

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

iAPARTMENTS, INC.,
Petitioner,

v.

EDST, LLC,
Patent Owner.

IPR2022-01468
Patent 10,825,273 B2

Before ST. JOHN COURTENAY, III, KEVIN W. CHERRY, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

iApartments, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33 of U.S. Patent No. 10,825,273 B2 (Ex. 1001, “the ’273 patent”). EDST, LLC (“Patent Owner”) filed a Preliminary Response (Paper 8, “Prelim. Resp.”). We have authority under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we institute an *inter partes* review as to all the challenged claims of the ’273 patent based on all the grounds presented.

II. BACKGROUND

A. *Related Proceedings*

The parties identify two related federal district court cases. Pet. 13; Paper 4, 2 (Patent Owner’s Mandatory Notices). The parties also identify two related *inter partes* review proceedings and one related post-grant review proceeding. *Id.* In addition, Patent Owner identifies a related International Trade Commission investigation. Paper 4, 3.

B. *The ’273 Patent*

The ’273 patent describes an intelligent thermostat that can serve as a hub in a system for controlling and securing offline door locks and other smart devices within a multi-family property. Ex. 1001, 1:6–11. To illustrate, Figure 5 of the ’273 patent is reproduced below.

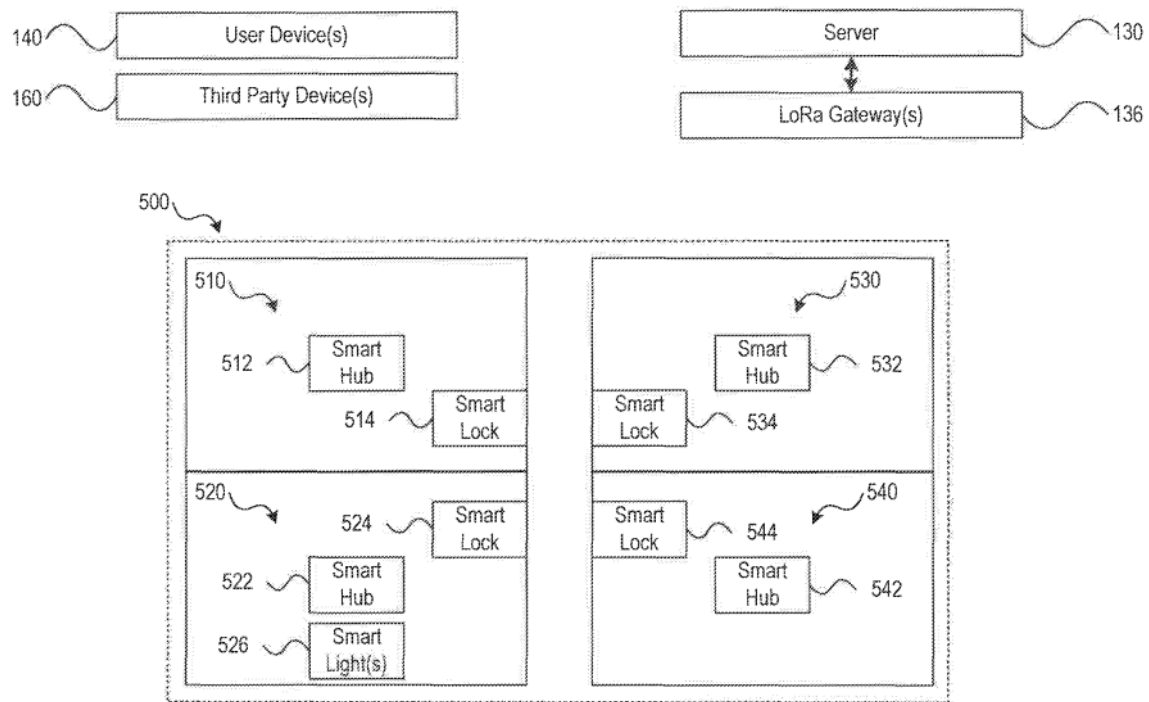


FIG. 5

Figure 5 shows an intelligent property management system. *Id.* at 18:33–36. Building 500 of a multi-family residential property includes apartments 510, 520, 530, 540. *Id.* at 18:26–38. Apartments 510, 520, 530, 540 include smart hubs 512, 522, 532, 542, as well as offline door locks 514, 524, 534, 544. *Id.* at 18:38–44. The '273 patent states in its background section that “offline door locks can only be controlled (e.g., locked and unlocked) by a device (e.g., a fob, smartphone, smartcard, etc.) that is placed in proximity to a sensor of the offline door lock.” *Id.* at 1:36–44.

Smart hubs 512, 522, 532, 542 provide gateways or bridges between server 130 and one or more smart devices in apartments 510, 520, 530, 540. *See* Ex. 1001, 2:26–31. A smart device may include a thermostat, a light fixture, or one of offline door locks 514, 524, 534, 544. *Id.* at 9:1–2, 18:44–50. Specifically, smart hubs 512, 522, 532, 542 communicate with

server 130 via Long Range (LoRa) gateway 136 and a first communication link, such as a LoRa wide area network (LoRaWAN) communication link; and they communicate with the smart devices via a second communication link, such as a non-LoRaWAN communication link. Ex. 1001, 5:63–64, 18:44–50; *see id.* at 13:31–35, Fig. 1. Server 130 provides a property management platform that property management personnel may use to send control information to a smart hub, which, in turn, sends a command to a smart device based on the control information. *See id.* at 12:17–24, 14:16–37. Control information includes information that identifies a smart device within an apartment and actions or parameters for configuring the identified smart device. *Id.* at 2:40–43. These actions or parameters may include retrieving the status of an offline door lock (locked or unlocked), disabling an access credential associated with an offline door lock, turning off a smart light, or setting a thermostat to a predetermined temperature. *Id.* at 12:17–30, 14:12–15, 19:29–33.

The '273 patent describes various ways the intelligent property management system of Figure 5 may work. For example, two residents may live in apartment 530, where each resident has an access credential loaded into third party device 160, such as a fob or smartcard. Ex. 1001, 18:65–19:1. If one resident becomes violent toward the other resident, property management personnel may remotely disable the aggressor resident's access credential by using the property management platform of server 130 to send control information to smart hub 532. *Id.* at 19:1–19. In response, smart hub 532 communicates with offline door lock 534 to disable the access credential. *Id.* at 19:13–19.

C. Illustrative Claim

Petitioner challenges claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33 of the '273 patent. Claims 1, 18, and 26 are independent. Claim 1 is illustrative of the claims under challenge:

1. A system for securing smart devices within an apartment of a multi-family residential property, the system comprising:

an offline door lock comprising:

a first memory storing access credential validation information; and

a lock processor configured to:

determine validity of received access credential information from a credential device based on the stored access credential validation information; and

a smart device hub comprising:

one or more processors;

a second memory communicatively coupled to the one or more processors;

a first interface configured to communicatively couple the one or more processors to a property management platform via a wide area network (WAN) communication link; and

a second interface configured to communicatively couple the one or more processors to the offline door lock via a non-WAN communication link;

where the one or more processors are configured to:

receive control information associated with the offline door lock from the property management platform via the WAN communication link where the control information identifies one or more access credentials to be disabled with respect to the offline door lock,

generate a command configured to disable the one or more access credentials identified in the control information; and

transmit the command to the offline door lock via the non-WAN communication link,

where the lock processor is configured to receive the command via the non-WAN communication link and to modify the stored access credential validation information to disable the one or more access credentials based on the command.

D. Asserted Grounds of Unpatentability

Petitioner challenges claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33 of the '273 patent on the following six grounds.
Pet. 15, 36–108.

Claims Challenged	35 U.S.C. § ¹	References/Basis
1, 2, 7, 9, 14, 18, 26	102	Cahill ²
1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, 33	103	Cahill, Deros ³
8	103	Cahill, Deros, Kraus ⁴
1, 2, 5–11, 18, 20, 21, 26, 28, 29	102	Kraus
14, 15, 17, 23, 25, 31, 33	103	Kraus, Ho ⁵
5, 6, 20, 28	103	Kraus, Wired ⁶

In support of its arguments, Petitioner relies on a Declaration of Philip C. Dumas (Ex. 1003).

