IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VIVINT LLC

Petitioner,

DUKE W. ZINSER
Patent Owner,

U.S. Patent No. 7,583,191
Issue Date: September 1, 2009
Title: SECURITY SYSTEM AND METHOD FOR USE OF SAME

Inter Partes Review No.:IPR2026-00300

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 7,583,191 UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §§42.1-.80, 42.100-.107

***Mail Stop* "*PATENT BOARD*"**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST

Exhibit #	***Description***
1001	U.S. Patent No. 7,583,191 ("the '191 Patent")
1002	Prosecution History of the '191 Patent ("File History")
1003	Declaration of Petitioner's Expert James Parker
1004	U.S. Patent Publication 2004/0086093 ("Schranz")
1005	Re-Exam Prosecution History of the '191 Patent
1006	U.S. Pat. No. 6,429,893
1007	U.S. Pat. No. 6,778,084
1008	U.S. Patent Publication 2002/0147982
1009	*Curriculum Vitae* of James Parker
1010	James Parker Patent Summary

I. INTRODUCTION

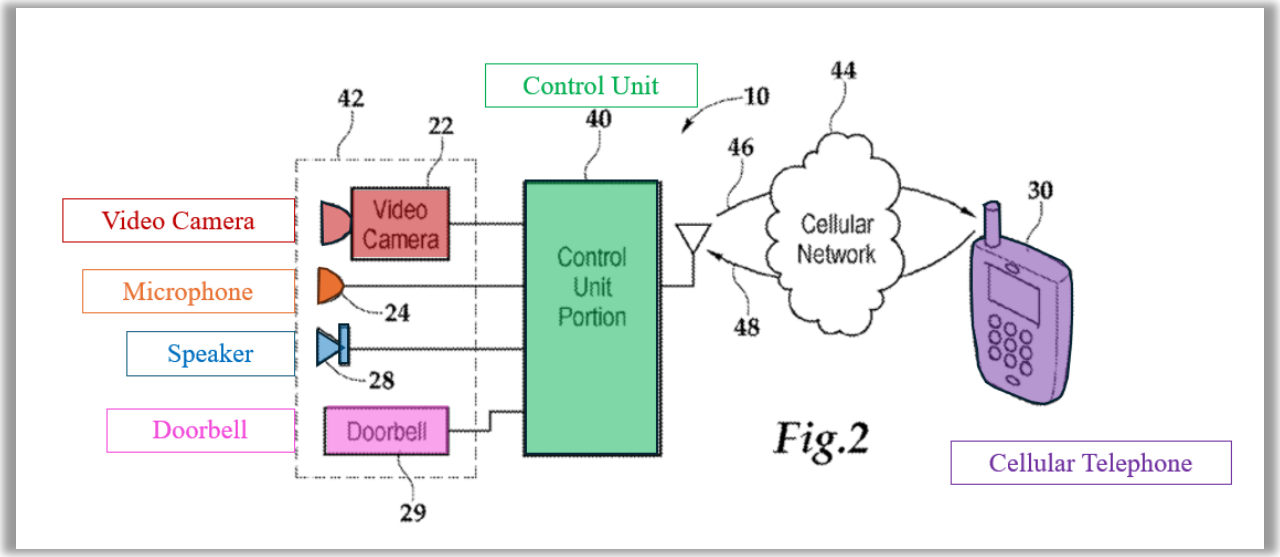
Vivint LLC ("Petitioner") hereby petitions for an *inter partes* review (IPR) of U.S. Patent No. 7,583,191 ("the '191 Patent", EX-1001). Petitioner respectfully submits that Claims 21-47, (the "Challenged Claims") of the '191 Patent are unpatentable under 35 U.S.C. §103 in view of following ground:

Grounds	Claims	Basis	References
Ground 1	21-47	103	Schranz

This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the Challenged Claims. Accordingly, it is respectfully requested that the Board institute an *inter partes* review.

