Trials@uspto.gov
571-272-7822

Entered: March 30, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SECURENET TECHNOLOGIES, LLC,
Petitioner,

v.

ICONTROL NETWORKS, INC.,
Patent Owner.

Case IPR2016-01919
Case IPR2016-01920
Patent 8,473,619 B2[1]

Before KEN B. BARRETT, PATRICK M. BOUCHER, and MINN CHUNG, *Administrative Patent Judges*.

CHUNG, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314(a) and 37 C.F.R. § 42.108

---

[1] This Order will be entered in each case. The parties are not authorized to use this caption style.

I. INTRODUCTION

SecureNet Technologies, LLC ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, and 59–62 of U.S. Patent No. 8,473,619 B2 (Ex. 1001, "the '619 patent"). IPR2016-01919, Paper 1 ("Pet."). Petitioner filed another Petition challenging claims 17, 18, 20–22, 29–31, 33, 35–41, 48–53, and 58 of the same patent. IPR2016-01920, Paper 1 ("'1920 Pet.").[2] Icontrol Networks, Inc. ("Patent Owner") filed a Preliminary Response in each case. IPR2016-01919, Paper 6 ("Prelim. Resp."); IPR2016-01920, Paper 6 ("'1920 Prelim. Resp."). We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b); 37 C.F.R. § 42.4(a).

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted unless the information presented in the Petition "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petitions and the Preliminary Responses, we conclude that the information presented in the Petitions does not establish a reasonable likelihood that Petitioner would prevail in showing the unpatentability of any of the claims challenged in the Petitions on the grounds set forth therein. Accordingly, we deny Petitioner's request to institute an *inter partes* review in each Petition.

---

[2] Because of the substantial overlap in the two proceedings, we will cite only to the Petition, the Preliminary Response, Papers, and Exhibits in IPR2016-01919 unless otherwise noted.

II. BACKGROUND

A. Real Party In Interest

SecureNet Technologies, LLC identifies itself as the real-party-in-interest. Pet. 1.

B. Related Proceedings

Petitioner asserts that the '619 patent has been asserted in the following patent infringement case: *Icontrol Networks, Inc. v. SecureNet Technologies, LLC*, No. 15-807-GMS (D. Del.). Pet. 1. Petitioner also filed petitions seeking *inter partes* review of certain claims of U.S. Patent No. 8,073,931 in IPR2016-01909 and of U.S. Patent No. 8,478,844 in IPR2016-01911 and IPR2016-01916. Pet. 1–2; Paper 4, 2.

III. THE '619 PATENT

A. Described Invention

The '619 patent describes an add-on security system that integrates with the conventional security systems existing at the premises to provide remote monitoring and control functions. Ex. 1001, Abstract, col. 3, ll. 45–62. According to the '619 patent, the remote monitoring and control functions are provided by introducing a combination of two interconnected modules: a gateway and a security server. *Id.* at col. 6, l. 66–col. 7, l. 3.

Figure 1 of the ’619 patent is reproduced below.

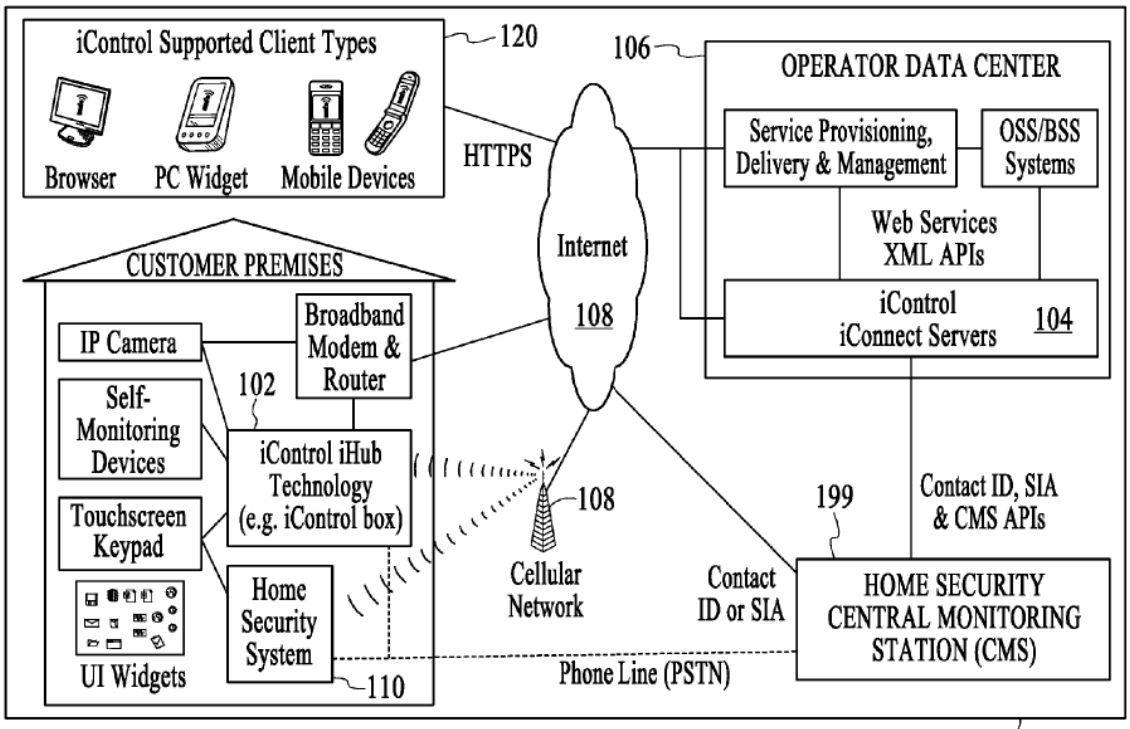

FIG.1

Figure 1 shows a block diagram of an integrated system in an exemplary embodiment of the ’619 patent. *Id.* at col. 3, ll. 7–8, col. 6, ll. 53–54. As shown in Figure 1, integrated system 100 includes gateway 102 and security servers 104 coupled to conventional home security system 110. *Id.* at col. 6, ll. 54–57; *see also* col. 4, ll. 34–40 (describing the integrated system as comprising a gateway (also referred to as an iHub gateway) and security servers (also referred to as iConnect servers)). At a customer’s home or business, the gateway connects and manages home security and monitoring devices. *Id.* at col. 6, ll. 57–59. The gateway also communicates over communication network 108 with the security servers located in the service provider’s data center 106. *Id.* at col. 6, ll. 59–64. The combination of the