III. DISCUSSION

A. Claim Construction

In an *inter partes* review proceeding, we construe a claim of a patent “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” *See* 37 C.F.R. § 42.100(b). That standard involves construing claims in accordance with

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. §§ 102 and 103, effective March 16, 2013. Because the application from which the ’273 patent was filed before this date, the pre-AIA version of §§ 102 and 103 apply.

² Cahill, U.S. Publ’n No. 2019/0043289 A1, published Feb. 7, 2019 (Ex. 1005).

³ Deros et al., U.S. Publ’n No. 2018/0110093 A1, published Apr. 19, 2018 (Ex. 1007).

⁴ Kraus et al., U.S. Publ’n No. 2010/0283579 A1, published Nov. 11, 2010 (Ex. 1006).

⁵ Ho et al., U.S. Publ’n No. 2021/0319639 A1, published Oct. 14, 2021 (Ex. 1008).

⁶ Michael McCole, *How to Make Nest’s Thermostat Your Smart-Home Hub*, WIRED (Feb. 10, 2016, 5:42 AM), <https://www.wired.com/2016/02/iotcookbook-nest/> (Ex. 1013).

the ordinary and customary meaning of such claims as would have been understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc).

Petitioner proposes constructions for the claim terms “offline door lock” and “credential device.” Pet. 34–35. Patent Owner does not respond. *See generally* Prelim. Resp. For purposes of this Decision, we conclude that no claim term requires express interpretation at this time to resolve any controversy in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

B. Obviousness over Cahill and Deros

We turn now to Petitioner’s asserted grounds, starting with Petitioner’s assertion that claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33 of the ’273 patent would have been obvious over Cahill and Deros. Pet. 55–78. Patent Owner challenges certain aspects of Petitioner’s analysis. Prelim. Resp. 6–16, 19–27. For the reasons explained below, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing on this ground.

1. Overview of Asserted Prior Art

Before addressing the parties’ arguments, we provide an overview of the asserted prior art, Cahill and Deros.

a. Cahill

Cahill relates to an offline lock system. Ex. 1005 ¶ 2. Figure 1 of Cahill is reproduced below.

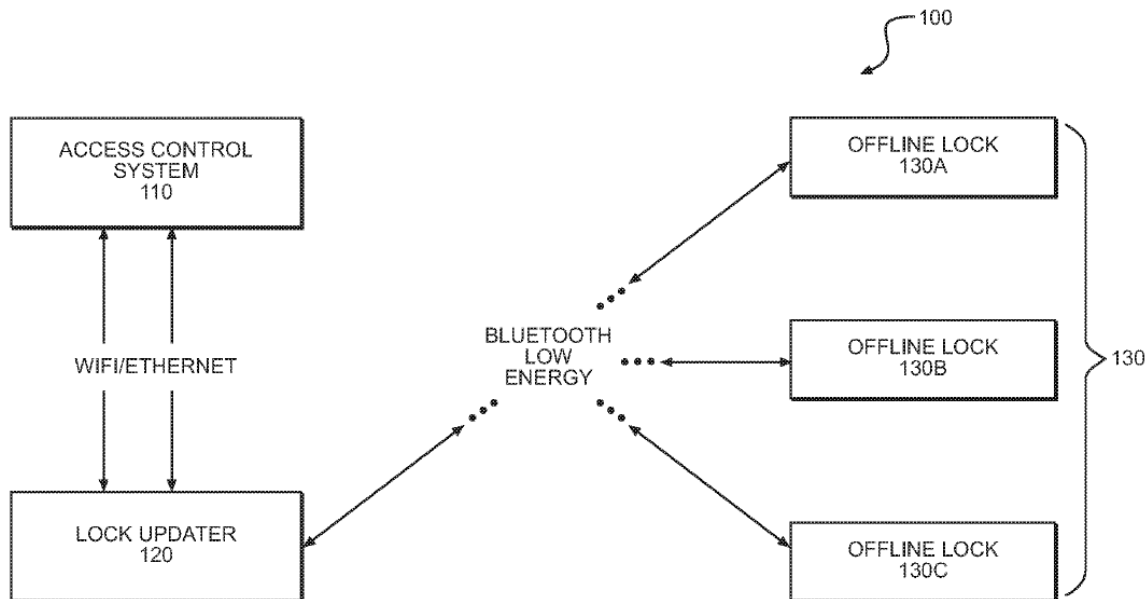


FIG. 1

Figure 1 of Cahill shows offline lock system 100, which includes access control system (ACS) 110, lock updater 120, and offline lock 130 (which may comprise one or more offline locks 130A, 130B, 130C). *Id.* ¶¶ 40–41. ACS 110 receives input from a user, where the input may include commands to access offline lock 130, monitor offline lock 130, or perform any other function regarding offline lock 130. *Id.* ¶ 45. Lock updater 120 receives signals and information from ACS 110 based on the user input and sends signals and information to offline lock 130. *Id.* ¶ 49. Each of ACS 110, lock updater 120, and offline lock 130 includes a device capable of wireless or wired communication with other wireless or wired devices, where the communications may be provided through, for example, wi-fi, satellite, broadcast radio, and ethernet. *Id.* ¶¶ 43, 46, 50.

Cahill explains that a user may enter a door locked by offline lock 130 with an identification object within “reader-range” of offline lock 130, such as a smartcard or fob. Ex. 1005 ¶¶ 86–87. If a user would like to change a setting or update access information for offline lock 130, the user may input a command (information) into ACS 110. Ex. 1005 ¶ 71. ACS 110 then sends the information to lock updater 120, which, in turn, sends the information to offline lock 130. *Id.* Offline lock 130 can thus be updated with the information that the user input into ACS 110. *Id.* Settings input into ACS 110 may include a Blacklist setting and a Credential Revalidation Date setting. *Id.* ¶ 78. The Blacklist setting causes selected offline locks 130 to prevent unauthorized users to access the locks. *Id.* ¶ 79. The Credential Revalidation Date setting sets information in a lock that will invalidate any credential that has not been updated since a predetermined time. *Id.* ¶ 80.

b. Deros

Deros describes a system for interfacing with and controlling internet-of-things (IOT) devices in a hotel room. Ex. 1007 ¶ 2. Figure 1 of Deros is reproduced below.

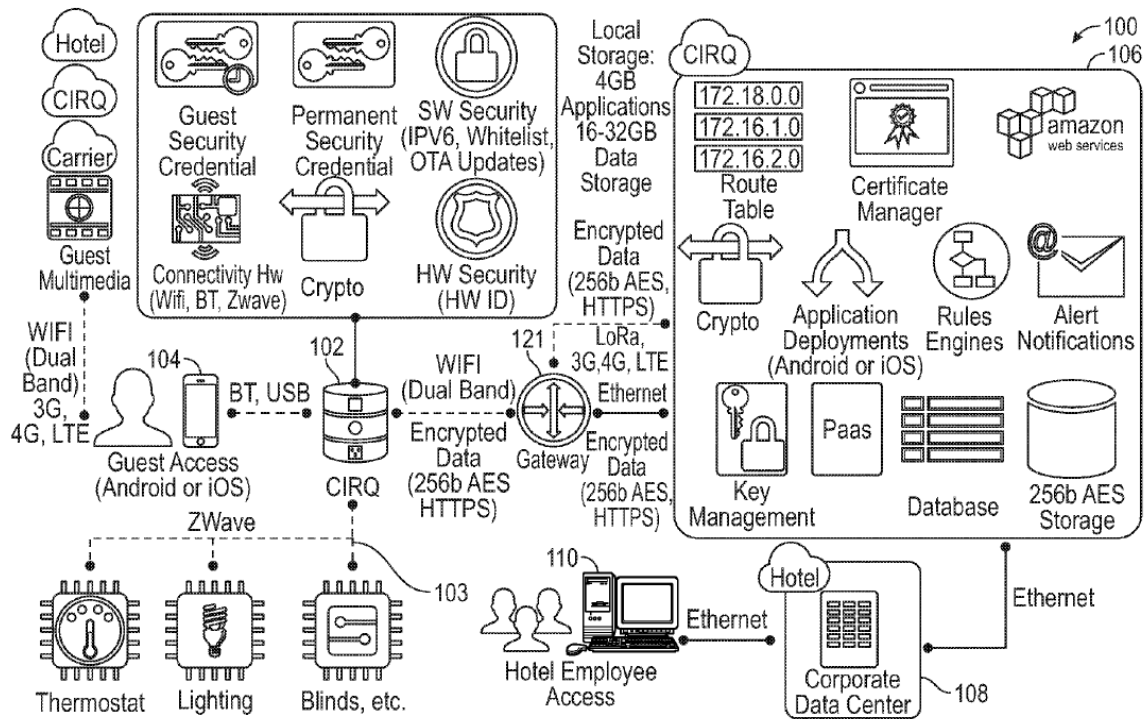


FIG. 1

Figure 1 of Deros shows system 100 for providing enhanced customization of a guest experience. *Id.* ¶ 37. System 100 includes in-room IOT module 102, which controls local IOT network 103, an associated mobile app running on guest mobile device 104, enterprise server 106, and property owner server 108, which communicates with facilities controller 110. *Id.* ¶ 37, Fig. 1. When guest device 104 is inside or near the hotel room, it communicates directly with IOT module 102. *Id.* ¶ 39. When guest device 104 is out of range of IOT module 102, guest device 104 communicates with enterprise server 106. *Id.*

