Trials@uspto.gov
571-272-7822

Paper 35
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.

Case IPR2016-00892
Patent 8,884,762 B2

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

GALLIGAN, *Administrative Patent Judge.*

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

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314 and 37 C.F.R. § 42.108, Mobile Tech, Inc. ("Petitioner") challenges the patentability of claims 1–27 ("the challenged claims") of U.S. Patent No. 8,884,762 B2 ("the '762 patent," Ex. 1001), owned by InVue Security Products Inc. ("Patent Owner").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during trial. For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–27 of the '762 patent are unpatentable. *See* 35 U.S.C. § 316(e) ("In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.").

A. Procedural History

On April 14, 2016, Petitioner requested an *inter partes* review of claims 1–27 of the '762 patent. Paper 4 ("Pet."). Patent Owner filed a Preliminary Response. Paper 8 ("Prelim. Resp."). In a Decision on Institution of *Inter Partes* Review, the panel instituted trial of claims 1–27 on the following grounds of unpatentability:

1. Whether claims 1, 2, 5–9, and 11–27 are unpatentable under 35 U.S.C. § 102 as anticipated by Belden.[1]

2. Whether claims 3 and 4 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Belden and Sedon;[2]

[1] US 2007/0159328 A1, published July 12, 2007 (Ex. 1002).

[2] US 2005/0073413 A1, published Apr. 7, 2005 (Ex. 1004).

3. Whether claim 10 is unpatentable under 35 U.S.C. § 103(a) as having been obvious over Belden and Rothbaum;[3]
4. Whether claims 1, 5–20, 22–25, and 27 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum and Denison;[4] and
5. Whether claims 2–4, 21, and 26 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum, Denison, and Ott.[5]

Paper 9 ("Dec. on Inst."), 24–25.

During the trial, Patent Owner filed a Response (Paper 18, "PO Resp."), and Petitioner filed a Reply (Paper 22, "Pet. Reply"). In addition, Patent Owner filed a Motion to Exclude evidence. Paper 26. Petitioner filed an Opposition to Patent Owner's Motion to Exclude (Paper 29), and Patent Owner filed a Reply in support of its Motion to Exclude (Paper 30).

An oral hearing was held on June 14, 2017, a transcript of which appears in the record. Paper 32.

B. Related Matters

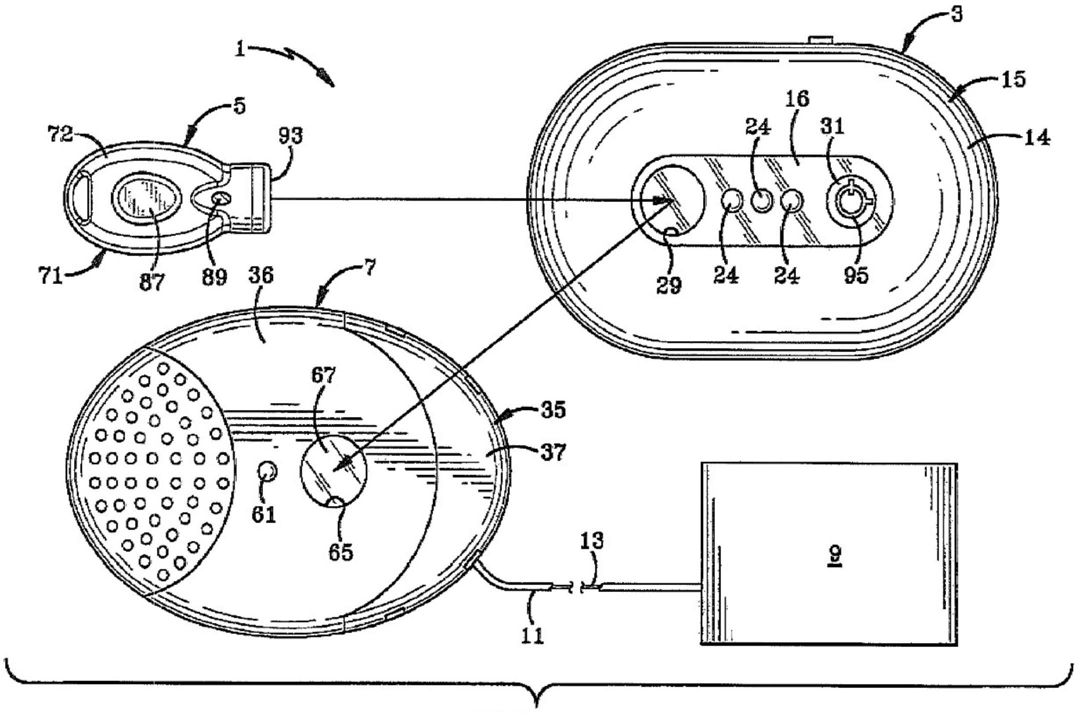
The parties indicate the '762 patent is at issue in *InVue Security Products Inc. v. Mobile Tech, Inc.*, 3:15-cv-00610 (W.D.N.C.). Pet. 1; Paper 7, 1. Petitioner also has filed petitions for *inter partes* review involving the same parties and related patents. Pet. 1; Paper 7, 1; Paper 13, 2–3; Paper 21, 1–2; IPR2016-00895, IPR2016-00896, IPR2016-00898, IPR2016-00899, IPR2016-01241, IPR2016-01915, IPR2017-00344, IPR2017-00345, IPR2017-01900, and IPR2017-01901. In addition, the

[3] US 5,543,782, issued Aug. 6, 1996 (Ex. 1005).
[4] US 2004/0201449 A1, issued Oct. 14, 2004 (Ex. 1003).
[5] US 6,380,855 B1, issued Apr. 30, 2002 (Ex. 1006).

parties identify certain patents and pending patent applications that may be affected by a decision in this proceeding. *See* Paper 7, 1; Pet. 1; Paper 13, 3; Paper 21, 2.

C. The '762 Patent and Illustrative Claim

The '762 patent relates to programmable security systems for protecting merchandise. See Ex. 1001, Abstract. Figure 1 of the '762 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 6:4–10. Programming station 3 randomly generates a unique security code (Security Disarm Code, or "SDC") that is transmitted via wireless (e.g., infrared) link to programmable key 5, which in turn stores the SDC in key memory. *Id.* at 6:29–31, 7:25–30, 9:7–13. 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 9:26–35.

Cable 11 extends between alarm module 7 and item of merchandise 9. Ex. 1001, 7:54–56, Fig. 1. 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 7:52–64. To disarm alarm module 7, programmable key 5 programmed with a valid SDC is placed into key receiving port 65 of alarm module 7, 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 without triggering an alarm. *Id.* at 10:47–59. Programmable key 5 then may be used to re-arm the alarm module. *Id.* at 10:59–63. "[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 10:66–11:4.

Claims 1 and 25 are independent claims. Claims 2–24 depend directly or indirectly from independent claim 1, and claims 26 and 27 depend from claim 25. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A programmable security system for protecting items of merchandise from theft, the programmable security system comprising:

> a programming station configured to generate a security code and having a memory for storing the security code;
>
> a programmable key configured to communicate with the programming station to receive the security code and to store the security code in a memory; and
>
> a security device comprising an alarm and a memory for storing the security code, the security device configured to be attached to an item of merchandise, the security device further comprising a switch configured to be actuated for activating the alarm in response to the integrity of the security device being compromised,
>
> wherein the programmable key is configured to communicate with the security device to arm or disarm the security device upon a matching of the security code stored in the memory of the security device with the security code stored in the memory of the programmable key.

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 [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,” and that “a key that is able to be programmed once is within the broadest reasonable interpretation of a ‘programmable key.’” Dec. on Inst. 5. The parties do not dispute this interpretation, and we do not perceive any reason or evidence that compels any deviation from the interpretation. Accordingly, we adopt the previous analysis for purposes of this Decision.

2. “Unique Security Code”

In the Decision on Institution, the panel stated that it “agree[s] with the parties that a randomly generated security code is within the broadest reasonable interpretation of ‘unique security code,’” but the panel did not further construe the term “unique security code.” Dec. on Inst. 5–6. The parties do not dispute this interpretation, and we do not perceive any reason or evidence that compels any deviation from the interpretation. Accordingly, we adopt the previous analysis for purposes of this Decision.