gateway and the security servers enables the users to remotely monitor the premises and control the premises' security system by using remote client devices 120, such as PCs and mobile devices. *Id.* at col. 6, l. 66–col. 7, l. 27.

The gateway integrates into a home network and communicates with the home security panel in wired and wireless installations. *Id.* at col. 4, ll. 37–40, col. 11, l. 53–55. The gateway supports various wireless protocols and can interconnect with home security control panels over a wireless communication link. *Id.* at col. 11, 58–60. Figure 13 of the '619 patent is reproduced below.

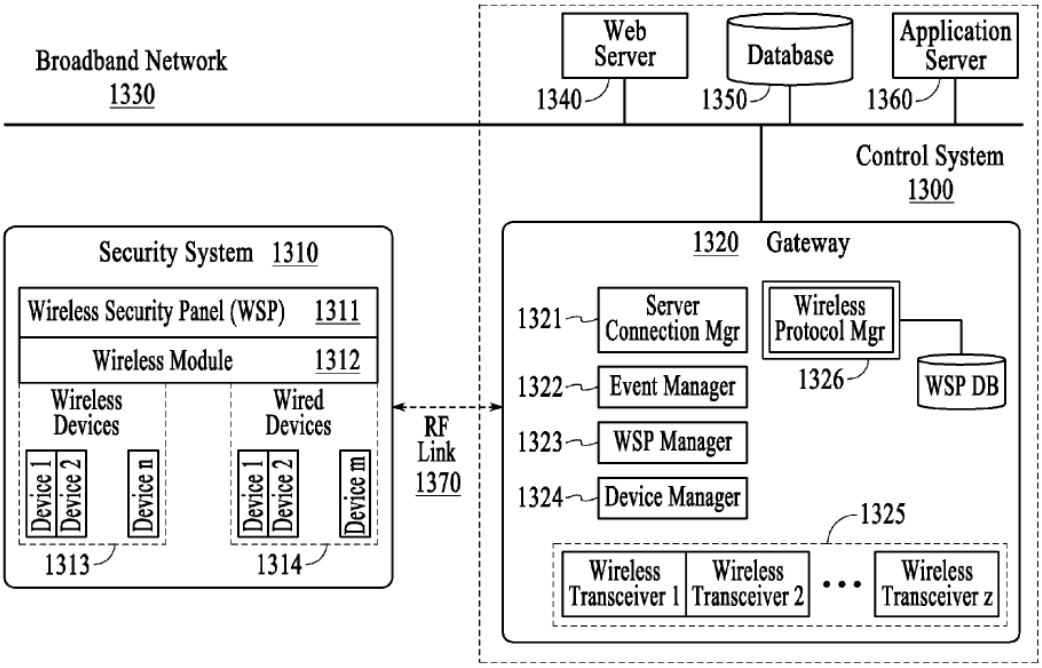

FIG.13

Figure 13 shows a block diagram of an integrated security system wirelessly interfacing to a home or business security system. *Id.* at col. 23, ll. 19–20. As shown in Figure 13, gateway 1320 is coupled to security system 1310, which may be any type of home or business security system. *Id.* at col. 23,

ll. 21–22, 34–35. Security system 1310 includes RF-capable wireless security panel (WSP) 1311 that acts as the master controller for security system 1310. *Id.* at col. 23, ll. 38–41. Gateway 1320 monitors and controls WSP 1311 and associated wireless devices 1313 and 1314 of security system 1310 over RF link 1370 using wireless transceiver 1325. *Id.* at col. 24, ll. 14–23. As shown in Figure 13, gateway 1320 includes WSP manager 1323, device manager 1324, and wireless protocol manager 1326. *Id.* at col. 24, ll. 4–5, Fig. 13. These components in conjunction implement interface protocols and algorithms to communicate with security system 1310. *Id.* at col. 24, ll. 4–14.

Figure 12 (not reproduced herein) illustrates a method of integrating the gateway with an existing security system in an exemplary embodiment. *Id.* at col. 22, ll. 17–19. Upon power up, the gateway initiates software and RF sequence 1220 to locate an existing security system by finding the wireless security panel of the security system. *Id.* at col. 22, ll. 23–25, Fig. 12. The gateway and installer then initiate sequence 1230 "to 'learn' the gateway into the security system," followed by sequence 1240 "to discover and learn the existence and capabilities" of the devices within the existing security system. *Id.* at col. 22, ll. 25–30. Figure 14 (not reproduced herein) is a flowchart that illustrates "wirelessly 'learning' the [g]ateway into an existing security system and discovering extant sensors." *Id.* at col. 24, l. 66–col. 25, l. 2. Upon power up, the gateway initiates sequences 1420 and 1425 to identify WSPs 1311 and wireless devices 1313, including all sensors in the existing security system. *Id.* at col. 25, ll. 2–6, Fig. 14 (sequence 1420, sequence 1425 ("Use Wireless transceiver to find all

sensors")). In another embodiment, the gateway is automatically installed with the security system by automatically discovering devices at the premises, such as sensors and cameras, and adding the discovered devices to the network of the integrated system. *Id.* at col. 25, ll. 44–45, 55–58.