II. OVERVIEW

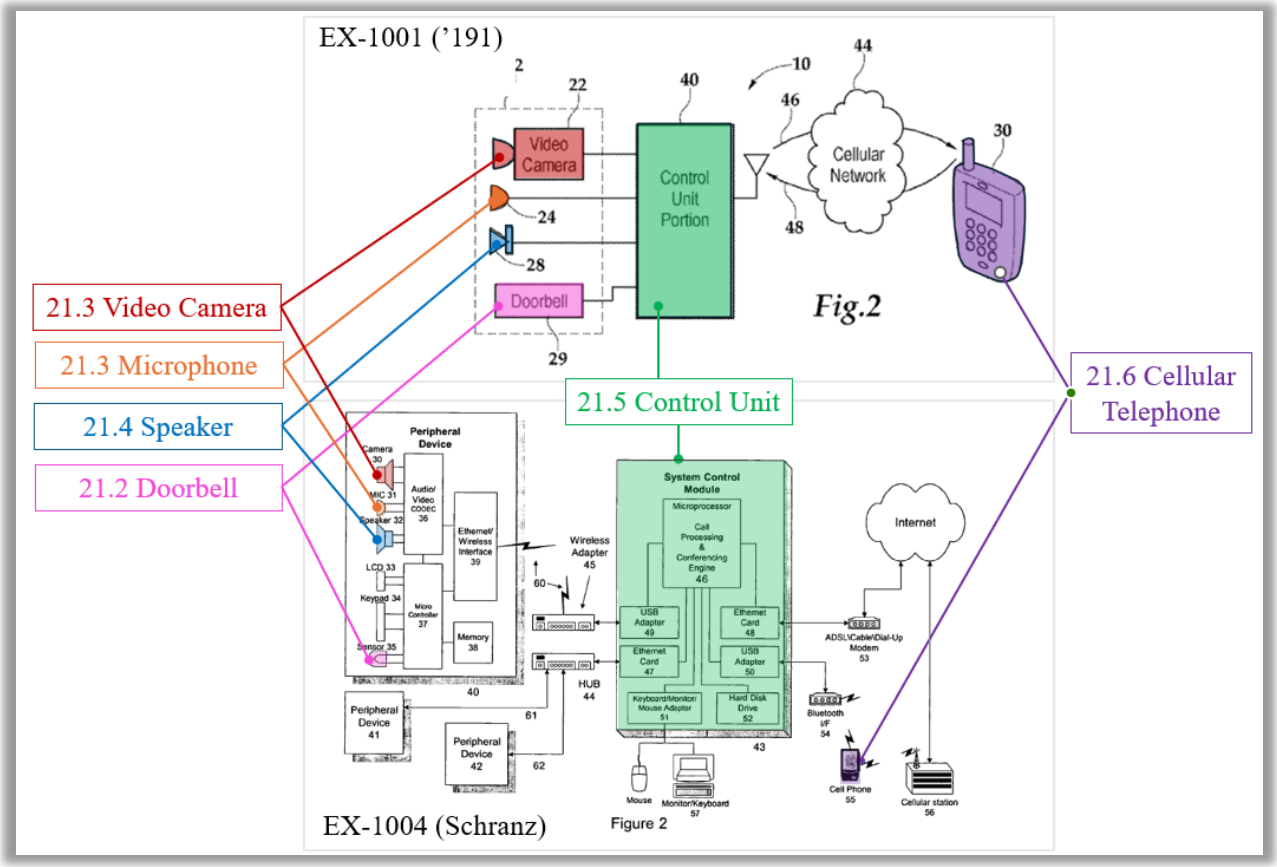
The '191 Patent is directed to a doorbell monitoring system to allow remote monitoring and surveillance. The architecture of the doorbell monitoring system is illustrated in Figure 2 of the '191 Patent and includes a control unit (green), in communication with video camera 22 (red), exterior microphone 24 (orange), exterior speaker 28 (blue) and doorbell 29 (pink).



EX-1001 Figure 2 (annotated to show limitations recited in independent Claim 21).

The control unit 40 interfaces with communication portion 42 and relays data and communications between the communication portion 42 and the cellular telephone 30 (purple) via a cellular network 44. In operation, when an individual approaches the doorway, an event is detected e.g., by ringing of the doorbell or the proximity detector. In turn, the video camera 22 and external microphone 24 capture visual and audio communications at the doorway 18 (not shown). The captured doorway visual and audio communications are transmitted to the cellular telephone 30 of the homeowner 16 via the control unit 40 that is in communication with the video camera 22, external microphone 24 and exterior speaker 28 as well as the cellular network for communicating with the cellular telephone 30.

The prior art Schranz reference discloses the identical architecture to provide doorbell monitoring services. The figure below illustrates a comparison of Figure 2 of the '191 Patent (top) with Figure 2 of Schranz (bottom) with common elements annotated with the limitations recited in independent Claim 21 of the '191 Patent:



EX-1001, Figure 2; EX-1004, Figure 2 (annotated).

Like the '191 Patent, Schranz discloses an architecture for a doorbell monitoring system that includes a control unit 43 (green), in communication with video camera 30 (red), exterior microphone 31 (orange), exterior speaker 32 (blue)

and doorbell 35 (pink).[1] The control unit 43 relays data and communications to the cellular telephone 55 (purple) via a cellular network. Like the '191 Patent, Schranz discloses that when an individual approaches the doorway, an event is detected, e.g., by ringing of the doorbell or the motion sensor. In turn, the video camera 30 and external microphone 31 capture visual and audio communications at the doorway. The captured doorway visual and audio communications are transmitted to the cellular telephone 55 via a control unit 43 that is in communication with the video camera 30, external microphone 31, and exterior speaker 32 as well as a cellular network for communicating with the cellular telephone 55. The Challenged Claims of the '191 Patent recite well-known features associated with a doorbell monitoring system as disclosed by Schranz and are therefore unpatentable.