3. "Upon a Matching"

Claim 1 recites that "the programmable key is configured to communicate with the security device to arm or disarm the security device *upon a matching* of the security code stored in the memory of the security device with the security code stored in the memory of the programmable key" (emphasis added). Claim 25 recites "actuating the programmable key storing the security code to communicate with the security device to arm or disarm the security device *upon a matching* of the security code stored in the security device with the security code stored in the programmable key" (emphasis added).

Patent Owner argues in its Response that "upon a matching" should be interpreted to mean "on or after a match." PO Resp. 4–11. Petitioner argues that the phrase means "as a result of a determination of a match." Pet. Reply 5–11. During the hearing, Patent Owner agreed to the "as a result of" portion of Petitioner's proposed interpretation but disagreed 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.*; Pet. 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 and 25 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 3:32–37 (“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”), 4:4–8 (“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." Ex. 1001, 10:47–52. 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 10:52–59. "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 10:59–63.

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 10:66–11:4 (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 11:4–8 (emphasis added); *see also id.* at 4:48–61 ("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." PO Resp. 11. 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 6 (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 '762 patent. *Id.* at 7–9. 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.'" Pet. Reply 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, 9:26–35 (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.*; Pet. Reply 9. Indeed, claims 1 and 25 separately recite the security device "storing" the security code and "arm[ing] or disarm[ing]" 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* PO Resp. 7–10 (citing Ex. 1001, 3:67–4:3, 4:45–47, 9:26–39, 11:27–29).

We also are not persuaded by Patent Owner's arguments (PO Resp. 8–9) regarding Figure 13 of the '762 patent, which is reproduced below.

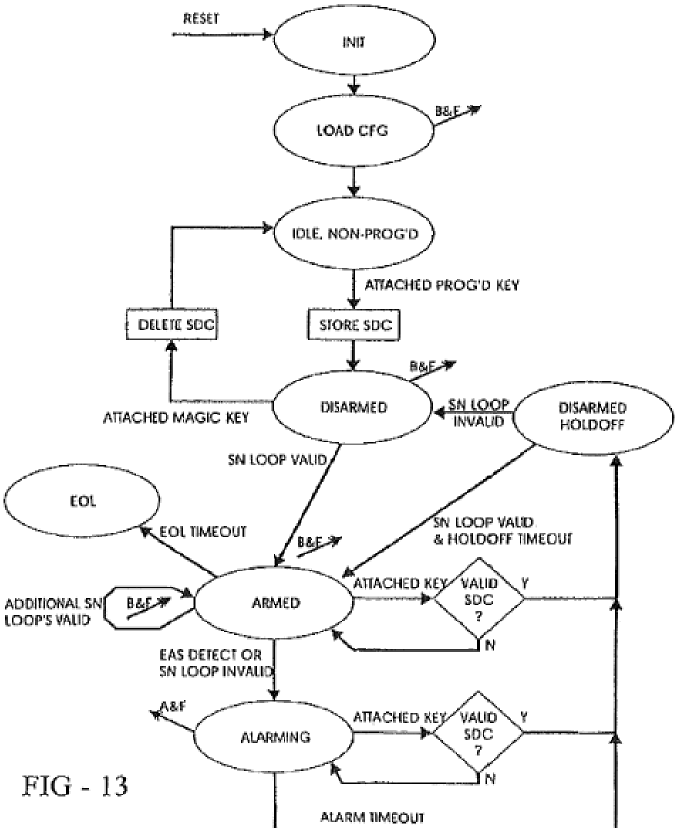


FIG - 13

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, 11:52–57. 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." PO Resp. 8. 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, 3:63–4:3, 7:50–8:4. 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.*, PO Resp. 17–18; Pet. Reply 6–7 & 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* Pet. 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 '762 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.

4. "Communicate" and "Configured to Communicate"

Petitioner argues that the terms "communicate" and "configured to communicate," as used in the challenged claims of the '762 patent, "encompass both wireless and wired forms of communication." 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, 3:4–16. Petitioner proposes this construction to argue that Application Number 11/639,102, to which the '762 patent claims priority, does not describe wired communication and, therefore, does not provide written description support for the claimed subject matter reciting "communicate" and "configured to communicate." *See* Pet. 17–20. In particular, Petitioner contends that the continuation-in-part application to which the '762 patent claims priority "broadened the meaning of the term 'communicate' 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." Pet. 19–20 (citing Ex. 1001, 3:4–19).

We do not agree that the recital of various "forms of data communication" (Ex. 1001, 3:4–19) in the '762 patent broadened the meanings of the term "communicate" and the phrase "configured to communicate" themselves. Rather, the "forms" of communication in the cited portion of the '762 patent merely represent examples of the media or means by which the communication occurs in various preferred embodiments. Ex. 1001, 3:4–19 (listing at least seven examples). Thus, Petitioner does not persuade us that we need to construe the terms "communicate" and "configured to communicate" expressly to encompass both wireless and wired communications.

B. Principles of Law

To establish anticipation, each and every element in a claim, arranged as recited in the claim, must be found in a single prior art reference. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). Although the elements must be arranged or combined in the same way as in the claim, "the reference need not satisfy an *ipsissimis verbis* test," i.e., identity of terminology is not required. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter 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). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness (i.e., secondary considerations). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. 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. Thaine Allison, testifies:

> [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 ¶ 22.

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.

PO Resp. 12 (citing Ex. 2001 ¶ 34). Patent Owner's declarants, Dr. Harry Direen and Mr. Christopher 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 the skill level of a person of ordinary skill in the art would have been that of a person having 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 in our obviousness analysis.

D. Unpatentability Challenge Based on Rothbaum and Denison (Claims 1, 5–20, 22–25, and 27)

Petitioner contends that the subject matter of claims 1, 5–20, 22–25, and 27 would have been obvious based on the combination of Rothbaum and Denison. Pet. 4, 35–54. 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 Allison Declaration to support its positions. *Id.* at 35–54.

1. Independent Claims 1 and 25

Petitioner relies on Rothbaum for teaching certain limitations of claims 1 and 25 and relies on Denison for teaching other limitations. *See* Pet. 35–46. 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. Analysis of Rothbaum

Claim 1 is directed to "[a] programmable security system for protecting items of merchandise from theft," and independent claim 25 is directed to "[a] method for protecting items of merchandise from theft." Petitioner contends Rothbaum discloses a security system for protecting merchandise, as illustrated in Figure 1 of Rothbaum, reproduced below. Pet. 35, 41, 45.

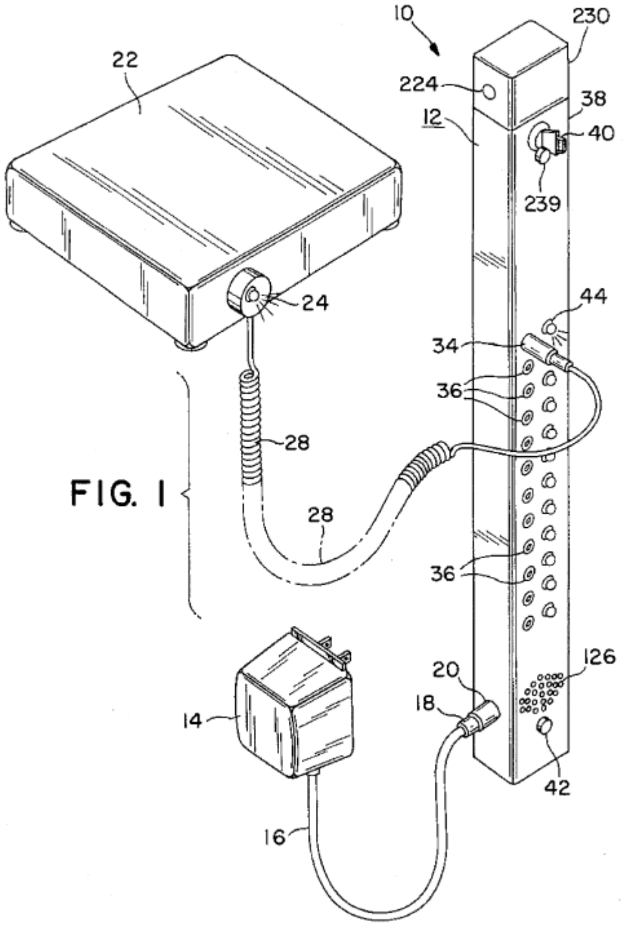


FIG. 1

In Figure 1, “a twelve jack security system 10 is shown which can protect twelve items of merchandise.” Ex. 1005, 5:10–11. We are persuaded by Petitioner’s argument, and we find Rothbaum discloses a security system for protecting items of merchandise from theft and a method for protecting items of merchandise from theft. *See, e.g.*, *id.* at 5:10–11, Fig. 1; *see also id.* at 1:6–9 (“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 Rothbaum’s disclosure of “strip or housing 12” connecting to article of merchandise 22 via “item cord 28” teaches a “security device configured to be attached to an item of merchandise,” as recited in independent claim 1, and "attaching a security device to an item of merchandise," as recited in independent claim 25. Pet. 35, 43–46 (citing, *inter alia*, Ex. 1005, Fig. 1, 5:62–6:4). We are persuaded by Petitioner's argument, and we find Rothbaum teaches these limitations of claims 1 and 25 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, 5:62–6:2 ("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."); *see also* Ex. 1015 ¶ 160.