After the gateway has completed the discovery and learning of the sensors and other devices and has been integrated into the existing security system, the integrated security system becomes operational. *Id.* at col. 22, ll. 41–44. The gateway has the ability to listen to network traffic and keep track of the status of all devices in the integrated system. *Id.* at col. 26, ll. 44–47, col. 27, ll. 6–8. The gateway utilizes the sensor updates, state changes, and supervisory signals of the network to maintain a current system of the premises being protected by the integrated system. *Id.* at col. 27, ll. 8–10. This data is sent to the security system server and stored in a database for use by server components. *Id.* at col. 27, ll. 11–13.

As discussed above, Figure 1 illustrates a gateway communicating with a security server over a communication network. Figure 2 (not reproduced herein) provides a more detailed illustration of the components of the security server. *Id.* at col. 7, ll. 34–36, Fig. 2. According to the '619 patent, the server components provide access to, and management of, the objects associated with the integrated security system installation. *Id.* at col. 8, ll. 29–31. Objects monitored by the gateway within the network where the gateway is located (i.e., the site or premises) are called "devices," which include sensors, cameras, home security panels, and other automation devices. *Id.* at col. 8, ll. 31–35, 37–41. The server components, identified as iConnect Business Components in Figure 2, store information about the

objects that are managed by the server. *Id.* at col. 9, ll. 47–49. For example, the iConnect Business Components has an interface, called DeviceConnect 260 (shown in Figure 2), to define the properties of the new devices that have been added to the integrated security system at the premises, including how the devices can be managed. *Id.* at col. 10, ll. 18–23. Common types of supported devices include sensors, home security panels, and IP cameras. *Id.* at col. 10, ll. 23–28.

As shown in Figures 1 and 2, the users or customers use client devices 120, such as a PC, a web browser, or a mobile device, to connect to the security servers to remotely monitor, control, and manage the security system at the premises. *Id.* at col. 6, l. 66–col. 7, l. 27, col. 7, l. 31–col. 8, l. 11, Figs. 1, 2.

B. Illustrative Claim

Of the challenged claims, claims 1, 60, and 61 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below with the key disputed limitations emphasized in *italics* and added paragraph breaks and indentations for the "wherein" clauses.

1. A system comprising:

a gateway located at a first location;

a connection management component coupled to the gateway and automatically establishing a wireless coupling with a security system installed at the first location, the security system including security system components,

wherein *the connection management component forms a security network by automatically discovering the security system components and integrating communications and functions of the security system components into the*

security network; and

a security server at a second location different from the first location,

wherein the security server is coupled to the gateway,

wherein the gateway receives security data from the security system components, device data of a plurality of network devices coupled to a local network of the first location that is independent of the security network, and remote data from the security server,

wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data,

wherein *the gateway* determines a state change of the security system using the processed data and *maintains objects at the security server* using the processed data,

wherein *the objects correspond to the security system components and the plurality of network devices*.

Ex. 1001, col. 46, ll. 29–54.

IV. PETITIONER'S CHALLENGES

A. Prior Art Cited in Petitioner's Challenges

Petitioner cites the following references in its challenges to patentability:

Reference and Relevant Dates	Designation	Exhibit No.
U.S. Patent Application Pub. No. 2004/0260427 Al (filed Apr. 8, 2004; published Dec. 23, 2004)	Wimsatt	Ex. 1004
U.S. Patent No. 6,580,950 B1 (filed Apr. 28, 2000; issued June 17, 2003)	Johnson	Ex. 1005

Reference and Relevant Dates	Designation	Exhibit No.
U.S. Patent No. 4,951,029 (filed Feb. 16, 1988; issued Aug. 21, 1990)	Severson	Ex. 1006
U.S. Patent Application Pub. No. 2003/0062997 A1 (filed Oct. 2, 2001; published Apr. 3, 2003)	Naidoo	Ex. 1007
U.S. Patent No. 6,748,343 B2 (filed Sept. 28, 2001; issued June 8, 2004)	Alexander	Ex. 1008
U.S. Patent Application Pub. No. 2003/0137426 A1 (filed Jan. 17, 2003; published July 24, 2003)	Anthony	Ex. 1009

B. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability in IPR2016-01919 (Pet. 3):

Claims Challenged	Statutory Basis	References
1–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, 59–62	§ 103(a)	Wimsatt, Johnson, and Severson

Petitioner asserts the following grounds of unpatentability in IPR2016-01920 ('1920 Pet. 3):

Claims Challenged	Statutory Basis	References
17, 18, 21, 22, 29–31, 33, 36, 58	§ 103(a)	Wimsatt, Johnson, Severson, and Naidoo
20, 35	§ 103(a)	Wimsatt, Johnson, Severson, Naidoo, and Anthony

Claims Challenged	Statutory Basis	References
37–41, 48–53	§ 103(a)	Wimsatt, Johnson, Severson, Naidoo, and Alexander

V. CLAIM CONSTRUCTION

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144 (2016) (holding that 37 C.F.R. § 42.100(b) "represents a reasonable exercise of the rulemaking authority that Congress delegated to the . . . Office"). Under the broadest reasonable interpretation standard, and absent any special definitions, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in view of the specification. *In re Translogic Tech. Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Petitioner does not propose any claim constructions in these proceedings. Pet. 4–5. Patent Owner criticizes Petitioner's approach but does not propose its own construction for any claim term. Prelim. Resp. 8–9. For purposes of this decision, we need not construe any claim term explicitly in order to determine whether there is a reasonable likelihood of Petitioner prevailing with respect to the challenged claims. *See* 35 U.S.C. § 314(a); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").

