as "strips or housings 12" [as taught by Rothbaum]. This is particularly true in stores where it is desirable to protect items of merchandise located in different departments, possibly on different sides of the store. A [person of ordinary skill in the art] would understand that as more items are in need of protection, it would be obvious and more cost-effective to simply add more modified Rothbaum devices, as opposed to ordering, designing and/or manufacturing a new "strip or housing 12" capable of protecting more items of merchandise. *See* Ex. 1015 at p. 70. Moreover, based on the teachings of Denison, which discloses multiple security devices

> each with the same "key code" and thus the same "access code" (*i.e.*, "security code") (*see* Ex. 1003 ¶¶ 36, 42, 45, 58), and knowledge in the art, a [person of ordinary skill in the art] would have been motivated to design the modified Rothbaum system such that multiple security systems are disarmed with the same "access code." This way, employees could be provided with keys containing the same code, allowing them to disarm multiple products within the store. *See* Ex. 1015 at p. 70.

Id. at 38–39. Petitioner's reasoning, supported by the testimony of Mr. Allison, is persuasive. Further, as explained above, Denison teaches a plurality of electronic keys, each with the same unique security code, for communication with the external computing devices and disarming a plurality of vending machine electronic locks. *See* Ex. 1003 ¶¶ 30, 42, 58, 59, Fig. 16 (depicting "Vending Machine 1" and "Vending Machine 2").

c. Summary

Based on the foregoing discussions of Rothbaum and Denison, we find that the combined disclosures of the references teach all of the limitations of claim 1. Patent Owner does not dispute that Rothbaum and Denison collectively teach the limitations of claim 1. Next, we address Petitioner's reasons as to why a person of ordinary skill in the art would have combined the teachings of Rothbaum and Denison.

d. Rationale to Combine Rothbaum and Denison and Reasonable Expectation of Success

Petitioner argues that Denison addresses various problems with mechanical locks on vending machines, such as key management and distribution and usage of keys. -898 Pet. 34–35 (citing Ex. 1003 ¶¶ 4–6, 9). For example, Denison discloses:

> One significant problem with conventional vending machines is the difficulties in managing the distribution and usage of the keys to ensure the security of the locks on the vending machines. The process of collecting money from the vending machines scattered at different places is a very manpower-intensive operation that requires many employees to go into the field with numerous mechanical keys for operating the locks on the vending machines. It requires a considerable amount of attention and efforts to manage and track the distribution of the keys to the field workers to keep the keys secure.
>
> Moreover, the mechanical keys and lock cores of vending machines are a point of attack for vandals. The keys can be lost or copied easily, and the stolen or copied keys may then be used by an unauthorized person to access the machines, and it is difficult to discover such misuses and security breaches. Also, a skilled vandal can easily pick or drill-out the lock core tumblers and measure the key cuts of the lock core tumblers to re-produce a like key and compromise the security. In the event a security breach is identified, the mechanical lock cores of the affected vending machines typically have to be manually replaced, which is a time-consuming and very costly process. Furthermore, mechanical keys and locks are devices that cannot be partially limited in operation they operate indefinitely if in use. Also, they do not have the ability to record access operation attempts of their operation.

Ex. 1003 ¶¶ 4–5.

Petitioner argues that these problems identified in Denison "would also have been problems present with the security system disclosed in Rothbaum." -898 Pet. 35 (citing Ex. 1015 ¶¶ 156–157). Petitioner's declarant, Mr. Allison, testifies that

> the problems resolved by Denison would also have been problems present with the security system disclosed in

> Rothbaum. . . . [T]he security device [in Rothbaum] is used to protect merchandise in the retail environment. In this environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals.

Ex. 1015 ¶ 156.

Petitioner argues that, to address the known problems with mechanical vending machine locks, Denison discloses the use of electronic, field-programmable keys and locks. -898 Pet. 34–35 (citing Ex. 1003 ¶¶ 9–10, 79). Denison describes the advantages of such electronic locks and keys:

> The use of the field-programmable electronic locks for vending machines provides an effective way to reduce theft and fraud in terms of unauthorized access to the machines. The electronic keys provide a greater level of key security compared to mechanical keys, as they cannot be copied as easily as conventional mechanical keys. The use of non-contact wireless data communication between the key and the lock prevents breeches of security associated with vandals measuring key cuts, copying keys and picking locks. The use of data encryption in the wireless communications between the key and the lock prevents the key code from being copied by electronic monitoring and eavesdropping. The data transmission between the key and lock may be implemented in the infrared range to provide close-proximity highly directional communication of secure codes to further prevent eavesdropping of the security codes and to prevent accidental unlocking of locks.
>
> The use of programmable electronic locks on vending machines and the associated electronic keys also provides advantages in terms of significant reduction in the costs associated with managing the distribution of the keys for unlocking the machines and the monitoring of the usage of the keys. Key IDs in addition to the key codes used in accessing the lock may be used to distinguish keys having the same key codes. Customized access limitations may be programmed by a

> supervisor into the electronic keys to restrict when and how they can be used to access the vending machines. Each key may also be programmed with a specific list of lock IDs identifying the electronic locks on vending machines that the key is allowed to unlock.

Ex. 1003 ¶¶ 9–10.

Petitioner contends a person of ordinary skill in the art "would have therefore been motivated to combine the teachings of Denison with Rothbaum to move from a mechanical key system to an electronic key system to achieve the advantages identified by Denison." -898 Pet. 35 (citing Ex. 1015 ¶¶ 156–157). Petitioner further contends a person of ordinary skill in the art would have

> fully understood how to create and use security devices with electronic keys well before the time of the alleged invention. With the Rothbaum security system, a [person of ordinary skill in the art] thus would have had a reasonable expectation of success in progressing from the Rothbaum mechanical key system to a programmable key system like that of Denison.

Id. at 36 (citing Ex. 1015 ¶¶ 158–162).

Patent Owner makes several arguments as to why Petitioner allegedly does not provide sufficient reasoning to justify the combination of Rothbaum and Denison, and in support it cites the testimony of Mr. Fawcett, a named inventor on the '247 patent. -898 PO Resp. 27–34 (citing Ex. 2013 ¶¶ 56, 57, 59, 60, 61–63, 65). For instance, Patent Owner disputes Petitioner's assertion that the "problems resolved by Denison would also have been problems present with the security system disclosed in Rothbaum." *Id.* at 30 (quoting -898 Pet. 35). Patent Owner argues:

> Nothing in Rothbaum . . . teaches or suggests that its mechanical key has any problems. *See* Ex. 2010, 227:23–228:1. Rothbaum's disclosure of a key is very straightforward,

> generally focusing on the basic functionality of the mechanical key. Ex. 1005 at 6:17–22. Rothbaum at no point mentions problems with such mechanical keys nor does it explicitly or implicitly suggest the mechanical key needs replacing or improvement. Ex. 2013 ¶60.

Id. at 30–31. Mr. Fawcett testifies similarly, citing column 6, lines 17–22 of Rothbaum in his testimony. *See* Ex. 2013 ¶ 60.[8]

Although we agree with Patent Owner that Rothbaum does not expressly disclose problems with its own key, Petitioner's contentions of obviousness are not premised on any such disclosure in Rothbaum. Rather, Petitioner contends, and Mr. Allison testifies, that the problems Denison identifies with respect to mechanical keys also would have been issues in Rothbaum's system, which uses mechanical keys. -898 Pet. 35; Ex. 1015 ¶ 156. Indeed, Mr. Allison explains that the security device of Rothbaum "is used to protect merchandise in the retail environment" and that, "[i]n this environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals." Ex. 1015 ¶ 156. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex. 1005, col. 6, ll. 20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 156. Therefore, we credit Mr. Allison's testimony that the problems Denison identifies with respect to mechanical keys also would have been issues in Rothbaum's system. *Id.*

[8] Although Mr. Fawcett cites column 7, lines 17–22 of Rothbaum, the quoted passage appears at column 6, lines 17–22 of Rothbaum. *See also* -898 PO Resp. 30–31 (citing Ex. 1005, col. 6, ll. 17–22).

Patent Owner also argues that Rothbaum's concerns with power conservation and device integration undermine Petitioner's rationale to combine. -898 PO Resp. 31–32. With respect to power conservation, Patent Owner argues:

> Rothbaum was also concerned with the need to conserve power in the closed loop system. Ex. 1005, 2:30–35. Denison's external computing device, keys and electronic lock, although working well on a vending machine without the same power concerns, would likely worsen the power drain that Rothbaum conscientiously seeks to minimize or avoid. Ex. 2013 ¶62.