Petitioner also argues Rothbaum discloses that its security device has an "alarm" (horn 126) and that Rothbaum's "tamper switch 225" teaches "a switch configured to be actuated for activating the alarm in response to the integrity of the security device being compromised," as recited in independent claims 1 and 25. Pet. 35, 40, 43, 45–46 (citing, *inter alia*, Ex. 1005, 6:15–22, 8:22–28, 12:10–18, Fig. 12). In particular, Petitioner argues that tamper switch 225 causes the horn to activate when the battery compartment is opened and that the integrity of the security device is compromised when the battery compartment is opened. *Id.* at 40. We are persuaded by Petitioner's argument, and we find Rothbaum teaches a security device having an alarm and "a switch configured to be actuated for activating 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, 12:10–18. We find that the integrity of the security device is compromised when the battery compartment is opened. *See* Ex. 1015, 77–78.

Petitioner further argues Rothbaum teaches a key for disarming the security device after a security breach occurs. Pet. 35 (citing Ex. 1005, 6:15–22, 8:22–28). We are persuaded by Petitioner's argument, and we find 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, 8:23–25.

Petitioner notes "Rothbaum, however, does not disclose that this 'key' is 'programmable' or used with a 'programming station,'" as recited in independent claims 1 and 25. Pet. 35. Petitioner relies on Denison for these limitations. *See id.* at 35–36.

b. Analysis of Denison

Petitioner contends "Denison discloses a security system having both a 'programmable key' and 'programming station.'" Pet. 35–36. Denison discloses the use of electronic locks for vending machines. Ex. 1003, Abstract, ¶¶ 2, 6. Figure 17 of Denison is reproduced below.

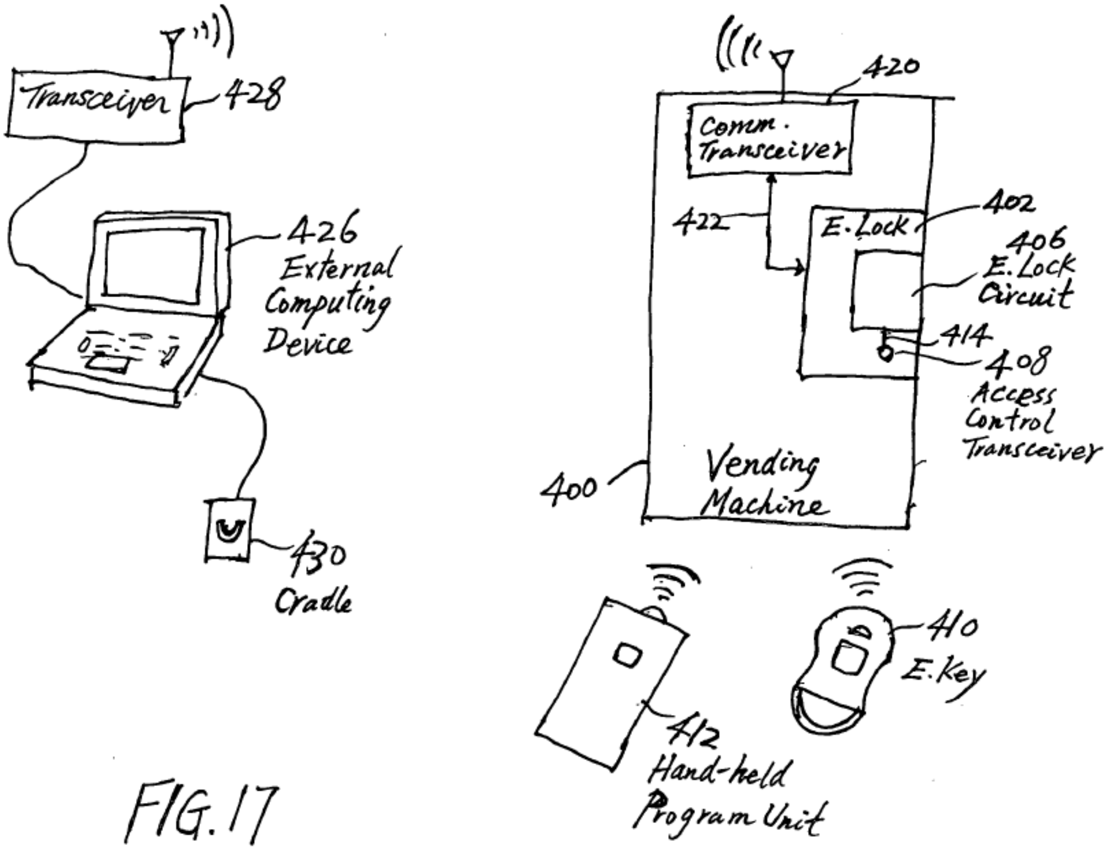


FIG. 17

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." Ex. 1003 ¶ 77.

i. Programming station

Petitioner contends Denison's "external computing device" is "a programming station configured to generate a security code and having a memory for storing the security code," as recited in claim 1. Pet. 36, 40–42 (citing Ex. 1003 ¶¶ 43, 79, 84, 86). In particular, Petitioner contends an "access code" stored within Denison's key code is a "security code" as claimed and further contends "[t]his access code is generated by the ‘external computing device’ (*i.e.*, ‘programming station’), which has a memory for storing the code.” Pet. 40 (citing Ex. 1003 ¶¶ 43, 79, 84).

We find Denison’s “external computing device” teaches a “programming station” that is “configured to generate a security code” and that has “a memory for storing the security code,” as recited in claim 1. These findings are 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 “external computing device 426 may also 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.” Ex. 1003 ¶ 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 we find, that Denison’s “access code” teaches a “security code,” as claimed. *See* Pet. 36, 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).”)).

Independent claim 25 recites “actuating a switch on a programming station so that the programming station generates a security code.”

Petitioner argues, and we agree, Denison discloses that external computing device 426 is a laptop computer. Pet. 44 (citing Ex. 1003 ¶ 78 ("[T]he external computing device 426, such as a laptop computer, is equipped with a wireless transceiver 428.")). Citing the testimony of its declarant, Mr. Allison, Petitioner contends a person of ordinary skill in the art "would readily understand from Denison that a keyboard or mouse, both of which contain numerous switches corresponding to the keys/buttons, would be used to cause the generation of the security code and that such use would have been obvious." Pet. 44–45 (citing Ex. 1015 ¶ 186). We are persuaded by Petitioner's argument, as supported by the testimony of Mr. Allison, and we find a person of ordinary skill in the art would have understood that a key or a button (having a switch) on the laptop would be used to cause the generation of the security code in Denison. *See* Ex. 1015 ¶ 186. Based on the evidence of record, including the testimony of Mr. Allison, we also conclude that actuating a switch, by pressing a button or key on the laptop, to cause the external computing device to generate an access code would have been obvious to a person of ordinary skill in the art based on Denison's disclosure that the external computing device is a laptop. *See id.* ¶ 186. Indeed, Denison discloses that the laptop is used by an operator. Ex. 1003 ¶ 86 (cited at Pet. 45) ("The operator also uses the laptop to program the same new access code into an electronic key").

ii. Programmable key

Petitioner further contends Denison's "electronic key" teaches "a programmable key configured to communicate with the programming station to receive the security code and to store the security code in a memory," as recited in claim 1, and "wherein a programmable key is configured to communicate with the programming station to receive and store the security code," as recited in independent claim 25. Pet. 35–36, 40–43, 45 (citing Ex. 1003 ¶¶ 6, 41–43, 60, 85, Figs. 1, 17). Petitioner argues "Denison discloses that the 'electronic key' communicates with the external computing device to receive the 'access code' (*i.e.*, security code) and to store it into a memory." *Id.* at 40–41 (citing Ex. 1003 ¶¶ 41, 85). We are persuaded by Petitioner's contentions, and we find Denison teaches the "programmable key" limitations of claims 1 and 25. These findings are 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 . . . .").