III. GROUNDS FOR STANDING 37 C.F.R. § 42.104(a)

Petitioners certify that the '191 Patent is available for *inter partes* review and that Petitioners are not barred or estopped from requesting an inter partes review of the Challenged Claims on the grounds identified herein. 37 C.F.R. § 42.104(a). This Petition is filed pursuant to 37 C.F.R. § 42.106(a).

[1] Schranz discloses that sensor 35 may be a doorbell signal. EX-1004, ¶48.

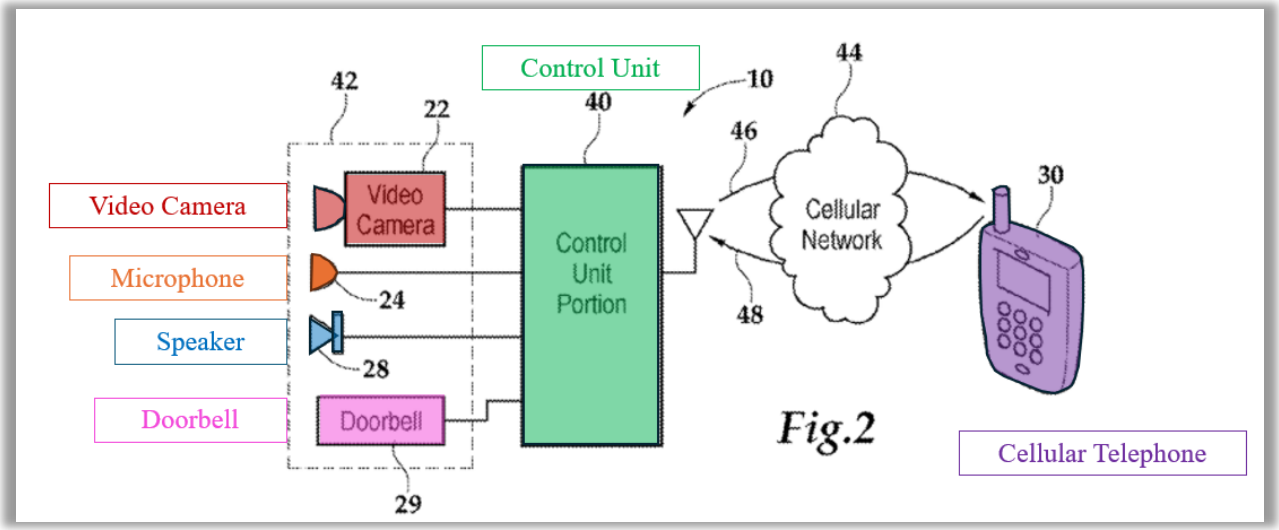
IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§II and IV-V of this Petition and in the attached Declaration of Petitioner's Expert, EX-1003, the subject matter claimed in the '191 Patent was obvious over the prior art to a person of ordinary skill in the art ("POSITA") at the time of the purported invention.

A. Overview of the '191 Patent

The '191 Patent is directed to a conventional security system that wirelessly streams audio and video from a property's entry point to a remote user's cellular telephone. EX-1001, Abstract. The '191 Patent explains that previous systems are merely "reactive" and typically only provide alarm monitors to predetermined third parties. EX-1001, 1:13-14, 1:23-26. The '191 Patent explains that there exists a need a for a "proactive" system that relays audio and visual information from the property to the remote user (*i.e.,* the property owner) during an alarm thereby deterring unwanted individuals. EX-1001, 1:31-44; EX-1003, ¶32.

Figure 2 illustrates the doorbell monitoring security system and connection to the remote user's cellular telephone.



EX-1001, Figure 2; EX-1003, ¶33.

As illustrated, the doorbell monitoring system utilizes a control unit 40 (green) to relay data from a communication portion 42 to the cellular network 44 and the remote user's telephone 30 (purple). EX-1001, 3:10-13. The communication portion 42 includes a video camera 22 (red) and microphone 24 (orange) for capturing audio and visual information at the doorway. EX-1001, 2:36-37, 3:13-17. The communication portion 42 also includes doorbell 29 (pink) for detecting a triggering event and speaker 28 (blue) to transmit audio from the remote user to the doorway. EX-1001, 2:38-47, 3:13-17; EX-1003, ¶34.

The '191 Patent explains that the system operates as follows: (1) An individual approaches the doorway; (2) The proximity detector is activated; (3) Video camera 22 and microphone 24 capture the visual and audio data; (4) The control unit processes the received audio-visual data from the video camera and

microphone; (5) The control unit notifies the remote user that a triggering event has occurred; (6) The control unit interfaces with the remote user's telephone allowing the remote user to receive additional information (*i.e.,* an image or a video file), and establish a real-time teleconferencing stream to the communication portion 42. EX-1001, Figure 5, 4:46-59, 6:13-67. The general operation of the system is illustrated by Figure 5 below. EX-1001, Figure 5; EX-1003, ¶35.