Id. at 32. The cited portion of Rothbaum, however, describes a drawback of closed loop security systems when the power is off, such as during a power outage (Ex. 1005, col. 2, ll. 30–35), and Rothbaum discloses the use of "an energy conservation mode" in which a battery supplies power in such circumstances (*id.* at col. 3, l. 63–col. 4, l. 14). Rothbaum does not appear to have the same concerns with power conservation during normal operation, as it discloses the use of a closed system that is powered by an AC adapter when power is on. *Id.* at col. 3, ll. 63–64 ("The instant invention is a closed system when drawing power from its AC adapter."). We do not find that Rothbaum's disclosure of the use of an energy conservation mode when power is off undermines Petitioner's asserted rationale to combine. Indeed, Denison's disclosure that external computing device 426 is a laptop computer (Ex. 1003 ¶ 78) complements Rothbaum's energy conservation mode because a laptop computer would have a battery and need not be plugged into an outlet at all times. For example, Denison describes that "an operator may drive to the building in which the vending machine is located. *In his service vehicle*, the operator uses a laptop computer that functions as the external computer device to wirelessly communicate with the electronic lock of the vending machine by sending RF signals." *Id.* ¶ 86 (emphasis added).

Patent Owner argues that

> [a person of ordinary skill in the art] would also not modify Rothbaum to add components that are not integrated. During prosecution of its application, Rothbaum described that the "invention provides a fully integrated security device [which] advantageously enables alarm and detection circuitry and connections to sensors be located within one housing [in] a completely self-contained unit." Ex. 2017, 4. Modifying Rothbaum to include a programming station and programmable key would lead to additional circuitry being outside the housing and a reduction in simplicity and security. Ex. 2013 ¶63.

-898 PO Resp. 31–32 (alterations in original). As we understand Petitioner's contentions, however, the security device of the Rothbaum-Denison combination remains an integrated device having alarm and detection circuitry and sensor connections located within one housing. In particular, as discussed above, Rothbaum's strip or housing 12 is a "security device" as recited in claim 1. Petitioner does not argue that the programming station of the Rothbaum-Denison combination would have alarm and detection circuitry and sensor connections. Therefore, the inclusion of a programming station in the combined Rothbaum-Denison security *system* would not affect the location of these components in the security device itself.

Patent Owner also argues that "Rothbaum in particular seems to be concerned with avoiding too much complexity," and, therefore, "[m]odifying Rothbaum's system (as alleged by [Petitioner]) to supplant a simple mechanical key with Denison's distributed electronic key system would only increase complexity, costs, and the risk of improper installation by adding extensive additional electronic components." *Id.* at 31 (citing Ex. 1005, col. 2, ll. 1–6; Ex. 2013 ¶ 61). We do not disagree that adapting Rothbaum's system to include electronic keys as taught by Denison may result in a more complex system, but this alone does not undermine Petitioner's asserted rationale for the combination. As the U.S. Court of Appeals for the Federal Circuit has stated, "a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006). "Instead, the benefits, both lost and gained, should be weighed against one another." *Id.* (quoting *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000)).

Even if the proposed combination introduces complexities that are not present in the system of Rothbaum alone, we also consider the advantages that electronic keys provide, as described in Denison, such as greater security and improved key management and distribution. *See* Ex. 1003 ¶¶ 9–10. We find such advantages would have outweighed any added complexity and motivated a person of ordinary skill in the art to adapt Rothbaum's system to use electronic keys. In other words, based on the disclosures of the references, a person of ordinary skill in the art would have considered the use of electronic keys to be a significant *improvement* to the mechanical system of Rothbaum, regardless of the minimal added complexity of such a change.

Further, we find credible Mr. Allison's testimony that a person of ordinary skill in the art "would have had a reasonable expectation of success in combining the electronic key system of Denison with the security system of Rothbaum" (*see* Ex. 1015 ¶¶ 158–162) because it is consistent with the evidence of record, including Denison's disclosure that security systems using electronic keys were well-known as of the relevant time.[9] *See* Ex. 1002 ¶¶ 3–10; *see also* Ex. 1001, col. 1, ll. 49–56 (the '247 patent disclosing the known use of both "mechanical" and "electrical" keys to arm and disarm "alarm modules or other security devices" in the "Background of the Invention" section). Mr. Allison's testimony and the disclosure of Denison are evidence that implementing electronic keys in security devices was well within the skill level of a person of ordinary skill in the art.

Patent Owner also faults Mr. Allison, Petitioner's declarant, for not having proposed a specific design for the combined system in his declaration. -898 PO Resp. 33. However, the Federal Circuit has

> consistently held . . . that "[t]he test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art."

MCM Portfolio LLC v. Hewlett-Packard Co., 812 F.3d 1284, 1294 (Fed. Cir. 2015), *cert. denied*, 137 S. Ct. 292 (2016) (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). Therefore, we discern no requirement for Petitioner to provide evidence of a specific design that allegedly meets the limitations of the claims.

Further, the Supreme Court has held that, "if a technique has been used to improve one device, and a person of ordinary skill in the art would

[9] Although Mr. Fawcett testifies regarding increased complexity of the proposed Rothbaum-Denison system (Ex. 2013 ¶ 61), we do not find testimony from Mr. Fawcett rebutting Mr. Allison's testimony regarding reasonable expectation of success.

recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR*, 550 U.S. at 417. As discussed above, Mr. Allison provides credible testimony that a person of ordinary skill in the art would have had a reasonable expectation of success in combining the teachings of Rothbaum and Denison. *See* Ex. 1015 ¶¶ 158–162. Indeed, as Petitioner points out (-898 Reply 22), both of Patent Owner's declarants, Dr. Direen and Mr. Fawcett, testify that a person of ordinary skill in the art "would have been adept at turning design concepts into working products." *See* Ex. 2001 ¶ 34; Ex. 2013 ¶ 39. Therefore, we are persuaded by Petitioner's contention that a person of ordinary skill in the art would have had a reasonable expectation of success in combining the teachings of Rothbaum and Denison. *See* -898 Pet. 35–36 (citing Ex. 1015 ¶ 158).

Patent Owner further notes that "[e]ach of the independent claims of the '247 patent requires a security device 'attached to an item of merchandise' and an 'alarm' configured to activate in response to the integrity of the security device being compromised." -898 PO Resp. 29. Patent Owner argues that Petitioner "has not truly addressed the underlying fundamental question of why a [person of ordinary skill in the art] would venture out of the field of merchandise security systems with alarms to vending machines without alarm systems."[10] *Id.* at 30. Patent Owner,

[10] Although these arguments may be interpreted as directed to the question of whether Denison is analogous art to the '247 patent, we understand these arguments to be directed instead to the question of whether Petitioner's asserted rationale to combine is sufficient, based on Patent Owner's clarification during oral argument. Tr. 95:11–97:2.

therefore, contends Petitioner fails to provide a sufficient rationale to combine Rothbaum and Denison. *See generally id.* at 27–34.

We disagree with Patent Owner. Rather, having considered the arguments of the parties and based on the evidence of record, we are persuaded by Petitioner's contention that a person of ordinary skill in the art would have had reason to combine Denison's teachings of electronic keys and locks with the security system teachings of Rothbaum. *See* -898 Pet. 35–39. In particular, we find that a person of ordinary skill in the art would have been motivated to combine these teachings to take advantage of the numerous benefits of an electronic key system, as described in Denison. *See* Ex. 1015 ¶¶ 154–157; Ex. 1003 ¶¶ 9–10. For example, Denison discloses that "electronic keys provide a greater level of key security compared to mechanical keys, as they cannot be copied as easily as conventional mechanical keys." Ex. 1003 ¶ 9. Denison further discloses that the use of electronic locks and keys "provides advantages in terms of significant reduction in the costs associated with managing the distribution of the keys for unlocking the machines and the monitoring of the usage of the keys," and that "[c]ustomized access limitations may be programmed by a supervisor into the electronic keys to restrict" their use. *Id.* ¶ 10.

As discussed above, Mr. Allison provides credible testimony explaining that the security device of Rothbaum "is used to protect merchandise in the retail environment" and that, "[i]n this environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals." Ex. 1015 ¶ 156. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex. 1005, col. 6, ll. 20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 156.