IOT module 102 communicates with guest device 104 using a wired or wireless protocol, such as wi-fi or ethernet. Ex. 1007 ¶ 38. IOT module 102 communicates with devices in IOT network 103 using a wired or wireless protocol, such as ZWave or Bluetooth. *Id.* IOT module 102 communicates with enterprise server 106 using a wired or wireless protocol,

such as wi-fi, LoRa, or ethernet. *Id.* Likewise, server 106 communicates with property owner server 108 using a wired or wireless protocol, such as wi-fi, LoRa, or ethernet. *Id.*

2. Analysis

Turning to the claims, we address independent claims 1, 18, and 28 together. Claim 1 is directed to a “system for securing smart devices within an apartment of a multi-family residential property.” Claim 18 is directed to a “method for securing smart devices within an apartment of a multi-family residential property.” Claim 26 is directed to a “non-transitory computer-readable storage medium storing instructions that, when executed by one or more processors, cause the one or more processors to perform operations for securing smart devices within an apartment of a multi-family residential property.” Claims 18 and 26 recite similar limitations as claim 1. Petitioner relies primarily on its discussion of claim 1 for claims 18 and 26. Pet. 72–73, 75–76. Accordingly, we address claim 1 in detail. Our analysis of claim 1 applies to claims 18 and 26.

a. Independent Claim 1

Claim 1, directed to a system for securing smart devices, recites various limitations designated by Petitioner as limitations 1a through 1h. We address these limitations in turn.

i. Limitation 1a: “offline door lock”

Claim 1 recites “an offline door lock.” For this limitation, which Petitioner designates as limitation 1a, Petitioner cross-references its analysis

for limitation 1a with respect to anticipation by Cahill. Pet. 61. In that analysis, Petitioner identifies Cahill’s offline lock 130 as an “offline door lock.” *Id.* at 37–38. As support, Petitioner directs us to where Cahill teaches that “in order for a user to enter a door 150 locked by the offline lock 130, the user may use an identification object 140, such as a smart card, dongle, key-fob, chip, or access code/information programmed on an application running on a smart phone or other electronic device.” *Id.* at 37 (quoting Ex. 1005 ¶ 86).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited offline door lock of limitation 1a. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

ii. Limitation 1b: “first memory”

Claim 1 recites that the offline door lock comprises “a first memory storing access credential validation information.” For this limitation, which Petitioner designates as 1b, Petitioner cross-references its analysis for limitation 1b with respect to anticipation by Cahill. Pet. 61. In that analysis, Petitioner identifies Cahill’s storage unit 132 as a “first memory.” *Id.* at 38–39. As support, Petitioner directs us to Figure 4 of Cahill, which shows that offline lock 130 includes storage unit 132. *Id.* (citing Ex. 1005, Fig. 4). Petitioner also directs us to where Cahill teaches that “[t]he storage unit 132 may store information regarding the offline lock 130, identification and/or profile data of authorized users, identification and/or profile data of

unauthorized users, status types of the offline lock 130, and modes of the offline lock 130.” *Id.* at 38–39 (emphases omitted) (quoting Ex. 1005 ¶ 69).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited first memory of limitation 1b. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

iii. Limitation 1c: “lock processor”

Claim 1 recites that the offline door lock further comprises “a lock processor configured to: determine validity of received access credential information from a credential device based on the stored access credential validation information.” For this limitation, which Petitioner designates as limitation 1c, Petitioner cross-references its analysis for limitation 1c with respect to anticipation by Cahill. Pet. 61. In that analysis, Petitioner identifies Cahill’s controller 137 as a “lock processor.” *Id.* at 39–40. As support, Petitioner directs us to Figure 4 of Cahill, which shows that offline lock 130 includes controller 137. *Id.* at 40 (citing Ex. 1005, Fig. 4). Petitioner also directs us to where Cahill teaches that “[t]he controller 137 may include a central processing unit (CPU).” *Id.* at 39 (emphasis omitted) (quoting Ex. 1005 ¶ 76). Additionally, Petitioner directs us to where Cahill teaches that “[w]hen the offline lock 130 senses that the identification object 140 is within the reader-range, the controller 137 may decrypt the access privileges from the identification object 140 or access the storage unit 132 to verify whether the user has authorized access to open the offline lock 130.” *Id.* at 40 (emphasis omitted) (quoting Ex. 1005 ¶ 87).

Based on Petitioner's argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited lock processor of limitation 1c. Patent Owner does not challenge Petitioner's analysis for this limitation. *See generally* Prelim. Resp.

iv. Limitation 1d: "smart device hub," "processors," "second memory"

Claim 1 further recites "a smart device hub comprising: one or more processors; a second memory communicatively coupled to the one or more processors." For these limitations, which Petitioner designates collectively as limitation 1d, Petitioner cross-references its analysis for limitation 1d with respect to anticipation by Cahill. Pet. 61. In that analysis, Petitioner identifies Cahill's lock updater 120 as a "smart device hub," Cahill's CPU 122 as "one or more processors," and Cahill's storage unit 121 as a "second memory." *Id.* at 41–42. To support its position, Petitioner directs us to Figure 1 of Cahill, which shows that lock updater 120 connects to offline lock 130 (including offline locks 130A, 130B, 130C). *Id.* at 41 (citing Ex. 1005, Fig. 1). As discussed above, Cahill's offline lock 130 can be a singular offline lock, or it can include one or more of offline locks 130A, 130B, 130C. Ex. 1005 ¶ 41. Petitioner points to Cahill's teaching that "[t]he lock updater 120 may include a device capable of wireless or wired communication between other wireless or wired devices." Pet. 41 (emphasis omitted) (quoting Ex. 1005 ¶ 46).

Petitioner additionally directs us to Figure 3 of Cahill, which shows that lock updater 120 includes storage unit 121 and CPU 122. Pet. 41 (citing Ex. 1005, Fig. 3); *see also* Ex. 1005 ¶ 61 ("The lock updater 120 may

include a storage unit 121, a central processing unit (CPU) 122.”) (quoted by Pet. 41). We note that Figure 3 of Cahill also shows that storage unit 121 and CPU 122 are communicatively coupled to each other. Ex. 1005, Fig. 3 (bidirectional arrow between storage unit 121 and CPU 122).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited smart device hub of limitation 1d. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

v. Limitation 1e: “first interface”

Claim 1 recites that the smart device hub further comprises “a first interface configured to communicatively couple the one or more processors to a property management platform via a wide area network (WAN) communication link.” For this limitation, which Petitioner designates as limitation 1e, Petitioner relies on Cahill and Deros. Pet. 61–62.

To start, Petitioner cross-references its analysis for limitation 1e with respect to anticipation by Cahill. Pet. 61. In that analysis, Petitioner identifies Cahill’s transmitter 115 and receiver 124 together as a “first interface” and Cahill’s ACS 110 as a “property management platform.” *Id.* at 42–43. As support, Petitioner directs us to Figure 1 of Cahill, which, according to Petitioner, shows that “lock updater 120 is communicatively linked with access control system 110,” where lock updater 120 corresponds to the recited smart device hub. *Id.* at 42 (citing Ex. 1005, Fig. 1).