Petitioner further contends Denison teaches "the programmable key is configured to communicate with the security device to arm or disarm the security device upon a matching of the security code stored in the memory of the security device with the security code stored in the memory of the programmable key," as recited in claim 1. Pet. 36, 40, 43–44 (citing Ex. 1003 ¶¶ 36, 41, 42; Ex. 1015 ¶¶ 162–167). In particular, Petitioner contends

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 40 (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 we find Denison teaches that its electronic key is configured to communicate with the security device to *disarm* the security device upon a matching (i.e., as a result of a determination of a match) of the security code stored in the memory of the security device with the security code stored in the memory of the programmable key. 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.

Petitioner also contends Denison teaches "actuating the programmable key storing the security code to communicate with the security device to arm or disarm the security device upon a matching of the security code stored in the security device with the security code stored in the programmable key," as recited in independent claim 25. Pet. 36, 40, 44, 46 (citing Ex. 1003 ¶¶ 36, 37, 41, 42; Ex. 1015 ¶¶ 184–185). As with claim 1, Petitioner argues Denison teaches disarming the security device using the key. *Id.* at 44, 46. Petitioner further argues Denison teaches "actuating the programmable key," as recited in claim 25, because Denison discloses that "'START' button 36" is used to unlock the device. *Id.* at 44 (citing Ex. 1003 ¶ 37; Ex. 1015 ¶¶ 184–185). In particular, Denison discloses:

> [T]he electronic key 26 has a very simple profile, having only a "START" button 36 that can be activated by a user for lock opening and key code learning operations. In a preferred embodiment, the "START" button 36 need not be continuously pressed in order for the key to transmit the encrypted code to the lock. Instead, the user only has to only momentarily press the button 36, and the key will automatically stop transmitting after a few seconds . . . .

Ex. 1003 ¶ 37; *see also id.* at Fig. 1 (illustrating electronic key 26 having button 36 sending an unlock command). Based on this evidence, we find Denison teaches actuating its electronic key to communicate with the security device to *disarm* the security device upon a matching of the security code stored in the security device with the security code stored in the programmable key.

Based on the foregoing discussions of Rothbaum and Denison, we find that the combined disclosures of these references teach the limitations of independent claims 1 and 25. Patent Owner does not dispute that Rothbaum and Denison collectively teach all of the limitations of claims 1 and 25. *See* PO Resp. 26–33. 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 in support of its assertion that the subject matter of independent claims 1 and 25 would have been obvious.

c. *Combination of Rothbaum and Denison*

i. *Analogousness of Rothbaum and Denison*

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.” Pet. 37 (citing Ex. 1015 ¶¶ 172–173). The ’762 patent describes the “Field of the Invention” as follows:

> 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, 1:21–26. Therefore, the ’762 patent itself describes the relevant field of endeavor as “protecting merchandise from theft.” Furthermore, claims 1 and 25 are directed to a programmable security system and a method, respectively, “for protecting items of merchandise from theft.”

We find 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, 1:6–9.[6] Similarly, Denison’s disclosure of electronically-locking vending machines

[6] During oral argument, counsel for Patent Owner acknowledged that Rothbaum is analogous art to the ’762 patent. Tr. 94:21–22.

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]

ii. Rationale to Combine Rothbaum and Denison

Petitioner argues Denison addresses various problems with mechanical locks on vending machines, such as key management and distribution and usage of keys. Pet. 37 (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

[7] In its Response, Patent Owner argues that "[v]ending machines are not analogous to retail merchandise systems (using alarms) as [Petitioner] alleges." PO Resp. 28. 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 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 '762 patent. Tr. 95:11–97:2.

> 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 these problems identified in Denison "would also have been problems present with the security system disclosed in Rothbaum." Pet. 37 (citing Ex. 1015 ¶¶ 172–173). 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. As discussed above, the security device 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 ¶ 172.

Petitioner argues that, to address the known problems with mechanical vending machine locks, Denison discloses the use of electronic, field-programmable keys and locks. Pet. 37 (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.” Pet. 37 (citing Ex. 1015 ¶¶ 172–173). 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. In connection 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 39 (citing Ex. 1015 ¶¶ 174–178).

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 Christopher J. Fawcett, a named inventor on the ’762 patent. PO Resp. 26–33 (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 Pet. 37). 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. 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

[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* PO Resp. 30 (citing Ex. 1005, 6:17–22).

identifies with respect to mechanical keys also would have been issues in Rothbaum's system, which uses mechanical keys. Pet. 37; Ex. 1015 ¶ 172. 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 ¶ 172. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex. 1005, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 172. 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.*

Patent Owner also argues that Rothbaum's concerns with power conservation and device integration undermine Petitioner's rationale to combine. PO Resp. 31. 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. 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, 2:30–35), and Rothbaum discloses the use of "an energy conservation mode" in which a battery supplies power in such circumstances (*id.* at 3:63–4:14). 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 3:63–64 ("The instant invention is a closed system when drawing power from its AC adapter."). We do not find 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." Ex. 1003 ¶ 86 (emphasis added).

Patent Owner also argues:

> 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.

PO Resp. 31 (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" discloses a security device. 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 30–31 (citing Ex. 1005, 2:1–6; Ex. 2013 ¶ 63). 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 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.

Furthermore, 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 ¶¶ 174–178) 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, 1:47–54 (the '762 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. PO Resp. 32. However, the Federal Circuit has

[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.

> 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.

Furthermore, 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 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 ¶¶ 174–178. Indeed, as Petitioner points out (Pet. Reply 24), 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* Pet. 37–38 (citing Ex. 1015 ¶ 174).

Patent Owner further notes that "the independent claims of the '762 patent require 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." 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 29–30. Patent Owner, therefore, contends Petitioner fails to provide a sufficient rationale to combine Rothbaum and Denison. *See generally id.* at 26–33.

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* Pet. 37–39. 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 benefits of an electronic key system, as described in Denison. *See* Ex. 1015 ¶¶ 172–173; 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

[10] Although these arguments may be interpreted as directed to the question of whether Denison is analogous art to the '762 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.

"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 ¶ 172. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex.1005, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 172.

Furthermore, 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 ¶¶ 174–178. 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.*

d. Conclusion as to Claims 1 and 25

In summary, we find the combination of Rothbaum and Denison teaches all of the limitations of claims 1 and 25, and we find 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. Patent Owner does not present any objective evidence of nonobviousness as to any of the challenged claims. We conclude, therefore, that the subject matter of claims 1 and 25 would have been obvious based on the combined teachings of Rothbaum and Denison.

2. Dependent Claims 5–20, 22–24, and 27

Petitioner further contends the subject matter of dependent claims 5–20, 22–24, and 27 would have been obvious based on the combination of Rothbaum and Denison. Pet. 46–55. Although Patent Owner provides specific arguments only with respect to dependent claim 20 and does not provide specific arguments with respect claims 5–19, 22–24, and 27 in this asserted ground of unpatentability, the burden remains on Petitioner to demonstrate unpatentability of all challenged claims. 35 U.S.C. § 316(e); *see also Dynamic Drinkware LLC, v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). We have analyzed Petitioner's contentions and supporting evidence in light of the limitations recited in dependent claims 5–20, 22–24, and 27, and we agree with and adopt Petitioner's analysis, as explained more fully below with respect to the particular subject matter recited in the dependent claims. *See* Pet. 46–55.

a. Dependent Claims 5–10 and 27

Dependent claim 5 recites: "The programmable security system of claim 1, further comprising an attachment cable attached to the security device." Each of dependent claims 6–10 depends from claim 5 and recites further features with respect to the attachment cable of claim 5.

With respect to claim 5, we find the combination of Rothbaum and Denison teaches a programmable security system, as discussed above with respect to claim 1, "further comprising an attachment cable attached to the security device," as asserted by Petitioner. *See* Pet. 46–47 (citing Ex. 1005, 5:54–57, 6:1–4, 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, 5:62–6:2.