Further, consistent with the evidence of record, including Mr. Allison's testimony, which we credit as discussed above, we find that a person of ordinary skill in the art would have had a reasonable expectation of success in combining Denison's electronic key teachings with the security system of Rothbaum. *See* Ex. 1015 ¶¶ 158–162. We also find that implementing electronic keys in security devices was well within the skill level of a person of ordinary skill in the art. *See id.*

e. Conclusion as to Claim 1

In summary, we find that the combination of Rothbaum and Denison teaches all of the limitations of claim 1, and we find that a person of ordinary skill in the art would have had reason to, and would have been motivated to, combine the teachings of Rothbaum and Denison in the manner asserted. Patent Owner does not present any objective evidence of nonobviousness as to any of the challenged claims. We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 1 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

3. Independent Claim 25

Method claim 25 recites many of the same limitations as system claim 1, and Petitioner's arguments are substantially similar for the two claims. *Compare* -898 Pet. 33–44 *with* -899 Pet. 34–46. For example, Petitioner relies on Rothbaum as teaching a “security device[] . . . configured to be attached to an item of merchandise” and comprising “an alarm configured to be activated in response to the integrity of the security device being compromised,” as well as a key for disarming the security device. -899 Pet. 34, 40, 41–45. As with claim 1, Petitioner notes that “Rothbaum does not disclose that [its] ‘key’ is ‘programmable’ or used with a ‘programming station,’” as recited in claim 25, and relies on Denison for these limitations. *Id.* at 34–36, 38–46. Patent Owner does not dispute that Rothbaum and Denison collectively teach the limitations of claim 25. We are persuaded that the combined disclosures of the references teach all of the limitations of claim 25, for the reasons stated by Petitioner and explained above with respect to the similar limitations of claim 1. *See supra* Section II.C.2.

Petitioner’s arguments as to why a person of ordinary skill in the art would have been motivated to combine the references’ teachings and would have had a reasonable expectation of success in doing so, as well as the supporting testimony of Mr. Allison, are similar to those made with respect to claim 1. *Compare* -898 Pet. 34–35 *with* -899 Pet. 35–37; *see* IPR2016-00899, Ex. 1015 ¶¶ 164–176. Patent Owner’s arguments in its Response likewise are similar. *Compare* -898 PO Resp. 27–34 *with* -899 PO Resp. 29–37; *see supra* Section II.C.2.d. For the reasons explained with respect to claim 1, we find that a person of ordinary skill in the art would have had reason to, and would have been motivated to, combine the teachings of Rothbaum and Denison in the manner asserted. Having reviewed the full record from trial, we conclude that Petitioner has shown, by a preponderance of the evidence, that claim 25 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

4. Independent Claim 31

Method claim 31 recites many of the same limitations as system claim 1 and method claim 25, and Petitioner's arguments are substantially similar. *Compare* -898 Pet. 33–44 *with* -899 Pet. 34–48. Petitioner primarily relies on its analysis of claim 25, but notes the differences between the two claims where applicable. -899 Pet. 46–48. In particular, claim 31 recites "the security code generated by the programming station and being unique thereto." Petitioner argues that Denison "discloses that the 'external computing device' (*i.e.*, 'programming station') randomly generates the 'access code,' meaning that it is unique to the external computing device, as the phrase is used in the '247 Patent." *Id.* at 47–48. Patent Owner argues that Petitioner "does not describe how a [person of ordinary skill in the art] would adapt the combination of Rothbaum/Denison to ensure that the code is unique *to the programming station*," given that "[n]ot all random codes are unique." -899 PO Resp. 37–38. Patent Owner's arguments are contingent on its proposed interpretation of "security code generated by the programming station and being unique thereto," with which we disagree for the reasons stated above. *See supra* Section II.A.4. Petitioner has shown sufficiently that the limitation is taught by Denison's generation of a six-digit random number (i.e., among 1,000,000 possible numbers) at the external computing device. *See* -899 Pet. 47–48 (citing Ex. 1003 ¶¶ 43, 79, 84); -899 Reply 27; *see also* Ex. 1016, 99:8–12 (Dr. Direen testifying that random number generation of "one in a hundred thousand" possibilities would be "unique as referred to in [a parent patent to the '247 patent with the same specification]"). We are persuaded that the combined disclosures of the references teach all of the limitations of claim 25, for the reasons stated by Petitioner and explained above with respect to the similar limitations of claims 1 and 25. *See supra* Sections II.C.2, II.C.3.

As to why a person of ordinary skill in the art would have been motivated to combine the references' teachings and would have had a reasonable expectation of success in doing so, Petitioner relies on its arguments regarding claim 25, which are similar to those made with respect to claim 1 and again supported by the testimony of Mr. Allison. *Compare* -898 Pet. 34–35 *with* -899 Pet. 35–37, 46–48; *see* IPR2016-00899, Ex. 1015 ¶¶ 164–176. Patent Owner's arguments regarding claims 25 and 31 in its Response likewise are similar to those regarding claim 1. *Compare* -898 PO Resp. 27–34 *with* -899 PO Resp. 29–37; *see supra* Section II.C.2.d. For the reasons explained with respect to claim 1, we find that a person of ordinary skill in the art would have had reason to, and would have been motivated to, combine the teachings of Rothbaum and Denison in the manner asserted. Having reviewed the full record from trial, we conclude that Petitioner has shown, by a preponderance of the evidence, that claim 31 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

5. Dependent Claim 12

Claim 12 depends from claim 1 and recites that "each of the plurality of security devices comprises a port for receiving one of the plurality of the programmable keys therein." Petitioner first points out that Denison's external computing device includes cradle 430 for receiving the electronic key so that the security code can be programmed into the electronic key. -898 Pet. 47. With respect to the claimed "security device," Petitioner explains, with supporting testimony from Mr. Allison, that

> a [person of ordinary skill in the art] would have found it obvious to incorporate an infrared port within the modified Rothbaum system disclosed above. Such an infrared port would require line of sight between the programmable key and the security device, thereby helping to prevent eavesdropping of the security codes and to prevent accidental disarming of the modified Rothbaum security device. Further, a [person of ordinary skill in the art] would have found it obvious to use the same type of key interface in the security device for receiving the programmable key ("electronic key") as used by the programming station ("external computing device"). In other words, it would be obvious to use a "cradle" (*i.e.*, port) for both the programming station and the security device.

Id. at 47–48 (citations omitted); *see* Ex. 1003 ¶¶ 9, 37, 77; Ex. 1015, 79–80.

Patent Owner contends that the assertions of Petitioner and Mr. Allison are conclusory and do not show sufficiently why a person of ordinary skill in the art would have modified the combined Rothbaum-Denison system to add a port to the security device for receiving a programmable key. -898 PO Resp. 35–36. Patent Owner further argues that Denison was "greatly concerned about tampering with conventional lock cores," and consequently "shield[ed] the transceiver and lock behind the buttons." *Id.* at 36–37 (citing Ex. 1003 ¶¶ 5, 37; Ex. 2007, 4; Ex. 2008, 3, 9). According to Patent Owner and Mr. Fawcett, a person of ordinary skill in the art would have been "greatly deterred from increasing access to the transceiver and lock of Denison by adding a port 'for receiving the programmable key therein,'" where the port would have been "visually detectable and invite[d] tampering, rather than being hidden behind the buttons." *Id.* at 37–38 (citing Ex. 2013 ¶¶ 75–77).

We disagree with Patent Owner. Petitioner provides sufficient reasoning as to why it would have been obvious to use a cradle (i.e., port) facilitating infrared communication with the electronic key for both the programming station and the security device. *See* -898 Pet. 47 (explaining that doing so would have "help[ed] to prevent eavesdropping of the security codes and to prevent accidental disarming of the modified Rothbaum security device"); Ex. 1015, 79–80. Petitioner's arguments are supported by the disclosure of Denison itself, which teaches infrared communication between the electronic key and lock and that infrared communication is "preferred because it is directional and short range." Ex. 1003 ¶¶ 9, 37, 77; *see* -898 Pet. 48. Further, Patent Owner's arguments do not address Petitioner's actual proposed combination, which involves modifying Rothbaum's system to use an electronic lock and key rather than a mechanical lock and key. Unlike the vending machine described in Denison, in Rothbaum's system, "the merchandise is accessible from the outside." *See* -898 Reply 26. Thus, we do not agree that a person of ordinary skill in the art would have been deterred from adding a port to the lock that already was attached to the merchandise and accessible.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 12 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

6. Dependent Claims 15 and 16

Claim 15 recites that "each of the plurality of programmable keys is configured to be inactivated after a predetermined period of time or a predetermined number of activations." Claim 16 depends from claim 15 and recites that "the programming station is configured to reactivate each of the plurality of programmable keys after the predetermined period of time or the predetermined number of activations." Petitioner argues that Denison teaches a personal computer for customizing "operation limits," for example, based on an employee's "work schedule" such that the key would only be enabled during certain hours. -898 Pet. 50–52 (citing Ex. 1003 ¶¶ 41, 60 ("The operation limits include, for example, time of data, date, number of days, number of accesses, number of accesses per day, etc."), 61, 78, Fig. 9 (showing "Key Access Control Limits," where the key is disabled at 4:00 PM on Saturday and enabled again at 7:00 AM on Sunday, and the key is limited to "100 accesses")). Petitioner further explains, with supporting testimony from Mr. Allison, that

> [w]hile Denison discloses the "personal computer" (a.k.a., "home base 210") performing this functionality, a [person of ordinary skill in the art] would have found it obvious to combine the functionalities of the home base and external computing device 426 (*i.e.*, "programming station"). Both are computers, communicate with the "electronic key 410" via a "cradle" and with the vending machines "wirelessly" over an "RF channel," and both perform "audit" functions. Thus, a [person of ordinary skill in the art] would have been motivated to combine the laptop and home base to reduce redundancies and the number of devices in the system.