VI. ANALYSIS OF PETITIONER'S PRIOR ART CHALLENGES

A. Obviousness over Wimsatt, Johnson, and Severson

Petitioner contends claims 1–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, and 59–62 are unpatentable under 35 U.S.C. § 103(a) as obvious over the combination of Wimsatt, Johnson, and Severson. Pet. 7–64. Petitioner submits a Declaration of James Parker (Ex. 1002) in support of its contention. We have reviewed the parties' contentions and supporting evidence. Given the evidence of record, we are not persuaded that Petitioner has established a reasonable likelihood of prevailing on this asserted ground as to any of these claims for the reasons explained below.

1. Relevant Principles of Law

A claim is unpatentable under § 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 the 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 skill in the art; and (4) where in evidence, objective indicia of non-obviousness (i.e., secondary considerations). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

2. Overview of Wimsatt (Ex. 1004)

Wimsatt describes a system and method for implementing a contextually sensitive user interface for home automation systems. Ex. 1004, Abstract, ¶¶ 3, 22. Figure 1 of Wimsatt is reproduced below.

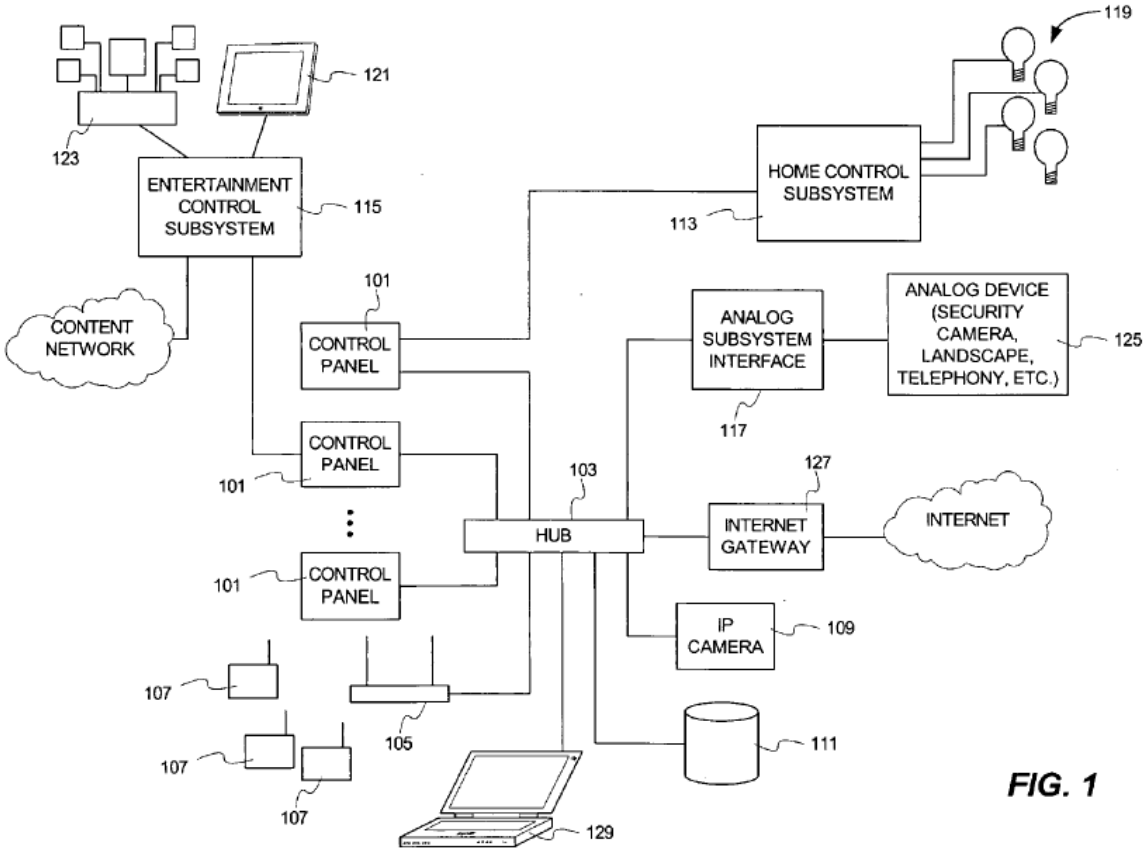

Figure 1 depicts an exemplary environment for implementing the system and method of Wimsatt. *Id.* ¶¶ 15, 34. According to Wimsatt, control panels 101 implement a programmable human interface that may include a touch-screen graphical user interface. *Id.* ¶¶ 34, 35. Wireless control panels 107 may also be used to implement similar functionality as control panels 101 in a wireless networking environment. *Id.* ¶ 37.

As shown in Figure 1 above, control panels 101 or 107 couple to home automation subsystems, such as lighting control subsystem 113 and entertainment control subsystem 115. *Id.* ¶ 39. The control panels connect to the subsystem interfaces using signaling protocols adopted by the subsystems. *Id.*

Wimsatt contemplates adding or adapting its control panels "on top of" the existing home automation subsystems, such as lighting control systems and security systems. *See id.* ¶ 23 (stating that the disclosed invention is useful because it builds "on top of" the existing home automation subsystems and that "a particular advantage" of the invention is adapting to the existing controlled devices or subsystems). Reflecting this intended use, Wimsatt describes a process implemented in control panels 101 or 107 for discovering the existing subsystems at the premises. *Id.* ¶ 45. When a control panel is coupled to a controlled device or subsystem, it interrogates the device or subsystem to learn the details of the control interface of the device or subsystem. *Id.* In some cases, this interrogation may simply be a matter of determining the controller type of the subsystem. *Id.* If the subsystem or the controlled device returns insufficient information during interrogation, the control panel can be programmed manually to support the controlled device or subsystem. *Id.*

According to Wimsatt, unlike conventional home automation systems, which required a separate, independent control system for each subsystem with a separate, dedicated human interface, Wimsatt's control panels can access and control any of the controlled devices or subsystems that are coupled to the control panels. *Id.* ¶¶ 43–44. By utilizing common interface

elements, the control panels of Wimsatt present substantially the same set of controls and provide similar graphical user interfaces to various home automation subsystems in a context sensitive manner. *Id.* ¶¶ 63, 77.