We also find the combination of Rothbaum and Denison teaches that "the alarm is configured to be activated" both "in response to cutting the attachment cable," as recited in claim 6, and "in response to detaching the attachment cable from the security device," as recited in claim 7. *See* Pet. 46–47 (citing Ex. 1005, 10:31–36). 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, 10:31–36.

With respect to claim 8, we find the combination of Rothbaum and Denison teaches that "the security device comprises a plurality of connection jacks" and that "the attachment cable is configured to be connected to one of the plurality of connection jacks." *See* Pet. 46–47 (citing Ex. 1005, 6:5–14, 6:28–30, 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, 6:28–30, Fig. 1.

We also find the combination of Rothbaum and Denison teaches that "the attachment cable extends between the security device and the item of merchandise," as recited in claim 9, and that "the at least one attachment cable comprises a helical coil," as recited in claim 10. *See* Pet. 46–47 (citing Ex. 1005, 5:62–63, 6:1–4, Fig. 1). Referring to Figure 1, Rothbaum discloses: "Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12. In the preferred embodiment, item cord 28 is coiled to allow for a longer length while minimizing entanglement." Ex. 1005, 6:1–4.

Claim 27 depends from independent claim 25 and recites that "the attaching comprises attaching a cable to the item of merchandise such that the cable extends between the security device and the item of merchandise." As with claim 9, which recites similar subject matter, we find that the combination of Rothbaum and Denison teaches the additional limitations of claim 27. *See* Pet. 55 (citing Ex. 1005, 5:54–57, 5:62–63, 6:1–4, Fig. 1).

b. Dependent Claims 11 and 12

Claim 11 depends from claim 1 and recites that "the security device further comprises a visual indicator configured to indicate a status of the security device," and claim 12 depends from claim 11 and recites that "the visual indicator is an LED." Rothbaum discloses:

> A bi-color LED is associated with each sensor circuit and is located on the housing next to the item cord connector. In its secure or non-alarm state, the LED displays a first color, e.g. green, indicating that the system is armed and the item of merchandise is protected. Upon the unauthorized removal of the sensor, the cutting of the item cable, or upon a similar security breach, the alarm will sound and the LED will change from its first color to a second or alarm color (green to red).

Ex. 1005, 3:38–47. Based on this disclosure of Rothbaum, we are persuaded by Petitioner's contentions, and we find, that the combination of Rothbaum and Denison teaches the limitations of claims 11 and 12. *See* Pet. 48–49 (citing Ex. 1005, 3:38–47).

c. Dependent Claims 13 and 14

Claims 13 and 14 depend from claim 1 and recite, respectively, that "the programmable key further comprises a visual indicator configured to indicate a status of the programmable key" and that "the programmable key comprises an internal battery." Denison discloses that "electronic key 26 also has a light-emitting diode (LED) 38 exposed through a hole in the housing of the key for indicati[ng] the operation status of the key," and it further discloses "electronic key 26 includes . . . a power source (e.g., a battery) 86." Ex. 1003 ¶¶ 37, 41. Based on this disclosure of Denison, we are persuaded by Petitioner's contentions, and we find, that the combination of Rothbaum and Denison teaches the limitations of claims 13 and 14. *See* Pet. 48–49 (citing Ex. 1003 ¶¶ 37, 41).

d. Dependent Claim 15

Claim 15 depends from claim 1 and recites that "the programming station comprises a switch configured to be actuated for programming the security code in the programmable key." As discussed above with respect to independent claim 25, Denison discloses that external computing device 426 (i.e., the "programing station") is a laptop and that "[t]he operator also uses the laptop to program the same new access code into an electronic key." Ex. 1003 ¶¶ 78, 86. Citing the testimony of its declarant, Mr. Allison, Petitioner contends a person of ordinary skill in the art "would have understood that a keyboard or mouse, both of which contain numerous switches corresponding to the keys/buttons, would be used to cause the programming, and, in any event, this would have been obvious." Pet. 48 (citing Ex. 1015, 84). We are persuaded by Petitioner's argument, as supported by the testimony of Mr. Allison, and we find a person of ordinary skill in the art would have understood that a key or a button (i.e., a switch) on the laptop (programming station) would be used to program the security code in the programmable key. *See* Ex. 1015, 84; Ex. 1003 ¶ 86. Therefore, we find that the combination of Rothbaum and Denison teaches the limitations of claims 15.

e. Dependent Claim 16

Claim 16 depends from claim 1 and recites that "the programming station comprises a port for receiving the programmable key therein." Referring to Figure 17, Denison discloses that "external computing device 426 may further include a cradle 430 for receiving the electronic key 410 or the hand-held programming unit 412." Ex. 1003 ¶ 78. Denison further discloses that "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." *Id.* ¶ 85. Petitioner contends that, "[b]ecause the 'cradle' provides an interface through which a security code ('access code') is programmed from the programming station ('external computing device') to the programmable key ('electronic key'), a [person of ordinary skill in the art] would understand that the 'cradle' is a 'port.'" Pet. 50 (citing Ex. 1015, 84–85). We are persuaded by Petitioner's argument, as supported by the testimony of Mr. Allison, and we find that Denison's cradle teaches a port for receiving a programmable key. *See* Pet. 49–50 (citing Ex. 1015, 84–85; Ex. 1003 ¶¶ 78, 85.

f. Dependent Claim 17

We are persuaded by Petitioner's argument, and we find, that the combination of Rothbaum and Denison teaches that "the programmable key is configured to wirelessly communicate with the security device," as recited in claim 17. *See* Pet. 51 (citing Ex. 1003 ¶ 37 ("The key 26 and the lock preferably communicate with each other wirelessly, which may be via an infrared or radio frequency (RF) channel. In a preferred embodiment, the wireless communications between the key and the lock is via infrared transmissions.")).

g. Dependent Claim 18

We are persuaded by Petitioner's argument, and we find, that the combination of Rothbaum and Denison teaches that "the security device comprises a power source," as recited in claim 18. *See* Pet. 51–52 (citing Ex. 1005, 9:56–65). In particular, Rothbaum discloses that its security device has a power supply back-up and that, "[i]n the event that either the AC adapter was pulled out of its outlet or the AC power main is turned off, the battery 226 provides the necessary power to keep the security system in its armed state." Ex. 1005, 9:56–62.

h. Dependent Claims 19 and 20

Claim 19 depends from claim 1 and recites that "the programmable key comprises a timer and . . . the programmable key is configured to be inactivated after a predetermined period of time." Claim 20 depends from claim 1 and recites that "the programmable key comprises a timer and . . .

the programmable key is configured to be inactivated if the security code stored in the memory of the programmable key is not reprogrammed or refreshed by the programming station within a predetermined period of time."

Petitioner contends:

> Denison also discloses "operation limits" that can be set for the electronic key such that the key becomes disabled (inactivated) after a "predetermined period of time" (e.g., "number of days"). *See* Ex. 1003 ¶ 60. It discloses that "a real-time clock integrated circuit (IC) 94" (i.e., "timer") is used for this purpose. *Id.* ¶ 41.

Pet. 50.

With respect to claim 19, we are persuaded by Petitioner's contentions, and we find the combination of Rothbaum and Denison teaches the limitations of claim 19. In particular, Denison discloses that its electronic key includes "a real-time clock integrated circuit (IC) 94 for generating data indicating the date and time." Ex. 1003 ¶ 41. Denison further discloses:

> [A]n electronic key may also be programmed with other types of limits of operation of the key. For instance, the key may be programmed with limit registers that contain values chosen by a supervisor to limit the operation of that particular key. In a preferred embodiment, the limit registers 200 (FIG. 4) are part of the non-volatile memory 52. The operation limits include, for example, time of data, date, *number of days*, number of accesses, number of accesses per day, etc. When the user of the key presses the button on the key to initiate a key code transmission, the microcomputer of the key first compares the limits set in the registers with a real-time clock in the key and an access counter in the key memory. *If any of the limits is exceeded, the key will not transmit the key code to the electronic lock and will terminate the operation*.

Ex. 1003 ¶ 60 (emphases added); *see also id.* at Fig. 9 (illustrating "Key Access Control Limits"). Thus, Denison teaches deactivating the key after any operating limit is exceeded, including "number of days," which teaches a "predetermined period of time."