As further support, Petitioner provides an annotated version of Figure 3 of Cahill, reproduced below. Pet. 42 (citing Ex. 1005, Fig. 3).

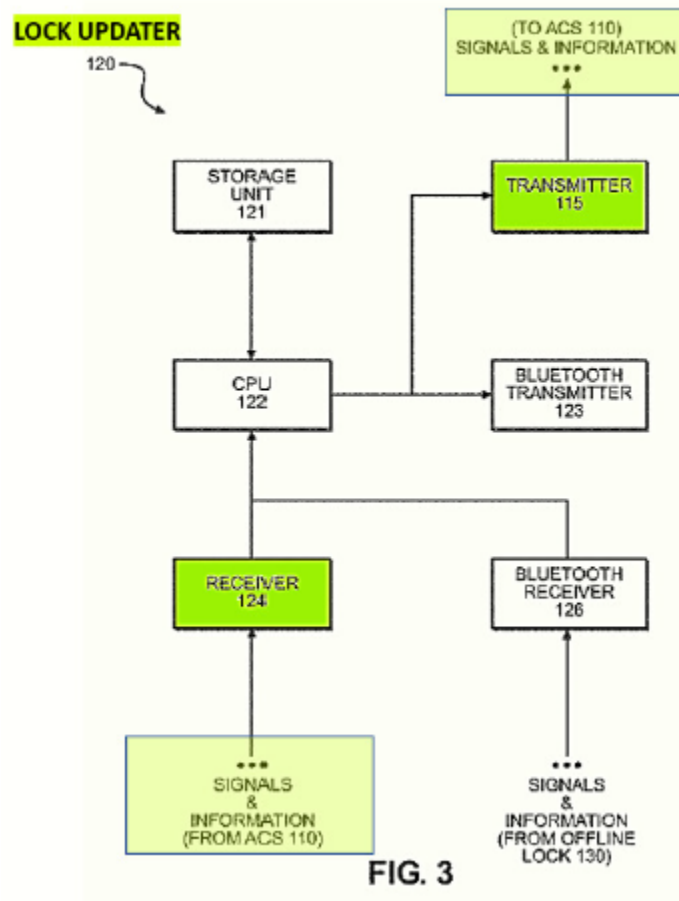


Figure 3 of Cahill, as annotated by Petitioner, is a diagram of lock updater 120. *See* Ex. 1005 ¶ 30. Petitioner asserts that “[l]ock updater 120 includes a receiver 124 and transmitter 115 to communicate with access control system [ACS] 110.” Pet. 42. Petitioner points to Cahill’s teaching that the “[w]ireless and wired communications of the ACS 110 may include wi-fi, . . . satellite communication, broadcast radio communication, Microwave radio communication, . . . Ethernet, etc., but are not limited thereto.” *Id.* at 43 (emphasis omitted) (quoting Ex. 1005 ¶ 43). According to Petitioner, Cahill’s “satellite, broadcast radio, [or] microwave communication link” provides a WAN communication link, as recited in

limitation 1e. *Id.* Petitioner relies on the declaration testimony of Mr. Dumas. *Id.* (citing Ex. 1002 ¶ 133).

To the extent that Cahill does not teach the recited WAN communication link, Petitioner relies on Deros. Pet. 61. In particular, Petitioner directs us to where Deros teaches that its IOT module 102 is “configured to communicate with the enterprise server 106 through a gateway 121 (such as the internet) using Wi-Fi, LoRa, 3G, 4G, LTE, Ethernet, or any suitable wired or wireless protocol.” Pet. 62 (emphasis omitted) (quoting Ex 1007 ¶ 38). Petitioner contends that “[i]t would have been obvious to a [person of ordinary skill in the art] to provide Cahill’s smart hub with a LoRa (long range) WAN communications gateway as expressly taught by Deros to be one of many suitable communications protocols.” *Id.* at 56; *see also id.* at 55 (“A [person of ordinary skill in the art] would have been motivated to modify Cahill’s smart hub (lock updater 120) to incorporate a LoRa communication link by the teaching Deros.”). As support, Petitioner asserts that “[u]sing a known LoRaWAN protocol, as disclosed in Deros, would be a simple substitution of one long range communication protocol (e.g., satellite, broadcast radio, and/or microwave) for another and would obtain predictable results of wide area long range communications, just like with satellite, broadcast radio, and/or microwave communication protocols.” *Id.* at 56. Petitioner further asserts that “[i]t would involve applying a known technique (use of LoRa) to a known device (a smart hub with long range communication abilities) ready for improvement to yield predictable results of low power, long range communication abilities under a known standard of LoRa.” *Id.* at 56–57. Petitioner adds that “LoRa networks use frequency ranges within the range

expressly disclosed in Cahill.” *Id.* at 56 (citing Ex. 1005 ¶ 46). Petitioner relies on the declaration testimony of Mr. Dumas. *Id.* at 56–57 (citing Ex. 1002 ¶¶ 164–170).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that its proposed combination of Cahill and Deros teaches the recited first interface of limitation 1e. We also are persuaded that Petitioner’s proffered reasoning for modifying Cahill’s system to use LoRa for communications as taught by Deros is sufficient for institution. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (“[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”); *see also KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007) (“[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result.”).

Patent Owner, however, challenges Petitioner’s analysis for this limitation. Prelim. Resp. 6–12, 19–27. We address Patent Owner’s challenge below. *See infra* Part III.B.2.b.

vi. Limitation 1f: “second interface”

Claim 1 recites that the smart device hub further comprises “a second interface configured to communicatively couple the one or more processors to the offline door lock via a non-WAN communication link.” For this limitation, which Petitioner designates as limitation 1f, Petitioner cross-references its analysis for limitation 1f with respect to anticipation by Cahill. Pet. 62. In that analysis, Petitioner identifies Cahill’s Bluetooth

transmitter 123 and Bluetooth receiver 126 together as a “second interface.” *Id.* at 43–44. As support, Petitioner directs us to Figure 1 of Cahill, which, according to Petitioner, shows that “Cahill’s lock updater 120 is communicatively linked to offline locks 130A-C,” where offline locks 130A–C comprise offline lock 130. Pet. 43 (citing Ex. 1005, Fig. 1).

Petitioner also provides an annotated version of Figure 3 of Cahill, which is reproduced below. Pet. 44.

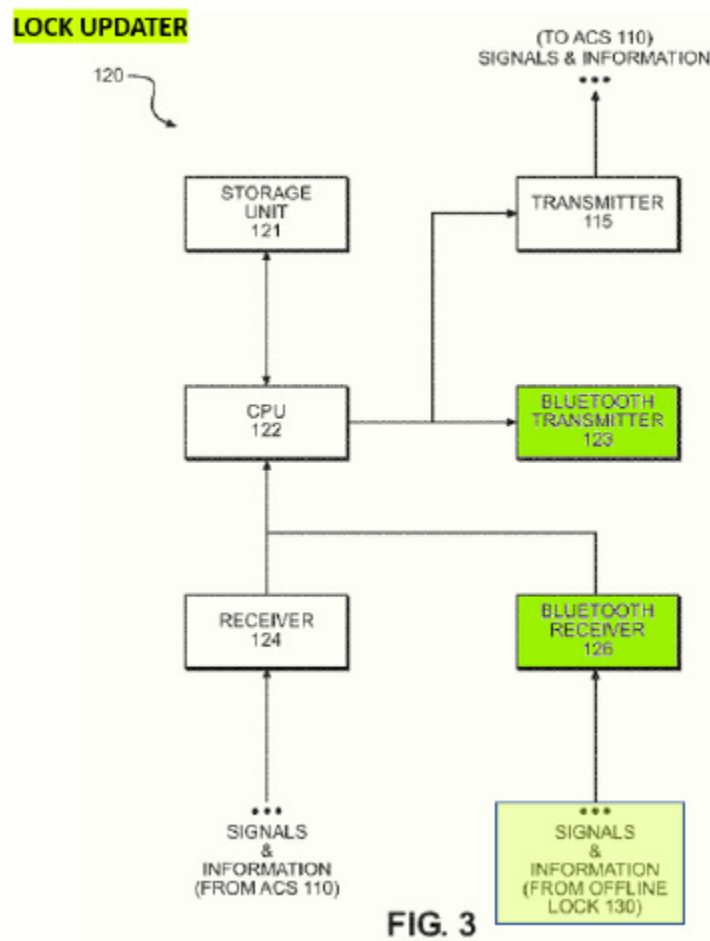


Figure 3 of Cahill, as annotated by Petitioner, is a diagram of lock updater 120. *See* Ex. 1005 ¶ 30. Petitioner points to Cahill’s teaching that “Bluetooth transmitter 125 may send signals and information to the offline lock 130, and the Bluetooth receiver 126 may receive signals and

information from the offline lock 130.” Pet. 44 (emphasis omitted) (quoting Ex. 1005 ¶ 65). Petitioner asserts that Cahill’s Bluetooth communication link provides a non-WAN communication link, as recited in limitation 1f. As support, Petitioner directs us to claim 14 of the ’273 patent, which recites that a “non-WAN communication link comprises . . . a Bluetooth communication link.” Pet. 44–45 (quoting Ex. 1001, claim 14).