3. Overview of Johnson (Ex. 1005)

Johnson discloses an "Internet based home communications system for allowing a homeowner to monitor and control various features of their home from a distant location via a global computer network." Ex. 1005, Abstract. Johnson discloses a system comprising a plurality of control devices, a control unit in communication with the devices and connected to the Internet, and a data center having server computers connected to the Internet and the control unit. *Id.* at col. 2, ll. 8–14.

> The homeowner is capable of monitoring and controlling the control device within the home by accessing a web page displayed by the data center through a conventional web browser on a computer. The homeowner can view, monitor and control features of their home through the web page such as viewing interior images of their home or adjusting the thermostat for the interior of their home. In addition, the control unit may notify the appropriate supplier when propane or food becomes low within the home through the global computer network.

Id. at col. 2, ll. 19–28. Control devices include "lighting controls, heating controls, moisture controls, freeze controls, pet feeding devices, propane gauge, interior cameras, exterior cameras, security system, smoke alarm and various other devices." *Id.* at col. 2, ll. 13–18.

4. Overview of Severson (Ex. 1006)

Severson discloses a programmable security alarm system including a system controller "which is programmably responsive to a plurality of distributed wireless and hardwired alarm sensors/transducers and which communicates with neighboring system controllers and a central station interactively monitoring a number of subscriber systems." Ex. 1006, col. 1, ll. 5–12. Each system controller is programmable with sensor/transducer numbers, options, and features. *Id.* at col. 23, ll. 60–63. Severson explains:

> Even further and without human intervention, once the sensors transducers are initially programmed, each system controller may be operated to "self-learn" each of its sensors. In this mode as the sensors/transducers report to the controller for the first time and after the controller confirms the existence of a proper house code or unit number, they are logged into the controller's RAM memory. Human error is thus minimized even though during hand programming with the wireless key pad 13, the circuitry performs a similar subroutine to log the assigned [sensor/transducer] S/T numbers into RAM.

Id. at col. 25, ll. 2–13.

5. Discussion

a. Claims 1, 60, and 61

Independent claims 1, 60, and 61 all recite "the connection management component" "forms" or "forming" "a security network by automatically discovering the security system components and integrating communications and functions of the security system components into the security network" and "the gateway . . . maintains objects at the security server using the processed data, wherein the objects correspond to the

security system components and the plurality of network devices." Ex. 1001, col. 46, ll. 35–39, 49–54; col. 49, l. 52–col. 50, l. 3; col. 50, ll. 12–19, 26–32, 40–45. These two limitations are identified by Petitioner as claim limitations 1[d] and 1[h], respectively, with respect to claim 1. Pet. 13, 25. We discuss each of these limitations below.

i) Limitation 1[d]

Petitioner contends that the combination of Wimsatt, Johnson, and Severson renders obvious the claim limitation identified by Petitioner as limitation 1[d], i.e., the limitation reciting "the connection management component forms a security network by automatically discovering the security system components and integrating communications and functions of the security system components into the security network" (the "two-part network formation limitation"). Pet. 13–18. The plain language of this claim limitation indicates that "the connection management component forms a security network" by performing two separate operations—that is, by "automatically discovering the security system components" and "integrating communications and functions of the security system components into the security network." We first address the parties' disputes regarding whether Wimsatt or Wimsatt in view of Severson teaches "automatically discovering the security system components."

Petitioner asserts that, although Wimsatt does not illustrate sensors in its security system, a person of ordinary skill in the art would have understood Wimsatt's security system to include sensors and that those sensors would be the "security system components" recited in the claims.

Id. at 10. Petitioner concedes that "Wimsatt does not explicitly disclose that its security system's sensors are automatically discovered using this [Universal Plug-and-Play (UPnP)] process – it only explicitly discloses that the 'security system' is discovered." *Id.* at 14. Petitioner then argues "[a] POSITA would have understood that discovering the security system would also include discovering its sensors." *Id.* (citing Ex. 1002 ¶ 92). Patent Owner asserts (Prelim. Resp. 12), and we agree, that this argument from Petitioner is too conclusory to satisfy Petitioner's burden. The cited portion of the expert testimony merely repeats, without adequate elaboration or explanation, Petitioner's argument and, therefore, similarly is conclusory. *See* Ex. 1002 ¶ 92.

Petitioner, arguing in the alternative, turns to Severson for the disclosure of a system having a controller that may "self-learn" sensors "without human intervention." Pet. 14 (citing Ex. 1006, col. 25, ll. 3–13). Petitioner asserts

> In describing a system installation process, Severson explains that the sensors and controller are mounted at the home and then "the controller is enabled and self-learns each of its sensors/transducers as they report their status." (Ex. 1006, 25:51-26:7; *see also, id.*, 23:60-25:50.) As a result, "[i]nstallation time is thereby reduced with minimal potential installer error, due to the CPU self-learning its reporting sensors." (*Id.*, 25:51-26:7.) This is similar to the auto-discovery process described in the '619 patent. (*See, e.g.*, Ex. 1001, FIG. 14, 24:66-26:5.)

Id. at 14–15.