Petitioner further contends:

> Claim 20 does not require that the key be reprogrammable or refreshable; rather, it requires that the key is configured to be inactivated if the security code stored in the memory of the programmable key is not reprogrammed or refreshed. In other words, the requirements of Claim 20 are met by a programmable key configured to be inactivated after a period of time.

Pet. 50–51.

Patent Owner argues that claim 20 "clearly requires that the security code, not the limits of operation, be refreshed to prevent inactivation." PO Resp. 34; *see also id.* at 35 ("[C]laim 20 requires that the reprogramming or refreshing occur *within* the period of time"). According to Patent Owner, however, "[a]t no point does [Petitioner] allege, or Denison teach or suggest, refreshing or reprogramming the *key code* in the key." *Id.* at 36.

We do not agree with Patent Owner that claim 20 requires reprogramming or refreshing the key. In the Decision on Institution, the panel explained:

> Claim 20 requires the inactivation of the programmable key if the condition to which Patent Owner refers does not happen "within a predetermined period of time." A condition that is *never* met is one that is not met "within a predetermined period of time," thus satisfying the conditional "if" language of claim 20.

Dec. on Inst. 23. Based on the full record at trial and applying the preponderance of evidence standard, we maintain the analysis of claim 20 in the Decision on Institution. Contrary to Patent Owner's arguments, reprogramming and refreshing the key code need not be performed to meet the limitations of claim 20. Rather, the claim requires that the key be configured to be inactivated if certain conditions (reprogramming or refreshing the security code) are not met within a predetermined period of time. Patent Owner appears to concede that Denison does not teach reprogramming or refreshing the access code in the key. *See* PO Resp. 36 (“At no point does [Petitioner] allege, or Denison teach or suggest, refreshing or reprogramming the *key code* in the key.”).

We find, therefore, Denison discloses a programmable key that is inactivated if the access code in the key is not reprogrammed or refreshed within a predetermined period of time because Denison does not describe refreshing or reprogramming the access code at all. As such, we are persuaded by Petitioner’s contention, and we find, that the combination of Rothbaum and Denison teaches the limitations of claim 20.

i. Dependent Claim 22

Claim 22 depends from claim 1 and recites that “the programming station is configured to generate a unique security code.” Petitioner argues Denison teaches randomly generating an access code. *See* Pet. 53 (citing Ex. 1003 ¶¶ 43, 84; Ex. 1015, 89). In particular, Denison discloses: “[T]he external computing device 426 may also 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.” Ex. 1003 ¶ 84. Denison also discloses that the access code is 6 digits having one million possible values. *Id.* ¶ 43 (“The next 6 digits in the key code are the access code (000,000 to 999,999).”). Based on this evidence, we find Denison discloses that external computing device 426 (i.e., the "programming station") is configured to generate randomly an access code having one million possible values, which we find to be within the broadest reasonable interpretation of a "unique security code," consistent with the claim interpretation set forth in the Decision on Institution.

Based on the evidence, therefore, we are persuaded by Petitioner's argument, and we find, that the combination of Rothbaum and Denison teaches that "the programming station is configured to generate a unique security code," as recited in claim 22.

j. Dependent Claims 23 and 24

Claim 23 recites: "The programmable security system of claim 1, further comprising a plurality of security devices." Claim 24 depends from claim 23 and recites that "each of the plurality of security devices is configured to communicate with the programmable key." With respect to these claims, Petitioner argues:

> 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 the "security systems" of Rothbaum (including "strips or housings 12"). 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. In addition, 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 replacement "strip or housing 12" capable of protecting more items of merchandise.
>
> Denison also discloses that there are multiple "vending machines accessible by an electronic key." Ex. 1003 ¶ 30. Thus, in light of these teachings, it would have been obvious to a

> [person of ordinary skill in the art] to combine the teachings of Rothbaum and Denison, wherein there are multiple security devices that communicate with the "electronic key" of Denison (i.e., "programmable key").

Pet. 53–54 (citing Ex. 1015, 89–90); *see id.* at 54–55 (citing Ex. 1003 ¶¶ 30, 42; Ex. 1005, 1:6–9).

We are persuaded by Petitioner's contentions. Indeed, Denison discloses, in Figure 16, "a schematic diagram showing vending machines accessible by an electronic key." Ex. 1003 ¶ 30; *see id.* at Fig. 16 (depicting "Vending Machine 1" and "Vending Machine 2"). Therefore, based on the evidence of record, we find the combination of Rothbaum and Denison teaches the limitations of claims 23 and 24. *See* Ex. 1015, 89–90.

k. Conclusion as to Dependent Claims 5–20, 22–24, and 27

In summary, we find the combination of Rothbaum and Denison teaches the limitations of dependent claims 5–20, 22–24, and 27, and, for the reasons discussed with respect to independent claims 1 and 25, we find 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. We conclude that the subject matter of dependent claims 5–20, 22–24, and 27 would have been obvious based on the combined teachings of Rothbaum and Denison.

E. Unpatentability Challenge Based on Rothbaum, Denison, and Ott (Claims 2–4, 21, and 26)

Petitioner additionally contends that the subject matter of claims 2–4, 21, and 26 would have been obvious based on the combination of Rothbaum, Denison, and Ott. Pet. 4, 55–58. Claim 2 depends from claim 1 and recites that "the security device further comprises a fastener." Claim 3 depends from claim 2 and recites that "the fastener comprises an adhesive," and claim 4 depends from claim 3 and recites that "the adhesive is configured to secure the security device to a support." Claim 21 depends from claim 1 and recites that "the switch is configured to engage a support when the security device is attached thereto, and wherein the switch is configured to be actuated for activating the alarm in response to removal of the security device from the support." Claim 26 depends from independent claim 25 and recites that "the attaching comprises attaching the security device to a support such that the switch of the security device engages the support."

1. Overview of Ott

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, 1:5–9. Figure 9 of Ott is reproduced below.

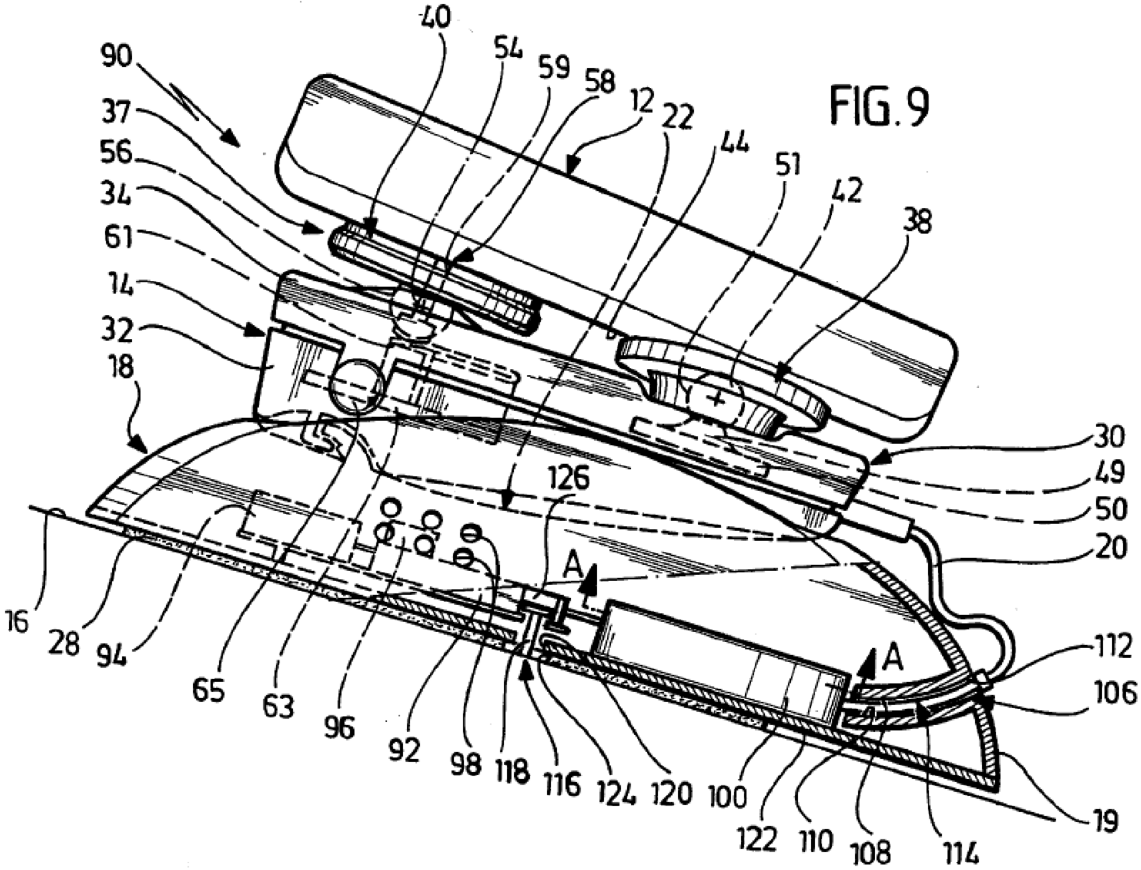


FIG.9

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 7:26–40, 11:43–12:2. Holding part 18 also has sensor element 116. *Id.* at 11:43–57. 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 11:45–12:2.