Id. at 51 (citations omitted); *see* Ex. 1015, 83–85.

Patent Owner contends that Denison's disclosure of the personal computer causing the key to become reactivated at a certain time does not teach the limitation of claim 16 because the alleged reactivation is "only as a result of the initial programming by the computer, not the computer *re*activating the programmable key after a predetermined period of time." -898 PO Resp. 38 (citing Ex. 2013 ¶ 81). Claim 16, however, simply recites that the programming station is "configured to reactivate" the programmable key. We do not see any requirement that the programmable key physically be brought to the programming station for reactivation or that the programming station perform some active step at the time of reactivation. Rather, we are persuaded that disabling and re-enabling the electronic key in Denison, such that its operation is "limit[ed]" during the disabled time, teach the inactivation and reactivation recited in claims 15 and 16. *See* -898 Pet. 50–52; Ex. 1003 ¶¶ 60–61.

Patent Owner also argues that Denison "fails to disclose anything about the personal computer updating or customizing the limits more than once" and that a person of ordinary skill in the art would have "know[n] that there are security risks associated with allowing changes to be made to operating limits on keys after initial programming." -898 PO Resp. 39–40. Again, we disagree. Denison discloses that "key operation limits may be set by the supervisor 208 of the employee that uses the electronic key 212 to access vending machines in the field." Ex. 1003 ¶ 61. "The limits for each key may be customized depending on, for instance, the work schedule or habits of the employee to whom the key is given." *Id.* Figure 9 of Denison "shows an exemplary user interface screen 216 for prompting the user 208 to enter the limits." *Id.* It would make little sense to make such a user interface available to the employee's supervisor if the operation limits for a key could only be customized once, as Patent Owner contends. If that were the case, for example, the supervisor could never make any changes when the employee's "work schedule" or "habits" change. *See id.* Further, we agree with Petitioner that any concerns regarding security would be alleviated by the fact that the operation limits are set by the employee's supervisor, who likely would keep the personal computer secure. *See* -898 Reply 28 (citing Ex. 1003 ¶ 61).

We conclude that Petitioner has shown, by a preponderance of the evidence, that claims 15 and 16 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

7. Dependent Claim 21

Claim 21 recites that "the unique security code is unique to a particular retail establishment or retail store." Similar to claim 31 addressed above, Patent Owner's arguments are contingent on its proposed interpretation of the "unique" phrase in claim 21, with which we disagree for the reasons stated above. *See* -898 PO Resp. 40–43; *supra* Sections II.A.4, II.C.4. Petitioner has shown that a person of ordinary skill in the art would have found it obvious to use one external computing device (i.e., "programming station") at each store and that Denison generates a six-digit random number (i.e., among 1,000,000 possible numbers) at each external computing device. *See* -898 Pet. 38–40, 53–56; -898 Reply 28–29; Ex. 1016, 99:8–12. We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 21 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

8. Dependent Claim 22

Claim 22 recites that "each of the plurality of programmable keys is configured to provide the unique security code to each of the plurality of security devices for storing the unique security code." Petitioner relies on Denison's description of a "learning mode" where "the electronic lock receives a key code transmitted from an electronic key." -898 Pet. 53–54, 56 (quoting Ex. 1003 ¶¶ 7, 45).

Patent Owner argues that the passages relied upon by Petitioner are from separate embodiments, citing Denison's prosecution history to show that an electronic lock learning a randomly generated security code from an electronic key was added (in a continuation-in-part application) to the previous disclosure of a lock that learns, from a key, an access code set by the factory. -898 PO Resp. 43–45 & n.8 (citing Exs. 1003, 2007, 2020). Patent Owner asserts that Petitioner improperly relies on "the disclosures of . . . two disparate embodiments and do[es] not address the differences in the embodiments and why they might be combined." *Id.* at 45. Further, according to Patent Owner, "Denison discloses long range communication between the external computer as a 'home base' and the vending machine and lock," which "obviates the need to use the key as an intermediary." *Id.* at 45–46 (citing Ex. 1003 ¶ 73; Ex. 2013 ¶¶ 89–90).

We disagree. Immediately preceding the first paragraph cited by Petitioner, Denison states that "the present invention provides a vending machine with a field-programmable electronic lock. The electronic lock can *learn a key code from a corresponding electronic key*, a hand-held program unit, *and/or* an external computing device via wireless communications." Ex. 1003 ¶ 6 (emphases added). We agree with Petitioner that by using "and/or," "Denison discloses a vending machine that can learn the key code from any of these devices," including the electronic key, and, therefore, Petitioner is not relying on separate embodiments of Denison. *See* -898 Reply 29. Similarly, Patent Owner's citation to paragraph 73 of Denison regarding the use of the external computer as a "home base" in one scenario (shown in Figure 15) does not negate Denison's teaching of using the electronic key to program the lock or Petitioner's explanation regarding why and how a person of ordinary skill in the art would have combined the teachings of Rothbaum and Denison. *See* -898 PO Resp. 45–46; -898 Pet. 34–39, 53–54, 56; Ex. 1003 ¶¶ 6–7, 73.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 22 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

9. Dependent Claims 29, 30, and 34

Claims 29 and 34 recite "changing the [unique] security code in the programming station to a new [unique] security code." Claim 30, which depends from claim 29, recites "providing the new unique security code to each of the plurality of programmable keys." Petitioner explains, with supporting testimony from Mr. Allison, that

> Denison discloses that the "external computing device" (*i.e.* "programming station") randomly generates the security code ("access code"). Denison also discloses that the "access code" that is part of the "key code" (*i.e.*, "unique security code") stored in a vending machine can be changed. A [person of ordinary skill in the art] would have understood or found obvious from the disclosures of Denison that this would occur by using the "external computing device" to generate a new security code ("access code"), then transferring that new code

> to one or more "electronic keys" (*i.e.*, "programmable keys"), and finally using those keys to reprogram the locks of the vending machines ("security devices") with the new security code.

-899 Pet. 51–53 (citing Ex. 1003 ¶¶ 42, 43, 51, 58–59, 84, 85; IPR2016-00899, Ex. 1015, 83–85).

Patent Owner and Mr. Fawcett read the disclosure of Denison differently. Patent Owner contends that Denison only teaches the external computing device *generating* access codes (Ex. 1003 ¶ 84) and the electronic key *changing* the key code in the memory of the lock (*id.* ¶ 51). -899 PO Resp. 39. Therefore, according to Patent Owner, "Denison clearly does not disclose changing the security code in the programming station to a new access code—only changing the key code in the lock memory." *Id.* Patent Owner further argues that the fact that the key code in the lock is changed "does not necessarily mean that a key code in the external comput[ing] device is (or needs to be) changed" because the external computer device can use multiple security codes. *Id.* at 39–40. Patent Owner asserts instead that "a different stored code from the external computer [would] replace the old code in the vending machine." *Id.* at 40 (citing Ex. 2013 ¶ 94).

After reviewing the two different readings advocated by the parties, we are persuaded that Petitioner's and Mr. Allison's explanation of how a person of ordinary skill in the art would have understood Denison is correct. Denison describes in detail the beginning of a process where the external computing device randomly generates an access code, a following step where the external computing device "program[s]" the electronic key, and the end of the process where the electronic key is used to program (or reprogram) the vending machine lock. *See, e.g.*, Ex. 1003 ¶ 84–85. Given that the access code can change, the most consistent reading of Denison is that the same process would be followed, beginning with the external computing device, such that the access code is first changed in the external computing device and then provided to the electronic keys (for distribution to the vending machines).