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited second interface of limitation 1f. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

vii. Limitation 1g: “receive control information,” “generate a command”

Claim 1 recites that the one or more processors of the smart device hub “are configured to: receive control information associated with the offline door lock from the property management platform via the WAN communication link where the control information identifies one or more access credentials to be disabled with respect to the offline door lock.” Claim 1 also recites that the one or more processors are configured to “generate a command configured to disable the one or more access credentials identified in the control information.” Petitioner designates these limitations collectively as limitation 1g.

For these limitations, Petitioner cross-references its analysis for limitation 1g with respect to anticipation by Cahill. Pet. 63. In that analysis, Petitioner identifies Cahill’s control settings for offline lock 130 as “control information.” Pet. 45–46. As support, Petitioner directs us to where Cahill

teaches that its ACS 110 includes “an input unit to allow a user to input information to change a setting of the at least one offline lock, update the at least one offline lock, and change access information of the at least one offline lock.” Ex. 1005 ¶ 24 (quoted by Pet. 45). Petitioner also directs us to where Cahill teaches that “[a] plurality of different type[s] of settings may be input into the ACS 110 to control the plurality of offline locks 130, such as a Lockdown setting, a Blacklist setting, a Credential Revalidation Date setting, a Lock Calendars setting, a Time Intervals setting, a Lock Groups setting.” *Id.* ¶ 77 (quoted by Pet. 46). We note that the Blacklist setting “is a setting that may be applied to the plurality of offline locks 130 that causes all or selected offline locks 130 within the [Bluetooth Low Energy] range of corresponding lock updaters 120 to prevent unauthorized users to access the offline locks 130.” *Id.* ¶ 79. We also note that the Credential Revalidation Date setting “is a setting that uses a parameter such as a ‘Minimum Validation Date,’ in order to set information in a lock that will essentially invalidate any credential that has not been updated since a predetermined time.” *Id.* ¶ 80 (cited by Pet. 46). According to Cahill, “[t]his is like a soft blacklist in that a user can force people to revalidate/update access privileges saved on their personal credentials.” *Id.* To illustrate, Cahill explains,

An example might be that all users receive access to the server room for a year, then later, an administrator desires to put a safe in that room and restrict access. The administrator can change users’ access privileges to the lock on the door and set the Minimum Validation Date for that lock to a particular day

Id. Petitioner asserts that Cahill’s “ACS would thus transmit this information to the lock updater to invalidate or disable offline lock 130 access.” Pet. 46 (citing Ex. 1005 ¶ 80).

As further support, Petitioner provides an annotated version of Figure 6 of Cahill, which is reproduced below. Pet. 46.

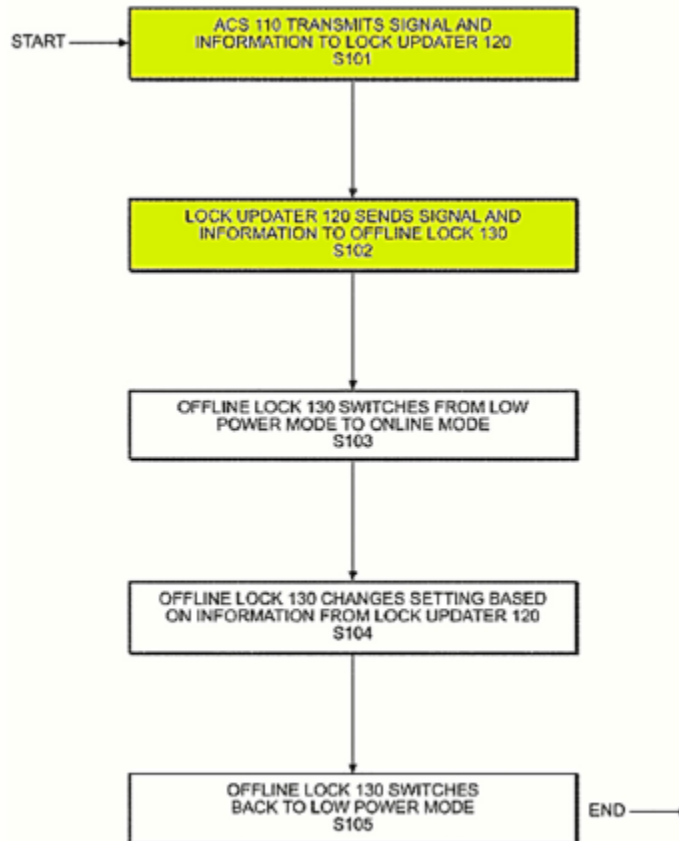


FIG. 6

Figure 6 of Cahill, as annotated by Petitioner, shows a method for changing a setting of offline lock 130. *See* Ex. 1005 ¶ 90. Petitioner's annotated figure highlights the first two steps. In step S101, ACS 110 (which corresponds to the recited property management platform) transmits a signal and information to lock updater 120 (which corresponds to the recited smart device hub). *Id.* ¶ 91, Fig. 6. In step S102, lock updater 120 sends a signal and information via Bluetooth communication to offline lock 130. *Id.* We note that in subsequent step S104, offline lock 130 changes its setting based on the information received from lock updater 120. Ex. 1005 ¶ 91, Fig. 6;

see also Pet. 47–48 (discussing Cahill’s step S104). Cahill explains that the method shown in Figure 6 pertains not only to changing a setting of offline lock 130 but also to other types of control and information distribution to offline lock 130. Ex. 1005 ¶ 91.

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited one or more processors of the smart device hub of limitation 1g. Patent Owner, however, challenges Petitioner’s analysis for this limitation. Prelim. Resp. 13–16. We address Patent Owner’s challenge below. *See infra* Part III.B.2.b.

viii. Limitation 1h: “transmit the command”

Lastly, claim 1 recites that the one or more processors of the smart device hub are further configured to “transmit the command to the offline door lock via the non-WAN communication link, where the lock processor is configured to receive the command via the non-WAN communication link and to modify the stored access credential validation information to disable the one or more access credentials based on the command.” For this limitation, which Petitioner designates as limitation 1h, Petitioner cross-references its analysis for limitation 1g⁷ with respect to anticipation by Cahill. Pet. 63. In that analysis, Petitioner directs us to where Cahill teaches that “[w]hen the user desires to change a setting, update and/or change

⁷ We believe Petitioner intended to cross-reference its analysis for limitation 1h with respect to anticipation by Cahill. Accordingly, we consider that analysis in our discussion of limitation 1h with respect to obviousness over Cahill and Deros.

access information, etc., of a particular offline lock 130, the user may input a command (e.g., information) into the ACS 110,” which, in turn, “access[es] a particular lock updater 120 that is within a [Bluetooth Low Energy] range of the particular offline lock 130.” Ex. 1005 ¶ 71 (cited by Pet. 47). Cahill teaches that “[t]he offline lock 130 may then receive the information from the lock updater 120, thereby allowing the offline lock 130 to be updated with the information the user input into the ACS 110.” *Id.* (quoted by Pet. 47).

Petitioner further provides an annotated version of Figure 6 of Cahill, which is reproduced below. Pet. 48.