2. Claims 2–4

Petitioner contends:

> 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 (*i.e.*, "support") using an "adhesive." 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 via fasteners, such as bolts, or fasteners with "adhesive," such as tape. This would have been obvious from the teachings of Ott (*see* Ex. 1006 at 7:27-31), or from basic knowledge in the art, including that Rothbaum itself discloses use of "double-backed tape" as a fastener, thus meeting the limitations of Claims 2-4. *See* Ex. 1005 at 5:62-67; *see also* Ex. 1015 ¶¶ 196-98.

Pet. 56.

We are persuaded by Petitioner's contentions. As an initial matter, we find Ott is analogous to the claimed invention because Ott describes "an apparatus for safeguarding a merchandise item against theft" (Ex. 1006, 1:5–6) and, therefore, is in the same field of endeavor as the '762 patent, as discussed above with respect to the analogousness of Rothbaum and Denison. *See, e.g.*, Ex. 1001, 1:21–22 ("The invention relates to security systems and methods for protecting merchandise from theft . . . .").

Furthermore, we find 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 ¶¶ 196–198. As Petitioner correctly asserts (Pet. 56), 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, 5:21–25. As Petitioner also correctly notes (Pet. 56), Rothbaum discloses using an adhesive such as "double-backed tape" for attaching other items. Ex. 1005, 5:62–67. 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, 11:43–45. 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).

We conclude that it would have been obvious to use an adhesive to mount strip 12 to a supporting structure in Rothbaum, and, therefore, we conclude the subject matter of claims 2–4 would have been obvious to a person of ordinary skill in the art based on the combination of Rothbaum, Denison, and Ott. *See* Ex. 1015 ¶¶ 196–198; *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).

3. Claims 21 and 26

Petitioner contends Ott's disclosure of switching plunger 118, which actuates microswitch 126 to turn on the alarm when holding part 18 is removed from lid 16 (Ex. 1006, 11:45–12:2), teaches the switch configurations of claims 21 and 26. Pet. 57–58. Petitioner further contends:

> A [person of ordinary skill in the art] would have been motivated to include the "switching plunger," as disclosed in Ott, on the bottom of Rothbaum's "housing." *See* Ex. 1006 at 11:45-12:2. That way, the alarm in the "security system" of Rothbaum would also activate if the entire housing were removed from its supporting structure, thus providing an extra layer of security and meeting the claim limitations of Claims 21 and 26. This especially would have been obvious given that Rothbaum discloses that its "housing" has anti-tamper capability, including a "tamper switch" that sets off the alarm when the "battery

> compartment" of the "housing" is removed. *See* Ex. 1005 at 12:10-18; *see also* Ex. 1015 ¶¶ 199-200.

Pet. 56–57.

We are persuaded by Petitioner's contentions. In particular, Ott discloses:

> In order to ensure that the apparatus 90 cannot be removed unnoticed together with the merchandise item 12 from the lid 16, the apparatus 90 comprises, in addition to the switching plunger 59—engaging against the merchandise item 12—and the corresponding switching element 61, a further sensor unit 116 for monitoring the proper fitting of the holding part 18 to the object 16 which is not at risk of theft. This sensor element 116 comprises a switching plunger 118, which engages through a central through hole 120 in the bottom wall 122 in the housing 19 of the holding part 18 and also through a corresponding cutout 124 in the adhesive pad 28 and engages against the lid 16. The switching plunger 118 is electrically connected to a switching element—disposed in the housing 19—in the form of a microswitch 126, which in turn is connected to the monitoring circuit 92. If the holding part 18 is removed from the lid 16 in an unauthorized manner, then the switching plunger 118, which is spring-loaded in the direction of the lid 16, actuates the microswitch 126. This last is detected as an alarm situation by the monitoring circuit 92, and a visual and acoustic alarm is thereupon output by means of the piezoelectric crystal 96 and the light-emitting diode 65 in the same way as in the event of unauthorized removal of the merchandise item 12 from the safeguarding part 14.

Ex. 1006, 11:45–12:2. We find a person of ordinary skill in the art would have been motivated to include Ott's "switching plunger" in the security device of Rothbaum because this would provide an extra layer of security in the event that the entire housing in Rothbaum were removed. This is supported by Mr. Allison's testimony that "the alarm in the 'security system' of Rothbaum would also activate if the entire housing were removed from its supporting structure, thus providing an extra layer of security and meeting the claim limitations of Claims 21 and 26." Ex. 1015 ¶ 199. Mr. Allison further testifies that such a modification also "would have been obvious given that Rothbaum discloses that its 'housing' has anti-tamper capability, including a 'tamper switch' that sets off the alarm when the 'battery compartment' of the 'housing' is removed." Ex. 1015 ¶ 200 (citing Ex. 1005, 12:10–18). Mr. Allison's testimony is consistent with the disclosures of the references and is persuasive.

We conclude, therefore, that the subject matter of claims 21 and 26 would have been obvious to a person of ordinary skill in the art based on the combination of Rothbaum, Denison, and Ott.

F. Availability of Belden as Prior Art

The '762 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, at (63). The '762 patent also claims the benefit of priority under 35 U.S.C. § 119(e) to a provisional application filed December 23, 2005. *Id.* at (60). The '762 patent in its priority chain contains a "continuation-in-part" application filed June 27, 2011 (Application Number 13/169,968 ("the '968 CIP application") (Ex. 1009)). Petitioner asserts that the challenged claims of the '762 patent are not supported by prior Application Number 12/770,321, filed April 29, 2010, or by Application Number 11/639,102 (Ex. 1007, "the '102 Application"), filed December 14, 2006, and which is the application published July 12, 2007 (Ex. 1002; Belden). Pet. 10–20. Petitioner asserts that because Application Number 11/639,102 does not provide 35 U.S.C. § 112, first paragraph, support for the challenged claims, the published Application Number 11/639,102 constitutes 35 U.S.C. § 102(b) prior art. Pet. 10–20.

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 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 of § 112 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 1572.

2. Disclosure of Belden – Arming upon a Matching

Petitioner argues that the '102 Application does not provide written description support for the limitation that "the programmable key is configured to communicate with the security device to *arm*[11] . . . the security device upon a matching of the security code stored in the memory of the security device with the security code stored in the memory of the programmable key," as recited in claim 1 and similarly recited in claim 25. 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 programmable key and security device. For example, claim 1 of the '102

[11] Petitioner does not dispute that the '102 Application provides written description support for the "disarm" aspect of the claims. *See* PO Resp. 15 n.5.

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 (emphasis 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 ’762 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.