Patent Owner disputes this contention and argues that Severson's self-learning is not "automatically discovering" within the meaning of the

claimed invention. Prelim. Resp. 13–14. Petitioner does not propose a construction for "automatically discovering," but, as quoted above, merely asserts that Severson's process is "similar" to that disclosed in the '619 patent. Pet. 15 (citing Ex. 1001, Fig. 14, col. 24, l. 66–col. 26, l. 5). The process described in the '619 patent and upon which Petitioner relies, however, indicates that the first step after gateway power-up, and *before* entering "learn mode," is for the gateway to "identify" accessible wireless security panels and wireless devices. Ex. 1001, col. 25, ll. 1–11, Fig. 14 (software sequences 1420 and 1425). In contrast, as Patent Owner notes, Severson discloses that the sensors and controllers are initially programmed in a manual process. Prelim. Resp. 13–14 (citing Ex. 1006, col. 25, ll. 3–6 ("Even further and without human intervention, *once the sensors transducers are initially programmed*, each system controller may be operated to 'self-learn' each of its sensors.") (emphasis by Patent Owner), 22–24, 51–61). Indeed, Severson describes that Severson's controller "self-learns" the sensors when those sensors report their status after first being programmed manually. Ex. 1006, col. 25, ll. 51–65. Thus, Severson suggests that the sensors must first be identified for the controller before Severson's controller "self-learns" those sensors "without human intervention." Even if Severson's process is "similar" to the learning process described in the '619 patent, we are not persuaded Petitioner has demonstrated sufficiently that Severson discloses "automatically discovering the security system components," as recited in the claims 1, 60, and 61.

Petitioner contends that it would have been obvious to a person of ordinary skill in the art to combine the "auto-discovery disclosure" of

Severson with Wimsatt and Johnson "so that the control panel 101 in Wimsatt can auto-discover the security sensors in addition to the discovering the security system controller." Pet. 15. Citing Severson and the Parker Declaration, Petitioner asserts that "[t]his would predictably result in an easier sensor installation process and reduce the likelihood of installer error." *Id.* (citing Ex. 1002 ¶ 93; Ex. 1006, col. 26, ll. 5–7). Patent Owner argues that Petitioner's contention is at odds with Wimsatt's description that its control panels communicate with a security system, not the underlying security system components, such as the security sensors. Prelim. Resp. 15–16 (citing Ex. 1004 ¶¶ 5, 23, 30, 31, 58, 62, 65). Patent Owner asserts that, because "Wimsatt's control panels are limited to functionality regarding the *status* of a security system" and do not communicate with or control individual security system components, Petitioner's proposed modification would unnecessarily complicate installation, not simplify it. *Id.* at 16.

We agree with Patent Owner that Wimsatt's control panels do not communicate directly with the security system components, such as the sensors. As discussed above in our overview of Wimsatt, Wimsatt is directed to providing control panels with consistent user interfaces to existing home subsystems, such as home automation systems and security systems. Ex. 1004 ¶¶ 3, 22, 23, 77. Hence, Wimsatt's control panels discover the existing subsystems at the premises, such as a security system, and learn the details of the *control interface* of the subsystems, but do not in general discover or communicate with the components internal to the subsystems, such as the security system components or sensors. *Id.* ¶ 45. Indeed, Wimsatt describes that "[i]n most cases it is *not necessary* for every

control panel 101/107 to have detailed knowledge of a particular controlled device or subsystem. Instead, it is *sufficient* to be aware of the existence of each controlled device and the functionality available from that device." *Id.* ¶ 46 (emphases added). Furthermore, because Wimsatt contemplates adding or adapting its control panels "on top of" the existing security systems (*id.* ¶ 23), Wimsatt's discovery process would have expected that the sensors would have already been installed and the sensor installation process previously completed. Hence, the record indicates that Wimsatt is *not* concerned with sensor installation processes, such as those described in Severson. Petitioner does not explain why the combination of Wimsatt and Severson would nonetheless "predictably result in an easier sensor installation process and reduce the likelihood of installer error." Pet. 15. The cited portion of the expert testimony repeats, without adequate elaboration or explanation, Petitioner's unpersuasive argument and, therefore, similarly is unpersuasive. *See* Ex. 1002 ¶ 93.

Petitioner's argument that Severson "illustrates the ability and desire for similar controllers to automatically discover devices at the security component level" (Pet. 15) is similarly unpersuasive because Wimsatt is not concerned with discovering security system components.

The rest of Petitioner's arguments regarding the reasons to combine Wimsatt with Severson and Johnson are too conclusory to satisfy Petitioner's burden. For example, similar to Petitioner's conclusory contention discussed above, Petitioner asserts that "Wimsatt already discloses an automatic discovery process for learning the security system so it would be obvious to a POSITA to further discover the sensors that form

part of that system." *Id.* (citing Ex. 1002 ¶ 94). Petitioner also contends that "[a] POSITA would understand that adding an extra step in the automatic discovery process to include discovery of the sensors would be easy to implement." *Id.* (citing Ex. 1002 ¶ 94). The cited portion of the expert testimony again repeats, without adequate elaboration or explanation, Petitioner's conclusory assertions. *See* Ex. 1002 ¶ 94. These conclusory statements are insufficient to provide the requisite "reasoned explanation" to justify combining Wimsatt with Severson and Johnson to teach "automatically discovering the security system components," as recited in claims 1, 60, and 61. *See In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016).

In addition, Petitioner does not demonstrate sufficiently that the combination of Wimsatt, Severson, and Johnson renders obvious the entire claim limitation identified by Petitioner as limitation 1[d], i.e., the "two-part network formation limitation," because Petitioner does not adequately address the limitation as a whole. As discussed above, the "two-part network formation limitation" recites that "the connection management component forms a security network" by performing two separate operations—that is, by "automatically discovering the security system components" *and* "integrating communications and functions of the security system components into the security network." Hence, in order to demonstrate the combination of Wimsatt, Johnson, and Severson renders the "two-part network formation limitation" obvious, Petitioner must identify the differences between the claimed subject matter (i.e., forming a security network by performing two operations discussed above) and the prior art

references, and demonstrate that the differences are such that the subject matter, as a whole, would have been obvious to a person having ordinary skill in the art. *See KSR*, 550 U.S. at 406. Petitioner makes no such showing in the Petition.