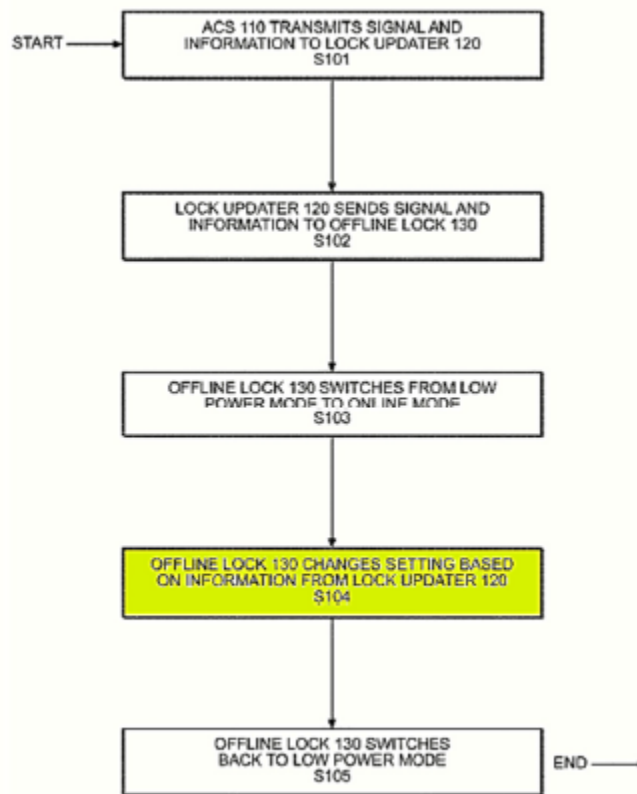


FIG. 6

Figure 6 of Cahill, as annotated by Petitioner, shows a method for changing a setting of offline lock 130. See Ex. 1005 ¶ 90. Petitioner’s

annotated figure highlights the fourth step. As discussed above with respect to limitation 1g, in step S101, ACS 110 (which corresponds to the recited property management platform) transmits a signal and information to lock updater 120 (which corresponds to the recited smart device hub). *Id.* ¶ 91. In step S102, lock updater 120 sends a signal and information via Bluetooth communication to offline lock 130. *Id.* In step S104, offline lock 130 changes its setting based on the information received from lock updater 120. *Id.*

Based on Petitioner’s argument and evidence, we are persuaded that Petitioner has shown sufficiently for purposes of this Decision that Cahill teaches the recited one or more processors of the smart device hub of limitation 1h. Patent Owner does not challenge Petitioner’s analysis for this limitation. *See generally* Prelim. Resp.

b. Patent Owner’s Arguments

As mentioned above, Patent Owner challenges Petitioner’s analysis for limitations 1e and 1g. With respect to limitation 1e, Patent Owner challenges Petitioner’s showing for the recited property management platform as well as Petitioner’s showing for the recited WAN communication link. With respect to limitation 1g, Patent Owner challenges Petitioner’s showing for the recited one or more processors of the smart device hub. We address these challenges in turn.

i. “property management platform”

Starting with the property management platform recited in limitation 1e, Patent Owner argues that “there must be a ***platform*** that

facilitates **property management** tasks or functions.” Prelim. Resp. 8. Patent Owner contends that “Petitioner has not met its burden to show that Cahill discloses the claimed ‘property management platform’” because “Petitioner does not explain why or how Cahill’s ACS 110 performs any property management functions.” *Id.* at 9–10; *see also id.* at 11–12 (“Petitioner here fails to explain the significance of the evidence (i.e., Cahill’s ACS 110) with respect to the claimed limitation (i.e., the ’273 Patent’s ‘property management platform’).”). According to Patent Owner, “Cahill’s ACS 110 performs purely security functions,” whereas “[t]he ’273 Patent is clear that ‘property management’ functions are **additional** functionality above and beyond ‘security’ functions.” *Id.* at 8–9 (citing Ex. 1001, 2:32–51, 8:15–22, 8:34–41, 8:63–9:2, 9:28–34). Patent Owner adds that “Petitioner’s mapping implies an interpretation [of “property management platform”] that is **broader** than the plain meaning.” *Id.* at 10.

We disagree with Patent Owner. As discussed above, Petitioner identifies Cahill’s ACS 110 as corresponding to the recited property management platform, and we are persuaded by Petitioner’s argument and evidence in this regard. *See* Pet. 42–43, 61–62. That Petitioner does not explain why or how Cahill’s ACS 110 performs any property management functions does not change our analysis. Claim 1 recites nothing about facilitating or performing management functions. We note that claim 5, which depends from claim 1, relates to operating a thermostat; but that does not translate to claim 1, which is broader than claim 5, requiring performance of management functions. *See RF Del., Inc. v. Pac. Keystone Techs., Inc.*, 326 F.3d 1255, 1264 (Fed. Cir. 2003) (“An independent claim usually covers a scope broader than the preferred embodiment, especially if

the dependent claims recite the precise scope of the preferred embodiment.”); *Phillips*, 415 F.3d at 1324 (“[A]n independent claim should be given broader scope than a dependent claim.”).

Additionally, none of the cited portions of the ’273 patent specification requires additional functionality beyond security functions, as Patent Owner contends. *See* Prelim. Resp. 8; Ex. 1001, 2:32–51 (stating that “smart thermostat hub may also provide functionality for automating and improving various property management tasks” (emphasis added)); *id.* at 8:15–22 (describing smart hub 300 specifically); *id.* at 8:34–41 (describing smart hub 200 specifically); *id.* at 8:63–9:1 (describing modular smart thermostat hub 400 specifically); *id.* at 9:28–9:34 (describing modular smart thermostat hub 400 specifically). Indeed, the ’273 patent describes a system with just one smart device, which may be an offline door lock. Ex. 1001, 4:12–13, 9:1. The ’273 patent teaches that “[i]n FIG. 1, system 100 is illustrated as comprising smart hub 110, one or more smart devices 120, and server 130.” *Id.* at 4:12–13 (emphasis added). The ’273 patent further teaches that server 130 provides a property management platform, which can be used to improve security. *Id.* at 12:14–24. As an example, the ’273 patent teaches,

[I]f a resident is unsure of whether his/her apartment was locked when they left, the resident may contact property management personnel to inquire about the status of the offline door lock, and the property management personnel may utilize a property management platform provided by server 130 to transmit control information to smart hub 110 associated with the resident’s apartment.

Id. at 12:17–24. In light of these teachings, we find that the ’273 patent contemplates a property management platform that provides just security functions, contrary to Patent Owner’s position.

Considering the language of the claims and the teachings in the specification of the ’273 patent, we find that Patent Owner does not adequately rebut Petitioner’s showing for the recited property management platform.

ii. “wide area network (WAN) communication link”

Turning to the WAN communication link recited in limitation 1e, Patent Owner argues that Petitioner “fails to explain why a [person of ordinary skill in the art] would have been motivated to combine Cahill and Deros.” Prelim. Resp. 20. According to Patent Owner, “Cahill’s listing of satellite, broadcast radio, and microwave is nothing more than a disclosure of different frequency bands,” which “are not types of ‘protocols,’ as Petitioner’s ‘simple substitution’ theory assumes.” *Id.* at 21. Patent Owner adds that “Petitioner’s ‘simple substitution’ theory also fails because it is not substantiated with evidence and reasoning,” as “Petitioner does not demonstrate or explain *why* it would have been a ‘simple’ substitution to modify Cahill’s system by employing a LoRaWAN in place of satellite, broadcast radio, and/or microwave transmissions.” *Id.*

We disagree with Patent Owner. As discussed above, Petitioner argues that modifying Cahill’s system to use a LoRaWAN protocol as taught by Deros would have been a simple substitution of one communication protocol for another. Pet. 56. Petitioner points to where Cahill teaches considering not only satellite, broadcast radio, and microwave, but also

various other communication methods including the well-known protocols Wi-Fi and Ethernet, as options for wired or wireless communications. Ex. 1005 ¶ 43 (cited by Pet. 43). Petitioner also points to where Deros teaches considering Wi-Fi, Ethernet, and LoRa, among various other communication methods, as options for wired or wireless communications. Ex. 1007 ¶ 38 (cited by Pet. 62). This teaching in Deros suggests using various communication methods including Wi-Fi, Ethernet, or LoRa interchangeably, thus supporting Petitioner’s simple substitution argument. A claimed invention that involves “the simple substitution of one known element for another” to “yield a predictable result” is obvious. *KSR*, 550 U.S. at 416–17. Here, the claimed invention may be obtained by modifying Cahill’s system to use LoRa for communications as taught by Deros. This is the substitution of one known communication protocol for another known communication protocol to obtain a predictable result. That satellite, broadcast radio, and microwave may not be types of protocols, as Patent Owner contends, does not adequately rebut Petitioner’s showing for obviousness.