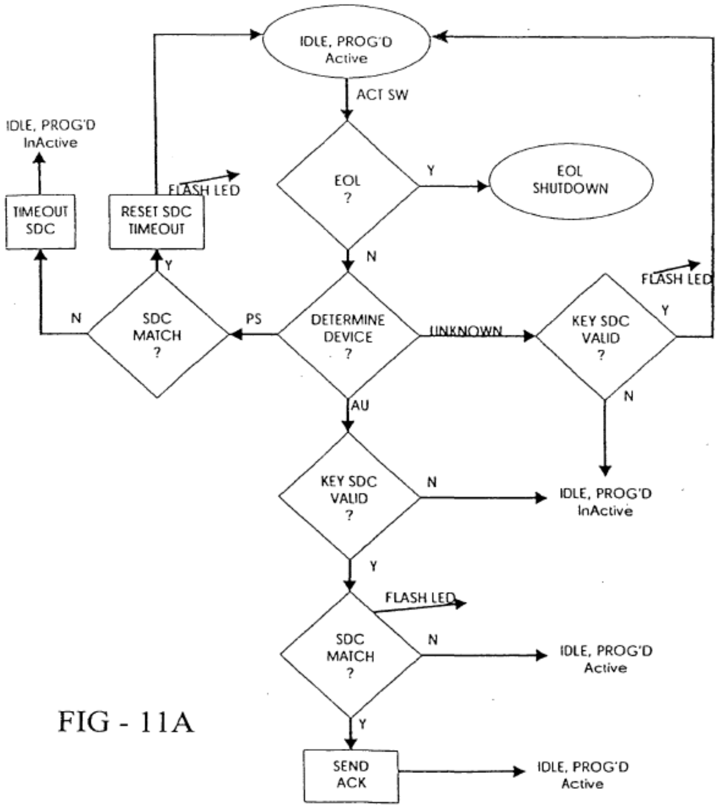


FIG - 11A

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. *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* PO Resp. 15–16, 20–21 & n.6; Ex. 2001 ¶¶ 27–28, 51–55; Ex. 2012 ¶¶ 58, 60–61. As re-arming is simply arming in a particular context (i.e., arming when the security device has been armed previously at least once), we are persuaded 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 and 25.

3. Disclosure of Belden – Communication

Petitioner additionally asserts that Belden is prior art because the ’102 Application provides written description support only for wireless communications whereas the challenged claims allegedly encompass both wireless and wired communications. *See* Pet. 6–7, 17–20.

We do not agree. Independent claims 1 and 25 of the ’762 patent require a programmable key that communicates or is “configured to communicate” with the programming station and with the security device. 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, 4:17–20. 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 6:17–20. 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 and with the security device, as recited in the independent claims of the ’762 patent. The ’102 Application’s disclosure that the key and the alarm modules communicate with each other (Ex. 1007, 4:17–20) also demonstrates that the inventors had possession, as of the filing of the ’102 Application, of the subject matter of claim 24 reciting that “each of the plurality of security devices is configured to communicate with the programmable key.”

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* Pet. 17–19; Pet. Reply 13–17. 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.” Pet. 18. We do not agree because, as we find above, the “configured to communicate” language of the claims finds express written description support in the ’102 Application’s description of communication among components of the system, irrespective of the means by which the communication occurs. Ex. 1007, 4:17–20, 6:17–20.

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.’” Pet. Reply. 13–14. Petitioner’s characterization does not tell the whole story. Although the Federal Circuit 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." [U.S. 5,111,310] col.3 ll.50–54 (emphases added). 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." *Id.* col.10 l.23–col.12 l.13; [U.S. 5,341,228] col.17 l.56–col.20 l.15. Accordingly, the 1990 and 1991 Applications disclose only a blue noise mask.

Research Corp., 627 F.3d at 872. 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 among components of the system, irrespective of the means by which the communication occurs.[12] Ex. 1007, 4:13–20, 6:17–20.

The pertinent inquiry is whether or not the '102 Application provides written description support for a programmable key that is configured to communicate with a programming station and with a security device, as recited in claims 1, 24, and 25 of the '762 patent. For the reasons discussed above, we find that it does. That the '968 CIP application to which the '762

[12] 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, 25:5–6, 12–13.

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.

G. Unpatentability Challenge – Anticipation by Belden

For the reasons discussed above, we find that the ’102 Application provides written description support for the claimed subject matter of arming upon a matching and communicating. Petitioner contends Belden anticipated claims 1, 2, 5–9, and 11–27. Pet. 20–31. As such, Petitioner does not contend Belden fails to provide disclosure for the subject matter of these claims other than with respect to arming upon a matching and communicating. Therefore, based on the record developed during trial, we determine that claims 1, 2, 5–9, and 11–27 of the ’762 patent are entitled to the benefit of the filing date of the ’102 Application and, therefore, that Belden is not prior art to these claims.

Petitioner has not shown, by a preponderance of the evidence, that claims 1, 2, 5–9, and 11–27 are unpatentable as anticipated by Belden under 35 U.S.C. § 102(b).

H. Unpatentability Challenges – Obviousness Based on Belden, Sedon, and Rothbaum (Claims 3, 4, and 10)

Petitioner additionally asserts that the subject matter of dependent claims 3 and 4 would have been obvious based on the combination of Belden and Sedon and that the subject matter of claim 10 would have been obvious based on the combination of Belden and Rothbaum. Pet. 4, 31–34. Therefore, Petitioner asserts that Belden is prior art to these claims.

Because we conclude that claims 3 and 4 are unpatentable over the combined teachings of Rothbaum, Denison, and Ott and that claim 10 is unpatentable over the combined teachings of Rothbaum and Denison, we need not separately assess the patentability of these claims based on Belden in combination with Sedon or Rothbaum. Therefore, we need not determine whether or not Belden is prior art to claims 3, 4, and 10.

III. MOTION TO EXCLUDE

Patent Owner filed a Motion to Exclude (Paper 26) Exhibits 1018, 1019, and 1020, which are dictionary definitions Petitioner cites in support of its construction of the phrase "upon a matching." Patent Owner argues that these exhibits are "irrelevant and prejudicial under [Federal Rules of Evidence] 401 and 403, as well as outside the permissible scope of a reply." Paper 26, 2. Patent Owner argues 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.*

We are not persuaded Exhibits 1018, 1019, and 1020 should be excluded. *See* 37 C.F.R. § 42.20(c) ("The moving party has the burden of proof to establish that it is entitled to the requested relief."); *see also* 37 C.F.R. § 42.64(c) ("Motion to exclude"). 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."

Paper 26, 2. The meaning of this phrase is "of consequence in determining" whether or not the '762 patent 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,[13] 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 cumulative evidence." Patent Owner does not explain in its Motion 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 this evidence should be excluded because it is "outside the permissible scope of a reply" and "should have been presented at the time of filing the petition." Paper 26, 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

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

evidence is not admissible (*e.g.*, relevance or hearsay) . . . ."). Even if Patent Owner's arguments were proper procedurally, however, Petitioner introduced this evidence in response to Patent Owner's arguments in its Response as to the meaning of "upon a matching." *See* Paper 29, 3–4. 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 the matching of the security codes and the arming or disarming of the security device" (i.e., "the keys [is] configured to arm or disarm the security device *as a result of* the matching of the codes").[14] *See* PO Resp. 4–11; Pet. Reply 6 & n.1 (citing Exhibits 1018, 1019, and 1020); Paper 29, 2–4. Pursuant to 37 C.F.R. § 42.23(b), "[a] reply may only respond to arguments raised in the corresponding . . . patent owner response." We determine 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 Motion 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)." Paper 26, 3. Patent Owner identifies various citations in Petitioner's Reply to which Patent Owner objects as misquotations of testimony or citations in incomplete testimony. Paper 26, 3–5. Patent Owner argues that, under Federal Rule of Evidence 106, "statements in the transcript cannot be read out of context of

[14] 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.3; Tr. 43:13–45:5, 50:18–21.

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 [Patent Owner]'s positions." Paper 26, 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 this matter 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 Motion to Exclude is denied as to Exhibits 1018, 1019, and 1020 and dismissed as moot as to Exhibits 1016 and 1017.

IV. CONCLUSION

Based on the information presented and the record developed during trial, we conclude that Petitioner has shown by a preponderance of evidence that (1) claims 1, 5–20, 22–25, and 27 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum and Denison; and (2) claims 2–4, 21, and 26 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum, Denison, and Ott. Petitioner, however, has not shown by a preponderance of evidence that claims 1, 2, 5–9, and 11–27 are unpatentable as anticipated by Belden.

V. ORDER

Accordingly, it is:

ORDERED that claims 1–27 of the ’762 patent have been shown to be unpatentable;

FURTHER ORDERED that Patent Owner’s Motion to Exclude (Paper 26) is *denied-in-part* and *dismissed-in-part*; and

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

PETITIONER:

Alan Norman
Anthony Blum
David Jinkins
Matthew Braunel
THOMPSON COBURN LLP
tc-ipr-mti@thompsoncoburn.com
ablum@thompsoncoburn.com
djinkins@thompsoncoburn.com
mbraunel@thompsobcoburn.com

PATENT OWNER:

Gregory Carlin
Warren Thomas
MEUNIER CARLIN & CURFMAN LLC
mti.invue.iprs@mcciplaw.com
wthomas@mcciplaw.com

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