Instead, Petitioner focuses largely on the integration of functions only, and asserts that a person of ordinary skill in the art would have understood that "the claimed 'security network' is formed in Wimsatt (as modified by Johnson and Severson) as a result of the control panel integrating the functions of the security system sensors." Pet. 17 (citing Ex. 1002 ¶¶ 98–100). Petitioner's analysis is largely devoid of a discussion regarding how a network may be formed by "automatically discovering the security system components." *See id.* at 17–18. The mere fact that Wimsatt (as modified by Johnson and Severson) teaches an integrated security system with sensors does not necessarily show that the control panel of Wimsatt "forms a security network" by "automatically discovering the security system components," e.g., the sensors, *and* "integrating communications and functions of the security system components into the security network." Hence, Petitioner's analysis is deficient because Petitioner does not demonstrate sufficiently how the combination of the references renders obvious the subject matter of the "two-part network formation limitation" as a whole. The cited portion of the expert testimony does not adequately address the "automatically discovering the security system components" aspect or the subject matter of the "two-part network formation limitation" as a whole, either, and, therefore, does not remedy the deficiency in Petitioner's argument. *See* Ex. 1002 ¶¶ 98–100.

Therefore, Petitioner does not demonstrate sufficiently that the "two-part network formation limitation" recited in claims 1, 60, and 61 is rendered obvious by the combination of Wimsatt, Johnson, and Severson.

ii) Limitation 1[h]

As discussed above, Petitioner identifies as claim limitation 1[h] the limitation reciting "the gateway . . . maintains objects at the security server using the processed data, wherein the objects correspond to the security system components and the plurality of network devices." Pet. 25.

Petitioner contends that the combination of Wimsatt and Johnson teaches this limitation. *Id.* at 26. Petitioner (*id.* at 26–27) points to the webpage shown in Johnson's Figure 3, which is reproduced below:

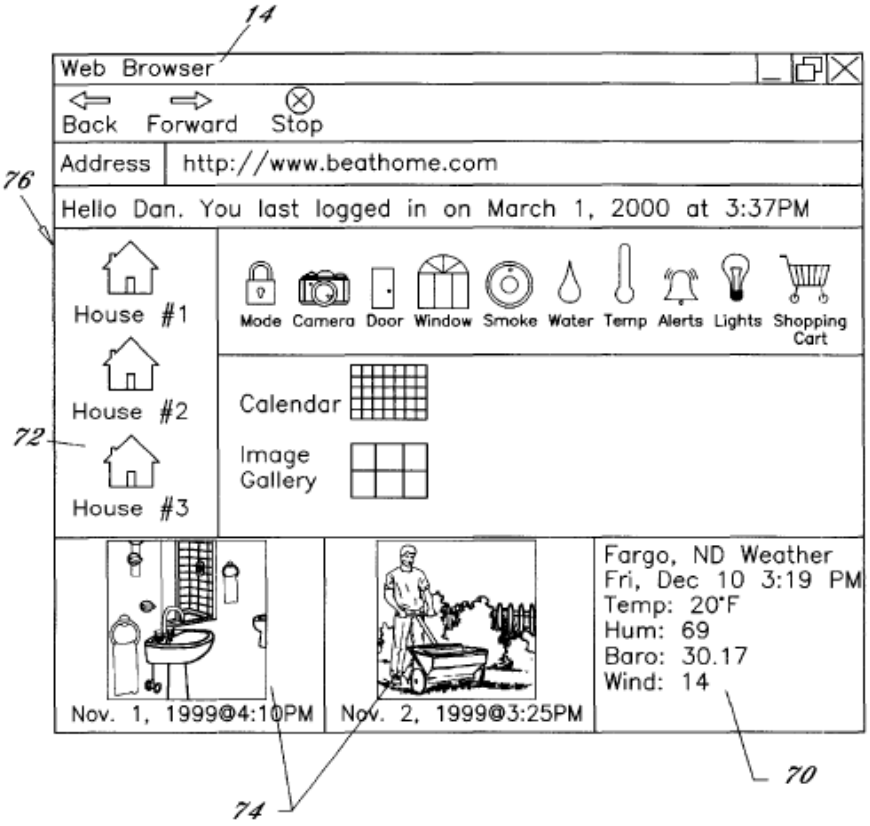

Figure 3 depicts "a browser containing the control page displaying some of the features of [Johnson's] invention that allow the homeowner to monitor and control their home through a global computer network such as the Internet." Ex. 1005, col. 3, ll. 30–33.

Petitioner asserts

> A POSITA would have understood that the icons illustrated on the above web page [of Johnson's Figure 3] represent particular controlled devices located within the home in Wimsatt. (Ex. 1002, ¶ 119.) These icons are the claimed "objects" maintained at the data center 20 servers. For example, the icon labeled "camera" is an object maintained at the server corresponding to the IP camera 109. Similarly, the icons labeled "door" and "window" are objects maintained at the server corresponding to a door sensor and a window sensor, respectively.

Pet. 28. The cited expert testimony appears to be the same assertion with no elaboration or explanation for the bases of the opinion. *See* Ex. 1002 ¶ 119.