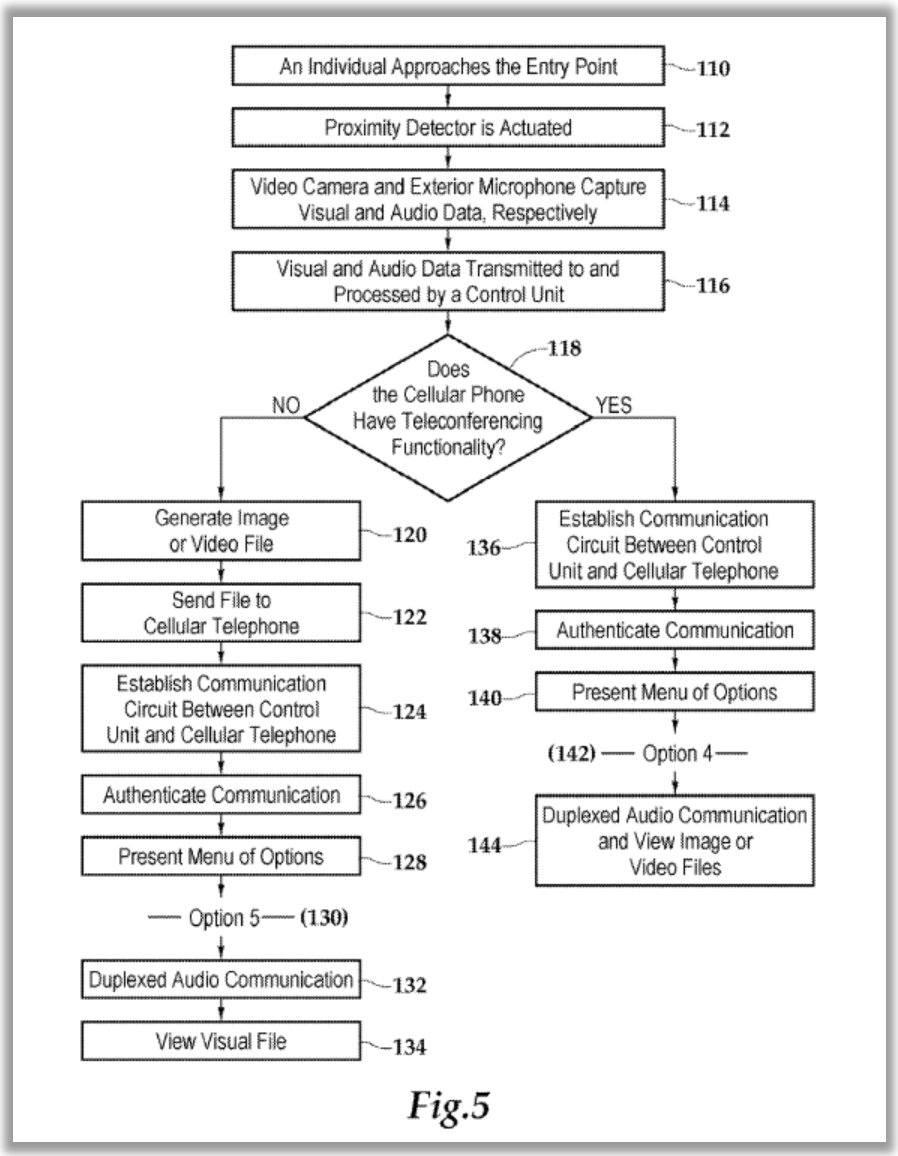


Fig.5

EX-1001, Figure 5.

The ’191 Patent issued with twenty claims where Claims 1, 8, 14 and 19 being independent. However, as discussed below, the ’191 patent was subject to a reexamination proceeding which resulted in a Reexamination Certificate that cancelled Claims 1, 8, 14 and 19, and found new Claims 21-47 patentable.

Claims 21 and 34 are independent claims. Claim 21 is representative:

[21.0] A doorbell monitoring system comprising:

[21.1] a doorway having an environment;

[21.2] a doorbell located in an entry point, activation of the doorbell being a triggering event;

[21.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;

[21.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

[21.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera

and the external microphone, and for communicating the received audio communications to the external speaker; and

[21.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit;

[21.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

[21.8] wherein the entry point visual and audio communications are wirelessly streamed to the control unit;

[21.9] wherein the control unit is configured to store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit wherein a control panel is configured to allow an individual to manage a security system;

[21.10] wherein an alarm system interface of the control panel is configured to interface with the security system;

[21.11] wherein the video camera is configured to collect the entry point visual communications captured by the single communications unit before the triggering event;