Further, Denison expressly states that prior art mechanical locks needed to be "manually replaced" when a security breach occurs, which was "a time-consuming and very costly process." *Id.* ¶ 5. Denison's "field-programmable electronic locks," which can be reprogrammed rather than having to be manually replaced, are explicitly designed to solve those problems. *See id.* ¶¶ 9, 51 ("This field-programmability of the electronic lock makes key management significantly easier and cost-effective, and provides a greater level of key security compared to mechanical keys. In contrast, with conventional vending machines using mechanical locks, the mechanical keys may be copied or stolen easily, and the entire lock core of each of the vending machines affected has to be replaced in order to change to a different key."). Thus, we agree with Petitioner that a person of ordinary skill in the art would have understood from the disclosure of Denison, or at minimum found it obvious based on such disclosure, that the same process as initial programming would be followed for a changed access code, i.e., the external computing device would generate a new access code (replacing the old one) and then transfer it to the electronic keys so that they could use it to reprogram the vending machine locks. *See* -899 Pet. 51–53; -899 Reply 28–29; IPR2016-00899, Ex. 1015, 83–85, 92.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claims 29, 30, and 34 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

10. Dependent Claims 3–11, 13, 14, 17–20, 23, 24, 26–28, 32, 33, and 35–37

Petitioner asserts that dependent claims 3–11, 13, 14, 17–20, 23, 24, 26–28, 32, 33, and 35–37 would have been obvious based on the combination of Rothbaum and Denison. *See* -898 Pet. 44–57; -899 Pet. 48–58. Although Patent Owner does not make any specific arguments with respect to these claims, and thereby waived any arguments as to their patentability apart from Patent Owner's arguments regarding the parent claims addressed above, the burden remains on Petitioner to demonstrate unpatentability of all challenged claims. 35 U.S.C. § 316(e); *see* IPR2016-00898, Paper 11, 3 ("Patent Owner is cautioned that any arguments for patentability not raised in the response will be deemed waived."); IPR2016-00899, Paper 10, 3; *Dynamic Drinkware LLC, v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). We have analyzed Petitioner's contentions and cited evidence, including the supporting testimony of Mr. Allison, and agree with and adopt Petitioner's analysis regarding dependent claims 3–11, 13, 14, 17–20, 23, 24, 26–28, 32, 33, and 35–37. *See* -898 Pet. 44–57; -899 Pet. 48–58; Ex. 1015, 67, 73–89; IPR2016-00899, Ex. 1015, 74, 81–85, 90–96.

For example, we agree with Petitioner and find that the combination of Rothbaum and Denison teaches "a plurality of attachment cables, each attachment cable configured to be attached to one of the plurality of security devices," as recited in claim 3. *See* -898 Pet. 44–45 (citing Ex. 1005, col. 5, ll. 54–57, col. 6, ll. 1–4, Fig. 1). In particular, Rothbaum discloses: "Hard goods sensor 24, including a sensor housing 23, is attached to the article 22 . . . . Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12."). Ex. 1005, col. 5, l. 62–col. 6, l. 2. Similarly, with respect to claim 4, we agree with Petitioner and find that the combination of Rothbaum and Denison teaches that "each alarm of the plurality of security devices is configured to be activated in response to cutting the attachment cable attached to the security device or detaching the attachment cable from the security device." *See* -898 Pet. 44–45 (citing Ex. 1005, col. 10, ll. 31–36). In particular, Rothbaum discloses:

> When an alarm condition occurs, i.e., either by removing sensor plug 34 from jack 36, by cutting sensor cable 28, or by removing the sensor 24 from article 22, the alarm horn 126 will sound and the red LED 110 on the strip, which corresponds to the sensor which has been breached, will light.

Ex. 1005, col. 10, ll. 30–35. With respect to claim 5, we agree with Petitioner and find that the combination of Rothbaum and Denison teaches that "each of the plurality of security devices comprises a plurality of connection jacks, and . . . each attachment cable attached to one of the plurality of security devices is configured to be connected to one of the plurality of connection jacks." *See* -898 Pet. 44–45 (citing Ex. 1005, col. 6, ll. 1–14, col. 6, ll. 28–30, Fig. 1). Rothbaum discloses a security system "having either twelve or twenty-four jacks 36 on the strip 12," and Figure 1 of Rothbaum illustrates item cord 28 connecting, via sensor plug 34, to one of the jacks 36 on strip 12. Ex. 1005, col. 6, ll. 28–30, Fig. 1.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claims 3–11, 13, 14, 17–20, 23, 24, 26–28, 32, 33, and 35–37 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

D. Obviousness Ground Based on Rothbaum, Denison, and Ott (Claim 2)

Petitioner contends that claim 2 would have been obvious based on the combination of Rothbaum, Denison, and Ott. -898 Pet. 57–58. Claim 2 recites that "each of the plurality of security devices further comprises an adhesive."

Ott "relates to an apparatus for safeguarding a merchandise item against theft, having a safeguarding part for fixing to the merchandise item and having a connecting cord for connecting the safeguarding part to an object which is not at risk of theft." Ex. 1006, col. 1, ll. 5–9. Figure 9 of Ott is reproduced below.

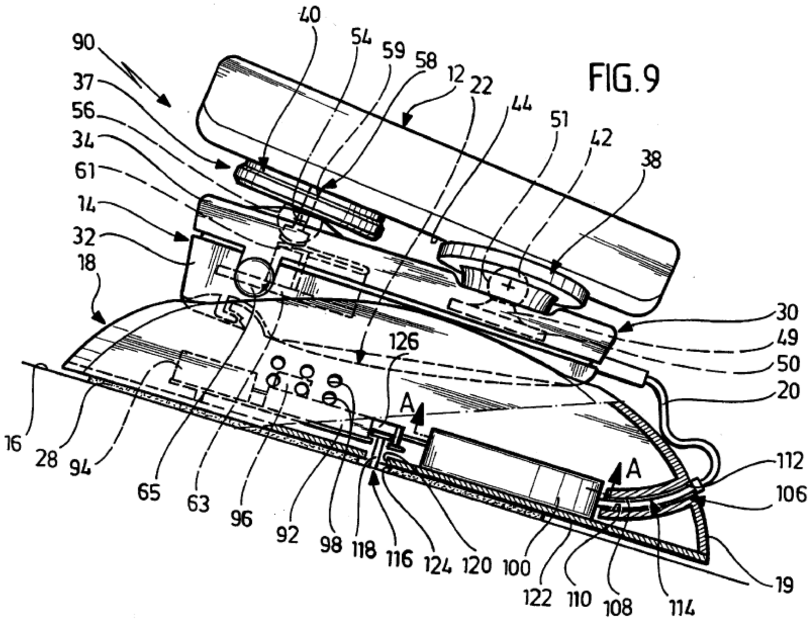


FIG.9

Figure 9 of Ott depicts apparatus 90 having holding part 18 affixed to an object such as lid 16 of a display case and having safeguarding part 14, which can be attached to item of merchandise 12. *Id.* at col. 7, ll. 26–40, col. 11, l. 43–col. 12, l. 2. Holding part 18 also has sensor element 116. *Id.* at col. 11, ll. 43–57. Ott also discloses switching plunger 118, which actuates microswitch 126 to turn on the alarm when holding part 18 is removed from lid 16. *Id.* at col. 11, l. 45–col. 12, l. 2.

Petitioner argues that

> a [person of ordinary skill in the art] would have been motivated to mount the “strip or housing 12” of Rothbaum onto a supporting structure using “adhesive,” thus meeting the limitation of Claim 2. Rothbaum discloses that the “housing” is “mounted” (*see* Ex. 1005 at 5:23–25), but it doesn’t specify how. A [person of ordinary skill in the art] would have understood and found obvious that it could be mounted with “adhesive,” such as tape. This would have been obvious from the teachings of Ott, or from basic knowledge in the art, including the fact that Rothbaum itself discloses use of “double-backed tape.” *See* Ex. 1005 at 5:62–67; *see also* Ex. 1015 ¶¶ 174–176.

-898 Pet. 57.

We are persuaded by Petitioner’s contentions. As an initial matter, we find that Ott is analogous to the claimed invention because Ott describes “an apparatus for safeguarding a merchandise item against theft” (Ex. 1006, col. 1, ll. 5–6) and, therefore, is in the same field of endeavor as the ’247 patent, as discussed above with respect to the analogousness of Rothbaum and Denison. *See, e.g.*, Ex. 1001, col. 1, ll. 24–29 (“The invention relates to security systems and methods for protecting merchandise from theft . . . .”); *supra* Section II.C.1.

Further, we find that a person of ordinary skill in the art would have had reason, and would have been motivated, to use an adhesive to mount Rothbaum’s strip 12 to a supporting structure. *See* Ex. 1015 ¶¶ 174–176.

As Petitioner correctly asserts (-898 Pet. 57), Rothbaum discloses that strip 12 is mounted: "Under normal operation, strip 12 is mounted in a location remote from the merchandise, and preferably near an AC outlet. Although the strip 12 is shown in a vertical orientation, it may be mounted in any orientation, including horizontally, without affecting its operation." Ex. 1005, col. 5, ll. 21–25. As Petitioner also correctly notes (-898 Pet. 57), Rothbaum discloses using an adhesive, such as "double-backed tape," for attaching other items. Ex. 1005, col. 5, ll. 62–67. Ott discloses that "holding part 18 of the apparatus 90 is fixed to the lid 16 by means of the adhesive pad 28, for example by means of a double-sided adhesive tape." Ex. 1006, col. 11, ll. 43–45. Thus, the evidence of record establishes that the use of adhesives for attaching items in security devices was well-known as of the relevant time and that using an adhesive would have resulted predictably in the attachment of two objects (the security device and the support).