We note Patent Owner’s contention that “Petitioner’s further allegation that a [person of ordinary skill in the art] would have been motivated to use a LoRaWAN in Cahill ‘*to improve battery life*’ of the connected smart devices such as *smart locks*’ is wrong and misguided.” Prelim. Resp. 22–24. Even if this were true, we still find Petitioner’s simple substitution argument sufficient for institution for the reasons given above.

We further note Patent Owner’s contention that “Deros does not teach a smart hub with LoRa.” Prelim. Resp. 24–27 (emphasis omitted). Patent Owner criticizes Petitioner’s obviousness argument because it “is based on

Petitioner’s characterization that ‘Deros discloses a smart hub (IOT module 102) with a first interface (LoRa gateway 121) to communicatively couple the smart hub to a property management platform via a WAN (LoRaWAN) link.’” *Id.* at 24–25 (quoting Pet. 62). According to Patent Owner, “the alleged ‘first interface’ with a LoRa communication link relied on by Petitioner is **not** part of the IOT module 102 that Petitioner equates to the claimed ‘smart device hub.’” *Id.* at 25.

Patent Owner’s focus on whether Deros teaches a smart hub with LoRa, however, disregards Deros’s broader teaching that Wi-Fi, Ethernet, or LoRa may be used interchangeably for communications. Ultimately, “[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.” *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). “Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.” *Id.* As Petitioner points out, Deros teaches that LoRa is “one of many suitable communications protocols,” including Wi-Fi and Ethernet. Pet. 56 (citing Ex. 1007 ¶ 38). Petitioner explains that it is for this reason, namely, a simple substitution, an ordinarily skilled artisan would have modified Cahill’s system to use LoRa for communications as taught by Deros. Pet. 55–57. As discussed above, we find this explanation provides sufficient rationale for why an ordinarily skilled artisan would have combined the teachings of Cahill and Deros. As such, Patent Owner does not adequately rebut Petitioner’s argument and evidence.

iii. “smart device hub” limitations

Regarding the one or more processors of the smart device hub recited in limitation 1g, Patent Owner argues that “Petitioner has not addressed the full extent of the[] detailed ‘smart device hub’ limitations,” which, according to Patent Owner, “require a ‘smart device hub’ with ‘one or more processors’ that [i] ‘receive control information . . . [that] identifies one or more access credentials to be disabled with respect to the offline door lock’ and [ii] ‘generate a command configured to disable the one or more access credentials identified in the control information.’” Prelim. Resp. 13.

Specifically, Patent Owner contends that “Petitioner analogizes Cahill’s ‘Blacklist’ setting to the claimed ‘control information . . . [that] identifies one or more access credentials to be disabled’ without any explanation of *what* Cahill’s ‘Blacklisting’ is, *how* it works, and *why* it identifies to-be-disabled access credentials.” *Id.* at 14. Patent Owner also contends that “Petitioner does not explain how the ‘signal and information’ sent by the ACS 110 and the seemingly *identical* ‘signal and information’ sent by the lock updater 120 represent two *different* aspects of the Challenged Claims—i.e., the claimed ‘control information’ and the separately claimed ‘command.’” *Id.* at 15–16. Patent Owner adds that “Petitioner is equally silent on what operation of Cahill’s lock updater allegedly constitutes ‘generat[ing]’ a command.” *Id.* at 16.

We disagree with Patent Owner. Petitioner’s showing for the claim requirement that the smart device hub receive control information is sufficient. As discussed above, Petitioner identifies Cahill’s control settings for offline lock 130 as the recited control information. Pet. 45–46 (asserting that “Cahill discloses a smart hub (lock updater 120) that receives control

information (settings)"). To support its position, Petitioner directs us to where Cahill teaches that "[a] plurality of different type[s] of settings may be input into the ACS 110 to control the plurality of offline locks 130, such as a Lockdown setting, a Blacklist setting, a Credential Revalidation Date setting, a Lock Calendars setting, a Time Intervals setting, a Lock Groups setting." Ex. 1005 ¶ 77 (quoted by Pet. 46). Petitioner also directs us to where Cahill describes the Credential Revalidation Date setting, which "uses a parameter such as a 'Minimum Validation Date,' in order to set information in a lock that will essentially invalidate any credential that has not been updated since a predetermined time." *Id.* ¶ 80 (cited by Pet. 46). According to Cahill, "[t]his is like a soft blacklist in that a user can force people to revalidate/update access privileges saved on their personal credentials." *Id.* To illustrate, Cahill explains,

An example might be that all users receive access to the server room for a year, then later, an administrator desires to put a safe in that room and restrict access. The administrator can change users' access privileges to the lock on the door and set the Minimum Validation Date for that lock to a particular day

Id. Thus, Cahill teaches control information (Credential Revalidation Date setting) that identifies one or more access credentials (access privileges to offline door lock 130 on the door of the server room) to be disabled (invalidated) with respect to the offline door lock (offline door lock 130), contrary to Patent Owner's position. *See* Prelim. Resp. 13; Ex. 1007 ¶ 80. That Petitioner characterizes the Credential Revalidation Date setting as "Blacklisting" is of no moment. Petitioner identifies Cahill's control settings generally as the recited control information. Pet. 46. These settings may include a Blacklist setting or a Credential Revalidation Date setting,

which Cahill describes as a “soft blacklist.” Ex. 1007 ¶ 80. For these reasons, Patent Owner does not adequately rebut Petitioner’s showing in this regard.

Patent Owner also does not adequately rebut Petitioner’s showing for the claim requirement that the smart device hub generate a command. We disagree with Patent Owner that the signal and information sent by Cahill’s ACS 110 and the signal and information sent by Cahill’s lock updater 120 are identical. *See* Prelim. Resp. 15–16. As discussed above, Figure 6 of Cahill (cited by Pet. 45–46) shows a method for changing a setting of offline door lock 130, where the setting may be input into ACS 110 to control offline door lock 130. Ex. 1005 ¶¶ 77, 90, Fig. 6. Referring to its Figure 6, Cahill teaches that ACS 110 (which corresponds to the recited property management platform) sends “a signal and information” to lock updater 120 (which corresponds to the recited smart device hub) in step S101, and that lock updater 120 then sends “a signal and information” to offline lock 130 in step S102. *Id.* ¶ 91 (emphases added). Although the signal and information sent by ACS 110 and the signal and information sent by lock updater 120 are related to the setting input into ACS 110, Cahill’s use of the term “a signal and information” for each of steps S101 and S102 (rather than the term “a signal and information” for step S101 and the term “the signal and information” for step S102) implies that the signal and information sent by ACS 110 is different than the signal and information sent by lock updater 120.

We note Patent Owner’s contention that Petitioner is silent on which of Cahill’s operations in Figure 6 satisfies the claim requirement of generating a command. *See* Prelim. Resp. 16. Again, we disagree with

Patent Owner. Figure 6 shows step S104 in which offline lock 130 changes its setting based on the information received from lock updater 120.

Ex. 1005, Fig. 6; *see also id.* ¶ 91. This implies that the signal and information sent by lock updater 120 includes a command to change a setting of offline lock 130. That Figure 6 of Cahill does not show a specific operation for generating a command, as Patent Owner seems to contend, does not take away from Cahill’s teaching that lock updater 120 sends a signal and information to offline lock 130, which, in turn, changes its setting based on the information received.

We further note Patent Owner’s contention that “Petitioner does not expound on how the lock updater operates to deny unauthorized users access, nor does Cahill.” Prelim. Resp. 14. This contention is unavailing because claim 1 does not limit *how* the recited smart device hub operates to deny unauthorized access beyond the claim requirements. As Patent Owner asserts, claim 1 requires that the smart device hub “[i] ‘receive control information . . . [that] identifies one or more access credentials to be disabled with respect to the offline door lock’ and [ii] ‘generate a command configured to disable the one or more access credentials identified in the control information.’” *Id.* at 13. For the reasons discussed above, Petitioner sufficiently shows that Cahill’s teachings satisfy these claim requirements.