[21.12] wherein the video camera is configured to collect additional visual communications after the triggering event;

[21.13] wherein the doorbell monitoring system is configured to establish communication with the control unit upon activation of the doorbell;

[21.14] wherein at least a portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone; and

[21.15] wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

B. Prosecution History of the '191 Patent

The '191 Patent was filed on November 14, 2006, as Application No. 11/559,808. EX-1001 (21-22). During prosecution, the examiner initially rejected claims 1-20 as anticipated by Chiang (U.S. 6,778,084). EX-1002, 58. In response, the applicant revised the independent claims to disclose a "doorbell monitoring system" rather than a "security system" and included a limitation requiring "a doorbell located in the doorway, the ringing of the doorbell being a triggering event." EX-1002, 80. The Applicant argued that Chang's intrusion detection devices, which include "glass breakage sensors or other shock sensors, motion

detectors, contact switches, proximity or alignment sensors" (U.S. 6,778,084, 4:1-4), does not disclose a "doorbell." EX-1002, 92. The examiner subsequently allowed the claims, and the Patent issued as U.S. 7,583,191 on September 1, 2009. EX-1002, 100.

On June 19, 2024, Patent Owner requested an *Ex Parte* Reexamination of the '191 Patent.

C. Priority Date of the Challenged Claims

The '191 Patent issued from an application filed on November 14, 2006. Thus, the priority date is November 14, 2006.

D. Claim Construction

Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction. EX-1003, ¶39.

E. Level of Ordinary Skill in the Art

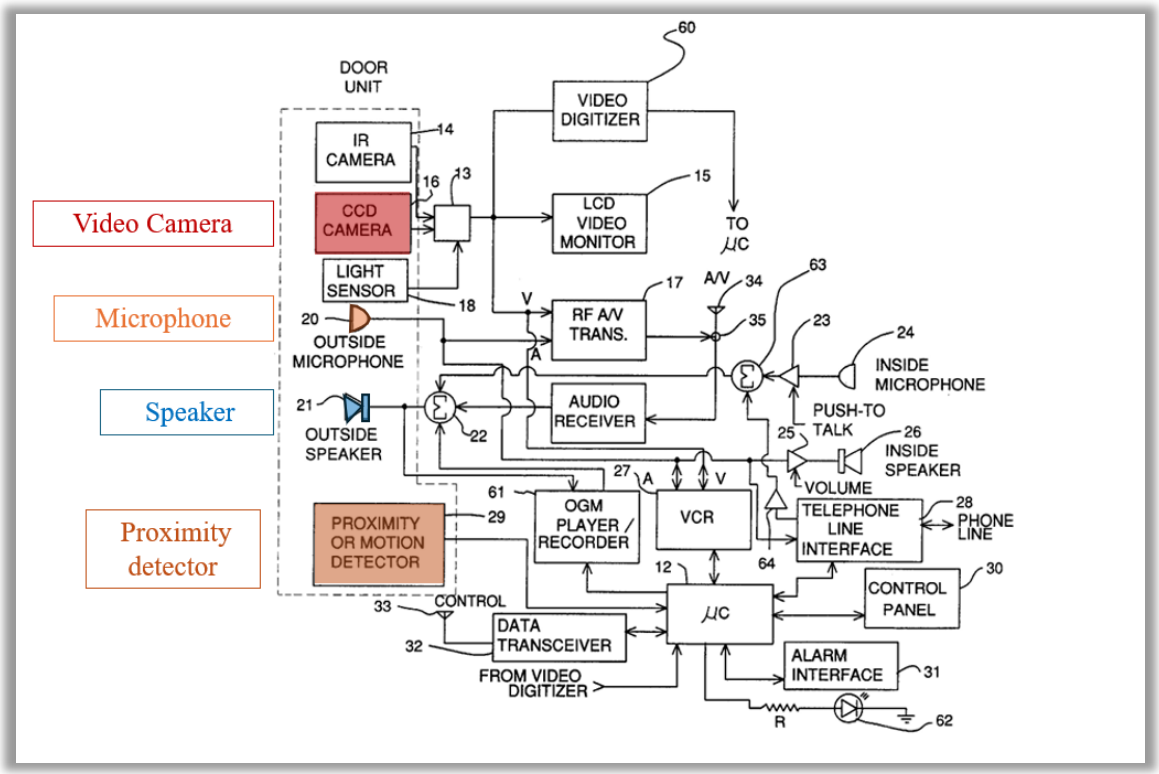
A Person of Ordinary Skill in the Art ("POSITA") in November 2006 would have been someone knowledgeable and familiar with communication protocols used by components in a security system for transferring information between components. A POSITA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having at least a bachelor's degree in electrical or electronic engineering, computer science, or a related field,

and at least two to three years of training or additional work experience in the area of security system components, or a related field. Additional hands-on and design experience could compensate for less formal education, and vice versa. The knowledge and skill of a POSITA is further reflected in the prior art references themselves, as well as the State of the Art, discussed below. EX-1003, ¶44.