Patent Owner relies on its arguments with respect to parent claim 1, and does not argue separately the limitation of claim 2. -898 PO Resp. 27–34; *see supra* Section II.C.2.d. We conclude that it would have been obvious to use an adhesive to mount strip 12 to a supporting structure in Rothbaum and that Petitioner has shown, by a preponderance of the evidence, that claim 2 would have been obvious based on Rothbaum, Denison, and Ott under 35 U.S.C. § 103(a). *See* Ex. 1015 ¶¶ 171–180; *see also KSR*, 550 U.S. at 417 ("[W]hen a patent simply arranges old elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, the combination is obvious." (internal quotation and citation omitted)).

E. Anticipation Ground Based on Belden (Claims 1, 3–34, 36, and 37)

We first determine whether Belden is prior art to claims 1, 3–34, 36, and 37. The ’247 patent claims the benefit of priority under 35 U.S.C. § 120 through a chain of applications to an application filed December 14, 2006. Ex. 1001, (63), col. 1, ll. 8–20. The patent also claims the benefit of priority under 35 U.S.C. § 119(e) to a provisional application filed December 23, 2005. *Id.*, (60), col. 1, ll. 8–20. The ’247 patent in its priority chain contains a “continuation-in-part” application filed June 27, 2011 (U.S. Patent Application No. 13/169,968 (Ex. 1009, “the ’968 CIP Application”)). Petitioner asserts that the challenged claims of the ’247 patent are not supported by prior U.S. Patent Application No. 12/770,321 (Ex. 1008, “the ’321 Application”), filed April 29, 2010, or by U.S. Patent Application No. 11/639,102 (Ex. 1007, “the ’102 Application”), filed December 14, 2006, and which published as Belden (Ex. 1002) on July 12, 2007. -898 Pet. 10–19; -899 Pet. 11–20. Petitioner asserts that because the ’102 and ’321 Applications[11] do not provide 35 U.S.C. § 112, first paragraph support for the challenged claims, Belden constitutes prior art to the challenged claims under 35 U.S.C. § 102(b). *Id.*

1. Legal Standard

To comply with the “written description” requirement of 35 U.S.C. § 112, first paragraph, an applicant must “convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in

[11] The substance of the ’102 and ’321 Applications is the same. *Compare* Ex. 1007 *with* Ex. 1008; *see* -898 Pet. 12; -898 PO Resp. 15 n.4. Thus, we refer herein to the ’102 Application for ease of reference.

possession of the invention. The invention is, for purposes of the 'written description' inquiry, whatever is now claimed." *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991) (emphases omitted). To "convey with reasonable clarity to those skilled in the art" may also be expressed in terms of whether the "necessary and only reasonable construction" to be given the disclosure by one skilled in the art clearly supports the limitation now claimed. *See Hyatt v. Boone*, 146 F.3d 1348, 1354 (Fed. Cir. 1998) ("We do not view these various expressions as setting divergent standards for compliance with § 112. In all cases, the purpose of the description requirement is 'to ensure that the inventor had possession, as of the filing date of the application relied on, of the specific subject matter later claimed by him.'") (quoting *In re Edwards*, 568 F.2d 1349, 1351–52 (CCPA 1978)).

One shows "possession" by descriptive means such as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. *Lockwood v. American Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997). "It is not sufficient for purposes of the written description requirement . . . that the disclosure, when combined with the knowledge in the art, would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose." *Id.*

The invention claimed does not have to be described *in ipsis verbis* to satisfy the written description requirement. *Union Oil Co. v. Atlantic Richfield Co.*, 208 F.3d 989, 1000 (Fed. Cir. 2000). The question of written description support should not be confused, however, with the question of what would have been obvious to the artisan. Whether one skilled in the art would find the instantly claimed invention obvious in view of the disclosure is not an issue in the "written description" inquiry. *In re Barker*, 559 F.2d

588, 593 (CCPA 1977). A description which renders obvious the invention for which the benefit of an earlier date is sought is not sufficient. *Lockwood*, 107 F.3d at 572.

2. Analysis

Petitioner argues that Belden is prior art to the challenged claims because the ’102 Application does not provide written description support for two limitations of independent claims 1, 25, and 31. *See* -898 Pet. 11–19; -898 Reply 10–16. We begin with these limitations and then proceed to the remaining limitations of the challenged claims.

a. Arming "Upon a Matching"

Petitioner argues that the ’102 Application does not provide written description support for the limitation that "each of the plurality of programmable keys is configured to *arm*[12] . . . each of the plurality of security devices upon a matching of the unique security code stored by the plurality of security devices with the unique security code stored by the plurality of programmable keys," as recited in claim 1 and similarly recited in claims 25 and 31. *See* -898 Pet. 11–16; -899 Pet. 12–17. We disagree.

The ’102 Application includes a number of broad statements that the security device is "controlled" upon a matching of the security codes in the

[12] Petitioner does not dispute that the ’102 Application provides written description support for the "disarm" aspect of the claims. *See* -898 PO Resp. 16 n.5. To the contrary, Petitioner contends that Belden (the publication of the ’102 Application) discloses disarming upon a matching of the security codes. *See* -898 Pet. 21–23; -899 Pet. 22–26. We agree. *See, e.g.*, Ex. 1002, Abstract, ¶ 63; Ex. 1007, p. 18, l. 14–p. 19, l. 7, p. 30.

programmable key and security device. For example, claim 1 of the ’102 Application recites the “security device being initially programmed with the security code from the key and subsequently being *controlled* by the key *upon matching* the security code of the key with the security code in the security device,” and claim 10 includes similar language. Ex. 1007, p. 25, ll. 8–10 (emphases added); *see also id.* at p. 24, ll. 3–6 (“Although the above description refers to the security code being a disarm code, it is understood that the code can activate and *control other functions and features of the security device* such as unlocking the device from the product, shutting off an alarm etc. without departing from the concept of the invention.” (emphasis added)), p. 26, l. 22–p. 27, l. 3 (claim 10). These portions do not specifically state that the “control[ling]” can be arming, however, so we look to other portions of the disclosure to determine the scope of such controlling.

The ’102 Application further discloses:

> In order to disarm alarm module 7, a validly programmed key 5 which is still within its active time period, will be placed into key receiving port 65 as shown in Fig. 5 and switch 85 is energized by depressing on member 87. Wireless communication systems 50 and 79 will deactivate alarm 51 enabling cable 11 to be removed from object 9 or from the alarm module jack 63 for sale of item 9 to a customer or for attachment of a new or different type of merchandise to the alarm module. After the desired product manipulation has occurred, *key 5 is then used to rearm the alarm module*. Again, key LED 90 and alarm module LED 61 will flash in various patterns to indicate that the disarming has occurred and then subsequently that the rearming has occurred.

Id. at p. 18, l. 14–p. 19, l. 1 (emphasis added). Thus, in addition to using the programmable key to disarm the alarm module, the key is "used" to re-arm the alarm module.

Figure 11A (which also appears in the '247 patent) shows that each time the programmable key is used, it is validated and checked to see if its security code matches the security code stored in the security device. Figure 11A of the '102 Application is reproduced below.

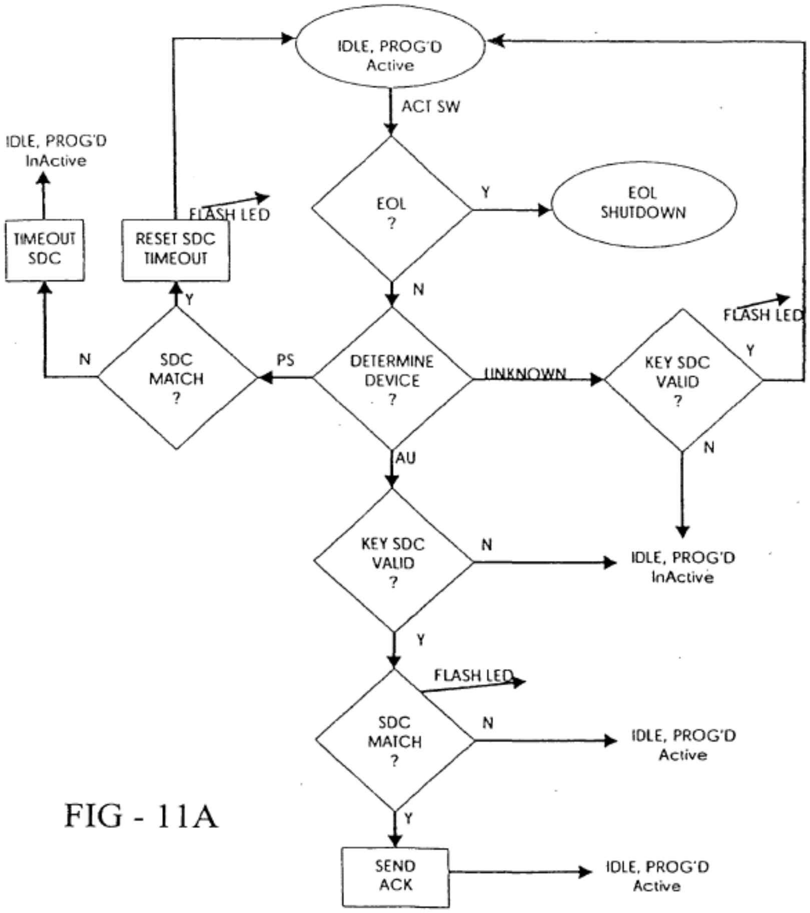


FIG - 11A

Figure 11A depicts "details of the operation of logic control circuitry 77 of programmable key 5," and shows "KEY SDC VALID?" and "SDC MATCH?" steps to determine the validity of the programmable key's security code and whether it matches the security code of the security device, respectively. *See id.* at p. 20, ll. 8–9. Importantly, Petitioner's declarant, Mr. Allison, agreed that a check is performed for a match of the security codes whenever the programmable key is used. Mr. Allison testified as follows:

> Q. Okay. And is it correct that [Figure] 11A teaches one of skill in the art that a check is done to see if an SDC is in the alarm unit and, if so, if it matches each time the key is used?
>
> MR. NORMAN: Objection. Form.
>
> A. Yeah. From this flowchart, there's only one arrow for alarm unit, and the first box is "key SDC valid?" with a yes or no.
>
> Q. . . . So that's a "yes"?
>
> A. That's a "yes."
>
> . . .
>
> Q. . . . If a key with an SDC is attached to an alarm module that has a different SDC, the key will not successfully rearm the alarm module because it won't get past the first step because the SDCs don't match?
>
> MR. NORMAN: Objection. Form.
>
> A. Yes. The key will not function in that alarm module.
>
> . . .
>
> Q. Okay. That first step happens whenever the usage of the key is with the alarm module. We already discussed that that first step always happens?
>
> A. Whatever your—one's intent is, *when you place the key into the port of the alarm module, there's a validity check.*
>
> *Q. Okay. Yeah. A comparison of the security code in the key and the security code in the alarm module?*
>
> *A. Yes.*

Ex. 2009, 135:11–20, 139:17–24, 140:24–141:8 (emphasis added).

We agree with Patent Owner and its declarant, Dr. Direen, that the '102 Application discloses using the programmable key to re-arm the security device, and that such re-arming involves reading the security code from the security device and determining whether it matches the security code of the programmable key. *See* -898 PO Resp. 17, 21–22 & n.6; Ex. 2001 ¶¶ 27–28, 51–55; Ex. 2012 ¶¶ 58, 60–61. Re-arming is simply arming in a particular context (i.e., arming when the security device has been armed previously at least once). *See, e.g.*, Ex. 2009, 91:24–92:7 (Mr. Allison agreeing that "[r]earmed would mean that it had to have been previously armed" and stating that he could not think of "any other differences between armed and rearmed"). We are persuaded, therefore, that the '102 Application provides sufficient written description support for arming the security device upon a matching (i.e., as a result of a determination of a match) of the security codes stored in the programmable key and security device, as recited in claims 1, 25, and 31.

b. "Configured to Communicate" and "Providing the [Unique] Security Code"

Petitioner also argues, with respect to the "configured to communicate" limitation of claim 1 and the "providing the [unique] security code" limitations of claims 25 and 31, that the '102 Application provides written description support only for wireless communications, whereas the challenged claims allegedly encompass both wireless and wired communications. *See* -898 Pet. 7, 17–19; -899 Pet. 7, 17–20.

We do not agree. Claim 1 of the '247 patent requires programmable keys that are "configured to communicate" with the programming station to "receive . . . the unique security code." Claims 25 and 31 similarly recite "providing the [unique] security code" to the programmable keys. The

’102 Application provides express disclosure of this subject matter. For example, the ’102 Application describes “ensuring that an active key always has sufficient internal power to receive the SDC and subsequently communicate with the alarm modules for disarming the modules when required.” Ex. 1007, p. 4, ll. 13–20. The ’102 Application further describes that “[a]nother aspect of the present invention is to enable the logic control circuit of the programming station to permanently inactivate the SDC in a smart key if the SDC contained therein does not match that of the programming station when in communication with the logic control circuit of the programming station.” *Id.* at p. 6, ll. 17–20; *see also id.* at p. 20, ll. 9–12, Fig. 12A (programming station performing the action of “SEND SDC TO KEY”). These two passages demonstrate that the inventors had possession, as of the filing of the ’102 Application, of a programmable key that is configured to communicate with the programming station to receive a security code, as recited in the independent claims of the ’247 patent.

Petitioner contends that “present invention” statements in the ’102 Application limit the scope of the disclosure of the ’102 Application to wireless communication only. *See* -898 Pet. 17–19; -898 Reply 12–16; -899 Pet. 17–20; -899 Reply 14–18. In particular, Petitioner argues that the ’102 Application “repeatedly limits its scope by using ‘present invention’ statements” and that “[n]owhere does the ’102 Application contain a disclosure of non-wireless communication.” *See* -898 Pet. 18; -899 Pet. 18–19. We do not agree because, as we find above, the “configured to communicate” and “providing the [unique] security code” limitations of the claims find express written description support in the ’102 Application’s description of communication between a programming station and programmable key to provide a security code, irrespective of the means by which the communication occurs. *See* Ex. 1007, p. 4, ll. 13–20, p. 6, ll. 17–20.

In support of its "present invention" argument, Petitioner cites, among other cases, *Research Corp. Techs., Inc. v. Microsoft Corp.*, 627 F.3d 859 (Fed. Cir. 2010). According to Petitioner, the Federal Circuit in *Research Corp.* found that "'the 1990 and 1991 Applications' limited to a 'blue noise mask' via 'present invention' statements could not provide support for the '772 patent, 'which claimed more than the disclosed blue noise mask.'" *See* -898 Reply 12–13, 16; -899 Reply 14, 18. Petitioner's characterization does not tell the whole story. Although the Court stated that "references to 'the present invention' strongly suggest that the claimed invention is limited to a blue noise mask," the Court went on to analyze the full disclosure of the priority applications, stating:

> The specification also explains that the "objects of the invention are accomplished by generating *a blue noise mask* which, when *thresholded at any gray level g, produces a blue noise binary pattern* appropriate for that gray level." Beyond this language, the figures in the patent only illustrate various aspects of a blue noise mask. Finally, all fifteen approved claims of the 1990 Application and all ten approved claims of the 1991 Application recite a "blue noise mask." Accordingly, the 1990 and 1991 Applications disclose only a blue noise mask.

Research Corp., 627 F.3d at 872 (citations omitted). The Court's determination was not based solely on "present invention" statements in the priority documents. Rather, the Court looked to the entire disclosure to determine that the priority applications "disclose only a blue noise mask." *See id.* Similarly, we look to the entire disclosure of the '102 Application, which expressly describes communication between a programming station and programmable key to provide a security code, irrespective of the means by which the communication occurs.[13] *See* Ex. 1007, p. 4, ll. 13–20, p. 6, ll. 17–20.

The pertinent inquiry is whether or not the ’102 Application provides written description support for communication between a programming station and programmable key to provide a security code, as recited in claims 1, 25, and 31 of the ’247 patent. For the reasons discussed above, we find that it does. That the ’968 CIP application to which the ’247 patent claims priority lists *additional* means or media through which communication takes place does not take away from the express disclosure of the ’102 Application.

c. Other Limitations

As explained above, we find that the ’102 Application provides sufficient written description support for arming the security device “upon a matching” of the security codes stored in the programmable key and security device, and the “configured to communicate”/“providing the [unique] security code” limitations, as recited in claims 1, 25, and 31. With respect to the remaining limitations, Petitioner asserts that Belden anticipates claims 1, 3–34, 36, and 37. *See* -898 Pet. 19–30; -899 Pet. 20–30. As such, Petitioner does not contend that Belden (the publication of the ’102 Application) fails to provide disclosure for the subject matter of these claims other than with respect to arming “upon a matching” and communicating the security code.

[13] Indeed, claim 1 of the ’102 Application broadly recites “a programming station for generating a security code into the key,” and claim 2, which depends from claim 1, limited that to a “wireless” interface for generating the security code into the key. Ex. 1007, p. 25, ll. 5–6, 12–13.