3. Summary

In view of the foregoing, we determine that Petitioner has demonstrated a reasonable likelihood of showing that independent claims 1, 18, and 26 would have been obvious over Cahill and Deros. Claims 2, 5–11, 14, 15, 17, 20, 21, 23, 25, 28, 29, 31, and 33 depend from claims 1, 18, or

26. Having reviewed Petitioner’s arguments asserting that claims 2, 5–11, 14, 15, 17, 20, 21, 23, 25, 28, 29, 31, and 33 would have been obvious over Cahill and Deros, (*see* Pet. 63–72, 74–75, 77–78), we also determine that Petitioner has demonstrated a reasonable likelihood of prevailing on its assertion as to these dependent claims.

C. Kraus-Based Grounds

Petitioner asserts three grounds based primarily on Kraus, which we refer to as the Kraus-based grounds. Specifically, Petitioner asserts that Kraus anticipates claims 1, 2, 5–11, 18, 20, 21, 26, 28, and 29 of the ’273 patent. Pet. 80–101. Petitioner also asserts that dependent claims 14, 15, 17, 23, 25, 31, and 33 would have been obvious over Kraus and Ho. *Id.* at 101–105. Additionally, Petitioner asserts that dependent claims 5, 6, 20, and 28 would have been obvious over Kraus and Wired. *Id.* at 105–108. Patent Owner challenges certain aspects of Petitioner’s analysis. Prelim. Resp. 28–43. For the reasons explained below, we express concern regarding Petitioner’s showing for the Kraus-based grounds.

Each of independent claims 1, 18, and 26 recites an “offline door lock.” Petitioner identifies Kraus’s door lock 60 as corresponding to the recited offline door lock. Pet. 81–82, 98, 100. Petitioner asserts that “Kraus discloses a door lock 60 that can only be opened or closed by a device such as a smart card placed in proximity to the door lock.” *Id.* at 82. As support, Petitioner directs us to where Kraus teaches a keyless entry system using smart cards. *Id.* at 81–82 (citing Ex. 1006 ¶ 71, Fig. 4).

In response, Patent Owner argues that “Petitioner does not show that Kraus satisfies [Petitioner’s] narrow interpretation of ‘offline door lock.’”

Prelim. Resp. 28. As support, Patent Owner points to Petitioner’s proposed construction of “offline door lock,” namely, “door lock that can only be controlled (e.g., locked and unlocked) by a device (e.g., a fob, smartphone, etc.) that is placed in proximity to a sensor of the offline door lock.” *Id.* at 28–29 (quoting Pet. 34). We note that Petitioner distinguishes an offline door lock from an online door lock, which may be controlled both remotely through an Internet-accessible network connection and locally by a device. Pet. 34 (citing Ex. 1001, 1:36–43). Patent Owner further points to where Kraus provides an illustrative example of how its system operates:

Once the devices are integrated into the mesh network, the homeowner is able to actuate, control, and access the devices using other network devices such as networked computers 80 (including computers networked via the Internet) and cell phones 30. For example, the homeowner could program the door lock 60 to transmit a signal to a cell phone 30 in response to actuation of a doorbell or an attempted entry into the home. The user could then send a signal from the cell phone 30 to turn on the light and could access the video from the camera 90 to determine who is at the door. If the party at the door is someone for whom the home owner wishes to allow entry, the homeowner could send a signal that unlocks the door.

Prelim. Resp. 30 (quoting Ex. 1006 ¶ 96) (highlighting added by Patent Owner). As Patent Owner correctly observes, “Kraus discloses that its door locks can be controlled remotely.” *Id.* Indeed, Kraus states that its “invention relates to . . . a door lock that can be monitored and controlled remotely through a mobile device or via a computer network using a radio frequency mesh network.” Ex. 1006 ¶ 2.

On the record before us, it does not appear that “Kraus discloses a door lock 60 that can only be opened or closed by a device such as a smart card placed in proximity to the door lock,” as Petitioner contends. *See*

Pet. 82. Accordingly, we express concern regarding Petitioner's showing for the recited offline door lock with respect to the Kraus-based grounds.

D. Remaining Grounds

Petitioner asserts that Cahill anticipates claims 1, 2, 7, 9, 14, 18, and 26 of the '273 patent. Pet. 36–55. Petitioner also asserts that dependent claim 8 would have been obvious over Cahill, Deros, and Kraus. *Id.* at 55–78. Patent Owner challenges certain aspects of Petitioner's analysis as to both grounds. Prelim. Resp. 6–16, 19–27 (challenging obviousness over Cahill, Deros, and Kraus); *id.* at 6–19 (challenging anticipation by Cahill). We have addressed most of Patent Owner's challenges to these grounds, which overlap with its challenges to Petitioner's asserted ground of obviousness over Cahill and Deros. *See supra* Part III.B.2.b; Prelim. Resp. 6–16, 19–27 (overlapping challenges).

With respect to Petitioner's asserted ground of anticipation by Cahill in particular, we note that Patent Owner additionally challenges Petitioner's showing for the recited WAN communication link. Prelim. Resp. 17–19. Patent Owner argues that “Cahill's disclosure of ‘e.g., satellite, broadcast radio, microwave communication link[s]’ does not disclose or even imply a WAN.” *Id.* at 17. According to Patent Owner, “[s]atellite, broadcast radio, and microwave are words that signify particular frequency bands for transmitting signals,” and they “do not define any particular transmission protocol” or “require any particular type of network or even the existence of a network at all.” *Id.* at 17–18. At this stage of the proceeding, Petitioner relies on the declaration testimony of Mr. Dumas to support its contentions regarding the recited WAN communication link. Pet. 43 (citing Ex. 1002

¶ 133). Patent Owner responds with attorney argument. *See* Prelim. Resp. 17–19. We determine that the record would benefit from further briefing on whether cited paragraph 43 of Cahill discloses the recited WAN communication link, and invite the parties to further develop this issue during trial. *See* Pet. 43 (citing Ex. 1005 ¶ 43).

IV. CONCLUSION

For the foregoing reasons, Petitioner has demonstrated on the record before us a reasonable likelihood that it will prevail in showing that claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33 of the '273 patent are unpatentable. Although we express concern as to Petitioner's showing for the Kraus-based grounds and determine that the record would benefit from further briefing on an issue related to Petitioner's showing for the ground of anticipation by Cahill, we institute trial on all challenged claims and all asserted grounds of unpatentability. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018) (holding that a decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition); Patent Trial and Appeal Board, Consolidated Trial Practice Guide, 5 (Nov. 2019), available at <https://www.uspto.gov/sites/default/files/documents/tpgnov.pdf> (“In instituting a trial, the Board will either (1) institute as to all claims challenged in the petition and on all grounds in the petition, or (2) institute on no claims and deny institution. The Board will not institute on fewer than all claims or all challenges in a petition.”). We have not, however, made a final determination with respect to the patentability of the challenged claims.

V. ORDER

For the reasons given, it is

ORDERED that *inter partes* review is instituted as to all challenged claims of the '273 patent, namely, claims 1, 2, 5–11, 14, 15, 17, 18, 20, 21, 23, 25, 26, 28, 29, 31, and 33, based on all grounds presented in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this Decision.

IPR2022-01468
Patent 10,825,273 B2

PETITIONER:

Gregory Gerwitz
Jonathan David
Wilfred Patrick
David Leach
LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK, LLP
ggewirtz.ipr@ldlkm.com
j david@lerner david.com
wpatrick@lerner david.com
dleach@lerner david.com

PATENT OWNER:

Joshua Griswold
Kenneth Darby
Kim Leung
FISH & RICHARDSON P.C.
IPR54577-0005IP1@fr.com
PTABInbound@fr.com
griswold@fr.com
kdarby@fr.com
leung@fr.com

Robert Greeson
Erik Janitens
Han Ling
NORTON ROSE FULBRIGHT US LLP
robert.greeson@nortonrosefulbright.com
erik.janitens@nortonrosefulbright.com
lu.ling@nortonrosefulbright.com