F. State of the Art

This section describes the State of the Art as of the Priority Date. This section, and the expert testimony and documentary evidence cited, provide additional factual support for the general knowledge, common understanding and skill of a POSITA as of the Priority Date. This section provides additional factual support and motivation to modify and combine the teachings in the references, and further demonstrates why doing so would involve a reasonable expectation of success. EX-1003, ¶45.

Prior art secuirty systems were generally used to monitor entrances to a building in order to prevent unauthorized access to the building. These systems used varous sensors to detect unauthorized persons. One such system is show below in Figure 1: EX-1003, ¶47.



EX-1006, Figure 1; EX-1003, ¶47.

The security system includes a door unit with several different types of sensors for generating signals, including a video camera 16 (red) for generating a video signal, an outside microphone 20 (orange) for generating an audio signal, an outside speaker 21 (blue) for playing an audio signal, and a proximity or motion detector 29 (brown) for detecting motion in the vicinity of the door. EX-1006, 4:10-54. A remote unit allows a person to remotely monitor the activity at the door, play video and audio captured at the door unit, and control the security system. EX-1006, 1:37-50. The remote unit also allows the remote user to communicate orally with a person at the door. EX-1006, 6:6-8; EX-1003, ¶48.

Another prior art security system, EX-1007, includes one or more cameras capable of capturing video and audio data, one or more audio devices capable of capturing and broadcasting audio data, and one or more intrusion devices capable of detecting any intrusion onto the premises, such as glass breakage sensors, motion detectors, contact switches, proximity or alignment sensors. One skilled in the art will appreciate that such system components are placed and installed about the premises to provide optimum surveillance and security capabilities while being inconspicuous or resistant to disablement. EX-1007, 3:56-4:8; EX-1003, ¶49.

The security components communicate with an on-premises master terminal box, and the master terminal box communicates wirelessly with a remote command unit. The master terminal box is capable of two-way wireless audio and video communication with the command unit. The remote command unit includes an LCD screen, speaker, video camera, and microphone to allow two-way wireless audio and video communication between the user of the remote command unit and the security components connected to the master terminal box. EX-1007, 4:9-5:2; EX-1003, ¶50.

Another prior art security system provided real-time monitoring with remote access through use of broadband features, including audio and video capabilities, web access and wireless capabilities. EX-1008, ¶30. The security system includes any type of sensor to detect alarm conditions including magnetic contact switches,

audio sensors, infrared sensors, motion detectors, fire alarms, and carbon monoxide sensors. EX-1008, ¶36. In addition, the security system includes one or more video cameras that operable to capture video of the monitored premises. EX-1008, ¶37; EX-1003, ¶51.

The video cameras can include "smart" cameras to perform video capture, compression and storage and to communicate with the security system using a wireless network. EX-1008, ¶84. The smart camera may perform many functions including but not limited to analyzing data from the video camera to determine whether an alarm condition exists, accessing data stored in memory; generating alarm video to transmit to the security system in response to detection of an alarm condition; and communicating with the security system and a remote user. The video camera may capture and record video continuously in memory, and then based on predefined criteria, older video may be discarded. The remote user may adjust the predetermined criteria including adjusting the recording times, duration, and total length of recordings. EX-1008, ¶81; EX-1003, ¶52.

In one prior art example, the video sent to the security system begins at least just prior to the occurrence of the alarm condition and may end after the conclusion of the alarm condition, which helps identify false alarms. EX-1008, ¶38. The remote user has the ability to control the functionality of the security system. Once authenticated, the remote user can control the functionality of the system including

arming or disarming the security system; adjusting sensitivities of the sensors; adjusting alarm condition detection sensitivity; remote surveillance; adjusting camera settings; and reviewing alarms and recordings. These functions may also include remote surveillance, referred to as "lifestyle video." EX-1008, ¶43. The smart camera is capable of streaming live audio and video from the residence during alarm conditions, as well as for lifestyle viewing over the world wide web. EX-1008, ¶82; EX-1003, ¶53.