Patent Owner does not dispute that Belden discloses the other limitations of the claims. We have reviewed the citations provided by Petitioner and are persuaded that the ’102 Application (which published as Belden) provides sufficient written description support for claims 1, 3–34, 36, and 37.

d. Conclusion

Based on the record developed during trial, we determine that the ’102 Application conveys with reasonable clarity to those skilled in the art that, as of its filing date, the inventors were in possession of the inventions recited in claims 1, 3–34, 36, and 37 of the ’247 patent. Accordingly, these claims are entitled to the benefit of the filing date of the ’102 Application (December 14, 2006) and Belden is not prior art to these claims. Petitioner has not shown, by a preponderance of the evidence, that claims 1, 3–34, 36, and 37 are anticipated by Belden under 35 U.S.C. § 102(b).

F. Obviousness Ground Based on Belden and Sedon (Claims 2 and 35)

Petitioner additionally asserts that claims 2 and 35 would have been obvious based on the combination of Belden and Sedon. *See* -898 Pet. 31–32; -899 Pet. 30–33. Because we conclude that claim 2 is unpatentable over the combined teachings of Rothbaum, Denison, and Ott, *see supra* Section II.D, we need not separately assess the patentability of claim 2 based on the combination of Belden and Sedon, and thus need not determine whether Belden is prior art to claim 2.

Claim 35 depends from claim 31 and recites that “the arming or disarming comprises arming the security device upon a matching of the security code generated by the programming station with the security code stored by the security device." Thus, whereas parent claim 31 requires one of two actions ("arming or disarming"), dependent claim 35 recites that the claim comprises the former (i.e., "arming").[14] As explained above, we are persuaded that the '102 Application provides sufficient written description support for arming the security device upon a matching of the security codes stored in the programmable key and security device. *See supra* Section II.E.2.a. Thus, claim 35 is entitled to the benefit of the filing date of the '102 Application and Belden is not prior art to claim 35. Petitioner has not shown, by a preponderance of the evidence, that claim 35 would have been obvious based on Belden and Sedon under 35 U.S.C. § 103(a).

G. Patent Owner's Motions to Exclude

The party moving to exclude evidence bears the burden of proof to establish that it is entitled to the relief requested—namely, that the material sought to be excluded is inadmissible under the Federal Rules of Evidence. *See* 37 C.F.R. §§ 42.20(c), 42.62(a). In each of its Motions to Exclude, Patent Owner moves to exclude Exhibits 1016–1020 submitted by Petitioner with its Replies. As the parties' arguments are substantially the same in both cases, we will refer herein to the papers filed in Case IPR2016-00898 for ease of reference.

Exhibits 1018, 1019, and 1020 are dictionary definitions Petitioner cites in support of its interpretation of the phrase "upon a matching." Patent Owner argues that these exhibits should be excluded "as irrelevant and

[14] Dependent claim 36 recites that the claim comprises the latter (i.e., "disarming").

prejudicial under [Federal Rules of Evidence] 401 and 403, as well as outside the permissible scope of a reply." -898 Mot. 2–3. Patent Owner argues that Petitioner "provides no justification for why extrinsic evidence can be resorted to in this case, nor why these particular references (and not other dictionary and grammar sources) should control." *Id.* at 2.

We are not persuaded that Exhibits 1018, 1019, and 1020 should be excluded. Federal Rule of Evidence 401 provides that "[e]vidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." As Patent Owner acknowledges, Petitioner proffers these exhibits as evidence of the meaning of disputed claim language, specifically the phrase "upon a matching." *Id.* The meaning of this phrase is "of consequence in determining" whether the challenged claims are entitled to the benefit of the priority date of the '102 Application and whether they are anticipated or obvious over the asserted prior art, and Exhibits 1018, 1019, and 1020, even if not expressly relied upon in our Decision,[15] provide insight as to the meaning of the phrase "upon a matching." Therefore, we determine Exhibits 1018, 1019, and 1020 have some "tendency to make a fact more or less probable than it would be without the evidence" and are relevant under Federal Rule of Evidence 401.

Federal Rule of Evidence 403 provides that relevant evidence may be excluded "if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting

[15] We do not cite Exhibits 1018 and 1019 in our analysis. Nonetheless, we do not exclude this evidence from the record.

cumulative evidence." Patent Owner does not explain in its Motions why any of these factors substantially outweighs the probative value of Exhibits 1018, 1019, and 1020. We find the exhibits relevant and are not persuaded that they should be excluded under Federal Rule of Evidence 403.

We also are not persuaded by Patent Owner's arguments that Exhibits 1018, 1019, and 1020 should be excluded because they are "outside the permissible scope of a reply" and "should have been presented at the time of filing the petition." -898 Mot. 2–3. A motion to exclude is limited to arguing that material is inadmissible under the Federal Rules of Evidence. *See* 37 C.F.R. § 42.62(a), 42.64(c); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,767 (Aug. 14, 2012) ("A motion to exclude must explain why the evidence is not admissible (*e.g.*, relevance or hearsay) . . . ."). Even if Patent Owner's arguments were proper procedurally, however, Petitioner introduced the evidence in response to Patent Owner's arguments in its Responses regarding the meaning of "upon a matching." Specifically, Patent Owner argued that the phrase means "on or after a match," and Petitioner cited the dictionary definitions in support of its argument that Patent Owner's proposal was unreasonably broad because "upon" requires a "causal relationship . . . between matching of the security codes and arming or disarming the security devices" (i.e., "the keys [are] configured to arm or disarm the security devices *as a result of* the matching of codes").[16] *See* -898 PO Resp. 4–12; -898 Reply 5–6 & n.1 (citing Exs. 1018–1020); -898 Opp. 3–4. Pursuant to 37 C.F.R. § 42.23(b), "[a]

[16] As explained above, Patent Owner subsequently agreed with the "as a result of" portion of Petitioner's proposed interpretation during the hearing. *See supra* Section II.A.2; Tr. 43:13–45:5, 50:18–21.

reply may only respond to arguments raised in the corresponding . . . patent owner response." We determine that Petitioner's Reply arguments, and evidence in support thereof, with respect to the meaning of the phrase "upon a matching" are permissible reply arguments.

In its Motions to Exclude, Patent Owner also "objects to [Petitioner]'s misquotation and limited introduction of transcript testimony from Chris Fawcett (Ex. 1017) and Harry Direen (Ex. 1016)." -898 Mot. 3. Patent Owner identifies various citations in Petitioner's Replies to which Patent Owner objects as misquotations of testimony or incomplete citations of testimony. *Id.* at 3–5. Patent Owner argues that, under Federal Rule of Evidence 106, "statements in the transcript cannot be read out of context of other supporting statements" and that "misquoted or partial testimony should be considered in context with other testimony on the subject or the alleged testimony support should be excluded as unsupportive of [Petitioner]'s positions." *Id.* at 3.

Federal Rule of Evidence 106 provides: "If a party introduces all or part of a writing or recorded statement, an adverse party may require the introduction, at that time, of any other part—or any other writing or recorded statement—that in fairness ought to be considered at the same time." This Rule provides a basis for including, rather than excluding, evidence. In this case, Exhibits 1016 and 1017 are the complete transcripts of the depositions of Dr. Direen and Mr. Fawcett, respectively, and, therefore, the additional portions of Exhibits 1016 and 1017 that Patent Owner cites for our consideration are already part of the record in these proceedings and have been considered in rendering our Decision. As such, Patent Owner's request for relief under Federal Rule of Evidence 106 is moot.

Based on the foregoing, Patent Owner's Motions to Exclude are denied as to Exhibits 1018, 1019, and 1020, and dismissed as moot as to Exhibits 1016 and 1017.

III. ORDER

Petitioner has demonstrated, by a preponderance of the evidence, that claims 1 and 3–37 are unpatentable over Rothbaum and Denison and that claim 2 is unpatentable over Rothbaum, Denison, and Ott under 35 U.S.C. § 103(a). Petitioner has not demonstrated, by a preponderance of the evidence, that claims 1, 3–34, 36, and 37 are anticipated by Belden under 35 U.S.C. § 102(b), or that claim 35 is unpatentable over Belden and Sedon under 35 U.S.C. § 103(a). We need not determine whether claim 2 is unpatentable over Belden and Sedon under 35 U.S.C. § 103(a).

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–37 of the '247 patent have been shown to be unpatentable; and

FURTHER ORDERED that Patent Owner's Motions to Exclude are *denied-in-part* and *dismissed-in-part*.

This is a final 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.

PETITIONER:

Alan H. Norman
Anthony F. Blum
David B. Jinkins
Matthew A. Braunel
THOMPSON COBURN
tc-ipr-mti@thompsoncoburn.com
ablum@thompsoncoburn.com
djinkins@thompsoncoburn.com
mbraunel@thompsoncoburn.com

PATENT OWNER:

Gregory J. Carlin
Warren J. Thomas
David S. Moreland
John Harbin
MEUNIER CARLIN & CURFMAN LLC
mti.invue.iprs@mcciplaw.com
wthomas@mcciplaw.com

Trent A. Kirk
INVUE SECURITY PRODUCTS INC.
trentkirk@invue.com