Patent Owner argues that Petitioner's analysis regarding this limitation is flawed and that Johnson does not disclose the recited "objects" maintained at the server. Prelim. Resp. 16–20. Patent Owner argues that Mr. Parker's "bald opinion" that one of ordinary skill would have understood the icons to represent particular controlled devices should be entitled to no weight. *Id.* at 17. Patent Owner contends that Johnson does not describe the nature of the icons. *Id.* Patent Owner also argues that there is depicted in Figure 3 only one each of a camera icon, a window icon, and a door icon, and persuasively argues that one would expect there to be more than one of each of these items in a house and, therefore, it would be illogical for the icons to correspond to a *particular* security system

component as alleged. *Id.* at 17–18. After a review of the portions of Johnson cited by Petitioner, we are unable to discern any elaboration regarding these icons that persuades us that Petitioner's proposition is correct. *See* Pet. 26–29. Additionally, and as Patent Owner notes, Petitioner apparently identifies Wimsatt's IP camera 109 as corresponding to the camera icon in Johnson's system. Prelim. Resp. 17–18 (citing Pet. 28). This mixing-and-matching of references' elements without adequate explanation is confusing rather than clarifying.

Accordingly, we are not persuaded that the icons in Johnson's Figure 3 would be understood by a person of ordinary skill in the art to correspond to recited objects corresponding to the security system components and network devices.

Even if Johnson's icons were found to be the claimed "objects," Petitioner does not persuasively demonstrate that those icons are maintained at the security server. *Cf.* Prelim. Resp. 19–20 (Patent Owner arguing that "[t]here is no explanation [in Johnson] regarding where those icons are maintained or what they even represent."). Indeed, Petitioner does not cite any disclosure in Johnson describing the "icons" in Figure 3 as "objects" maintained at the server. Petitioner's conclusory assertion and the corresponding equally conclusory testimony from Mr. Parker that "[t]hese icons [of Johnson] are the claimed 'objects' maintained at the data center 20 servers" are insufficient and not persuasive.

iii) Summary

Based on the record presented, the information presented in the Petition does not demonstrate a reasonable likelihood of Petitioner prevailing in its challenge to independent claims 1, 60, and 61 under 35 U.S.C. § 103(a) as obvious over the combination of Wimsatt, Johnson, and Severson.

b. Claims 2–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, 59, and 62

Claims 2–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, 59, and 62 each depend directly or indirectly from claim 1. Petitioner's arguments and evidence presented with respect to these dependent claims do not remedy the deficiencies in Petitioner's analysis of the challenged independent claims discussed above. *See* Pet. 29–54, 64. Therefore, Petitioner does not demonstrate a reasonable likelihood of prevailing in its challenge to dependent claims 2–9, 12–16, 19, 23–28, 32, 34, 42–47, 54–57, 59, and 62 under 35 U.S.C. § 103(a) as obvious over the combination of Wimsatt, Johnson, and Severson.

B. Obviousness over Wimsatt, Johnson, Severson, and Naidoo

In IPR2016-01920, Petitioner contends claims 17, 18, 21, 22, 29–31, 33, 36, and 58 are unpatentable under 35 U.S.C. § 103(a) as obvious over the combination of Wimsatt, Johnson, Severson, and Naidoo. '1920 Pet. 8–42, 56–57. Each of these challenged claims depends directly or indirectly from claim 1. Because of this, Petitioner first discusses independent claim 1. *Id.* at 9. For the two limitations discussed above in the context of IPR2016-01919—limitations 1[d] and 1[h]—Petitioner repeats the same or

substantially the same arguments we found unpersuasive. *See id.* at 14–19, 27–30. Petitioner's subsequent analysis of the dependent claims subject to this ground does not cure the deficiencies underlying Petitioner's challenge of independent claim 1. *See id.* at 30–42, 56–57. Thus, for the same reasons discussed above, Petitioner has not shown a reasonable likelihood of prevailing in its challenge to dependent claims 17, 18, 21, 22, 29–31, 33, 36, and 58 under 35 U.S.C. § 103(a) as obvious over the combination of Wimsatt, Johnson, Severson, and Naidoo.

C. Obviousness over Wimsatt, Johnson, Severson, Naidoo, and Anthony or Alexander

Petitioner adds the teachings of Anthony to the basic combination of Wimsatt, Johnson, Severson, and Naidoo in an asserted ground of obviousness as to dependent claims 20 and 35. '1920 Pet. 35–36, 42. Petitioner also contends that dependent claims 37–41 and 48–53 would have been obvious over the combination of Wimsatt, Johnson, Severson, Naidoo, and Alexander. *Id.* at 42–56. Each of these challenged claims depends directly or indirectly from claim 1, and Petitioner's subsequent analysis of the dependent claims subject to these grounds does not cure the deficiencies underlying Petitioner's challenge of independent claim 1. Thus, for the same reasons discussed above, Petitioner has not shown a reasonable likelihood of prevailing in showing that claims 20 and 35 would have been obvious over the combination of Wimsatt, Johnson, Severson, Naidoo, and Anthony, or in showing that claims 37–41 and 48–53 would have been

obvious over the combination of Wimsatt, Johnson, Severson, Naidoo, and Alexander.

VII. CONCLUSION

Based on the arguments and evidence presented in the Petitions, we conclude Petitioner has not demonstrated a reasonable likelihood that Petitioner would prevail in showing at least one of the challenged claims of the ’619 patent is unpatentable based on any asserted ground of unpatentability in IPR2016-01919 or IPR2016-01920. Therefore, we do not institute an *inter partes* review with respect to any of the challenged claims of the ’619 patent.

VIII. ORDER

In consideration of the foregoing, it is ORDERED that both Petitions are denied as to all challenged claims of the ’619 patent in each Petition, and no trial is instituted.

PETITIONER:

Erik B. Milch
Jennifer Volk-Fortier
Frank Pietrantonio
COOLEY LLP
emilch@cooley.com
jvolkfortier@cooley.com
fpietrantonio@cooley.com

PATENT OWNER:

Matthew A. Argenti
Michael T. Rosato
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com