V. IDENTIFICATION OF HOW CLAIMS ARE UNPATENTABLE

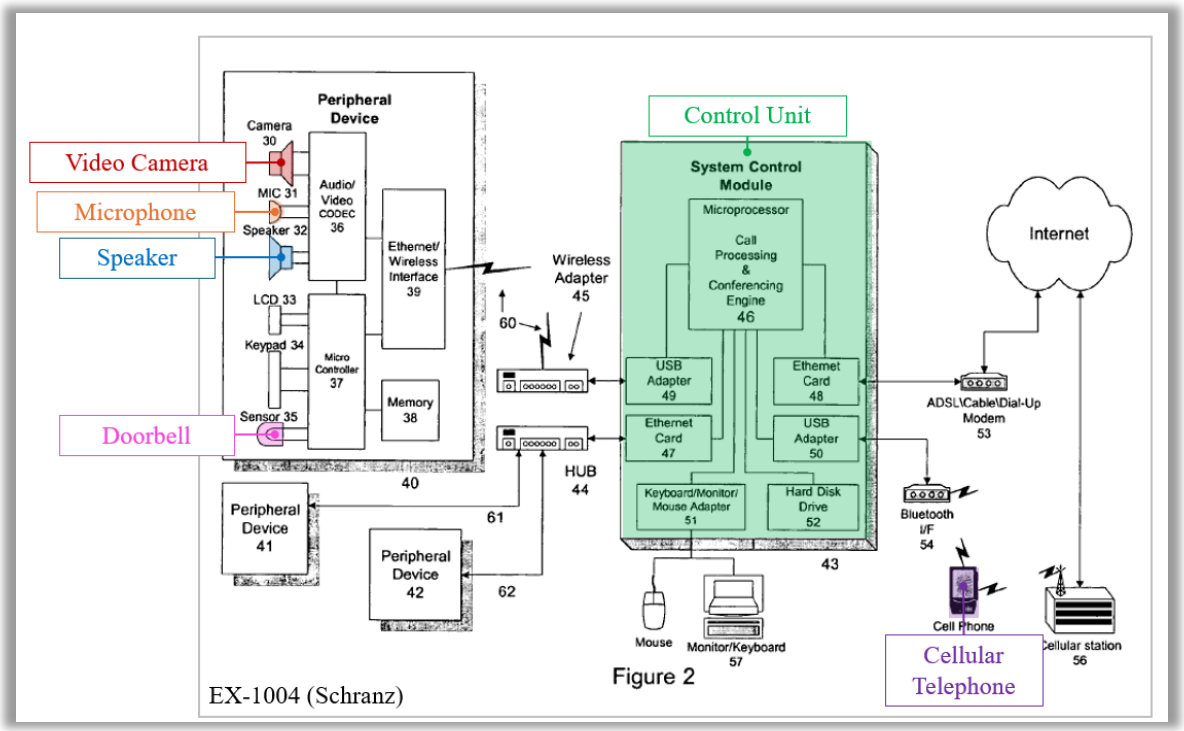
A. Ground 1: Claims 21-47 Are Obvious Over Schranz

1. The Schranz Reference

Schranz published as U.S. Patent Publication 2004/0086093 (EX-1004) titled "VOIP SECURITY MONITORING & ALARM SYSTEM" on May 6, 2004, from application no. 10/694,678 filed on October 29, 2003, and claims priority to provisional application no. 60/421,849 filed on October 29, 2002. Schranz qualifies as prior art under §102(b). It was not cited nor applied by the examiner during prosecution of the Challenged Claims.

Schranz is directed to a residential, commercial or industrial security monitoring and alarm system. It includes a plurality of peripheral devices in communication with a system control module (SCM). Figure 2 illustrates that peripheral devices 40, 41, and 42 are situated throughout the user premises at strategic exterior or interior locations, such as doors, windows, hallways or rooms.

These devices detect an event, called the detected agent, and signal the system control module (SCM) 43 via a wireline or wireless physical interface 60, 61 and 62, respectively. EX-1004, ¶47; EX-1003, ¶56.



EX-1004 Fig. 2; EX-1003, ¶56.

An Internet interface connects the SCM 43 to the Internet. Once notified of an alarm, the SCM 43 begins the process of establishing a VoIP call, defined as "Voice/Video over Internet Protocol" in Schranz (EX-1004, Abstract), with a remote user using VoIP call signaling protocols such as SIP or H.323. The remote user can be in the IP network, the PSTN or a cellular network. EX-1004, ¶47; EX-1003, ¶57.

The peripheral devices include a camera 30 (red), microphone 31 (orange), speaker 32 (blue), and sensor 35 that could include a doorbell (pink). The peripheral devices will be located in various strategic locations including an intercom located in hallways and rooms, a doorbell-intercom located at the main entrance to the premises, and an environmentally hardened security surveillance unit located exterior to the building. EX-1004, ¶48; EX-1003, ¶58.

Upon detection of an event the system establishes a Voice/Video over Internet Protocol (VoIP) call to a remote user or monitoring service. Schranz discloses that using VoIP technology leverages several inherent advantages related to IP packet networks. A VoIP call is one that uses a VoIP call signaling protocol to set up a call and a VoIP transport protocol to deliver the payload (audio and video information). Examples of VoIP call signaling protocols include, but are not limited to, the Session Initiation Protocol (SIP) from the Internet Engineering Task Force (IETF) and H.323 from the International Telecommunications Union (ITU). An example of a VoIP transport protocol includes, but is not limited to, the Real-Time Transport Protocol (RTP) from the IETF. EX-1004, ¶0001; EX-1003, ¶59.

Schranz explains that the peripheral devices, including the camera 30 (red) and microphone 31 (orange), are typically placed in "a doorbell-intercom located at the main entrance to the premises." EX-1004, ¶48. In armed mode, the peripheral devices, including camera 30 and microphone 31, monitor the

environment and notify the SCM when someone is at the door or when motion takes place. EX-1004, ¶¶58-59, 61. The SCM then provides a notification to the remote user. EX-1004, ¶¶64; 61. The SCM routes the audio and video data from the peripheral device to the remote agent. EX-1004 ¶¶24, 63-64; EX-1003, ¶60.

Schranz also discloses that a web server runs on the SCM and contains a user web application. The user can access this website remotely and securely through monitor/keyboard 57 using any Internet browser that supports the https protocol. The website is a graphical monitor and control program. The user can visually see the current configuration and the status of all peripheral devices. Moreover, the user can change the configuration and initiate a VoIP call to any one of the peripheral devices and can control all aspects of the system. EX-1004, ¶50; EX-1003, ¶61.

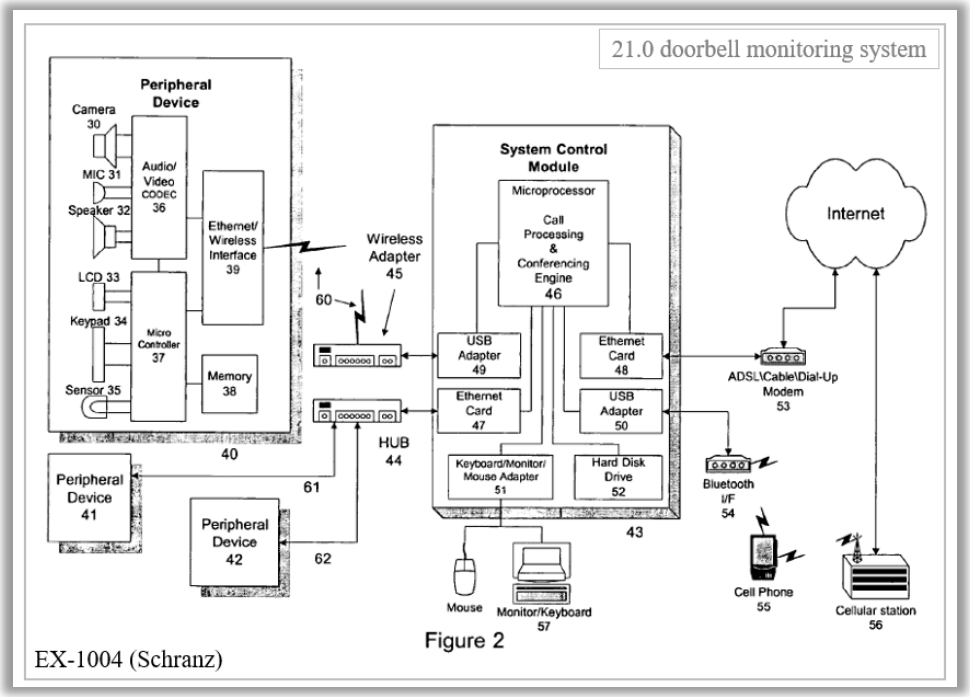
2. Detailed Application of Schranz to Claims 21-47

Claim 21

[21.0] A doorbell monitoring system comprising:

To the extent the preamble is limiting, Schranz discloses a VoIP security monitoring and alarm system in the form of a doorbell-intercom. EX-1004, Title, ¶48. The VoIP security monitoring and alarm system utilizes peripheral devices, including cameras, microphones, motion detectors, and doorbell signals, to detect an event and notify a remote user. EX-1004 Abstract, ¶48, *See also* ¶53

("Peripheral devices with varying functionality can be chosen and installed simultaneously, such as intercoms, doorbell-intercoms or surveillance units."). The VoIP security monitoring and alarm system can be located in hallways or "at the main entrance to the premises." EX-1004 ¶48. Therefore, Schranz discloses a *doorbell monitoring system* as shown below. EX-1003, ¶62.



EX-1004, Figure 2 (Annotated) ; EX-1003, ¶62.

[21.1] a doorway having an environment;

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system can be "situated throughout the user premises at strategic exterior or interior locations, such as doors, windows, hallways or rooms." EX-1004, ¶47. The VoIP security system utilizes a number of peripheral devices such as

"intercoms, doorbell-intercoms or surveillance units" that are mounted at strategic exterior locations to monitor "entrances to the building such as doors and windows." EX-1004, ¶53. Further, Schranz discloses a system control module connected to the peripheral devices that can be "located anywhere in the home." EX-1004, ¶53. A POSITA understood that Schranz discloses that a doorway located at an entrance to a building is the recited *doorway having an environment*. EX-1003, ¶3463.

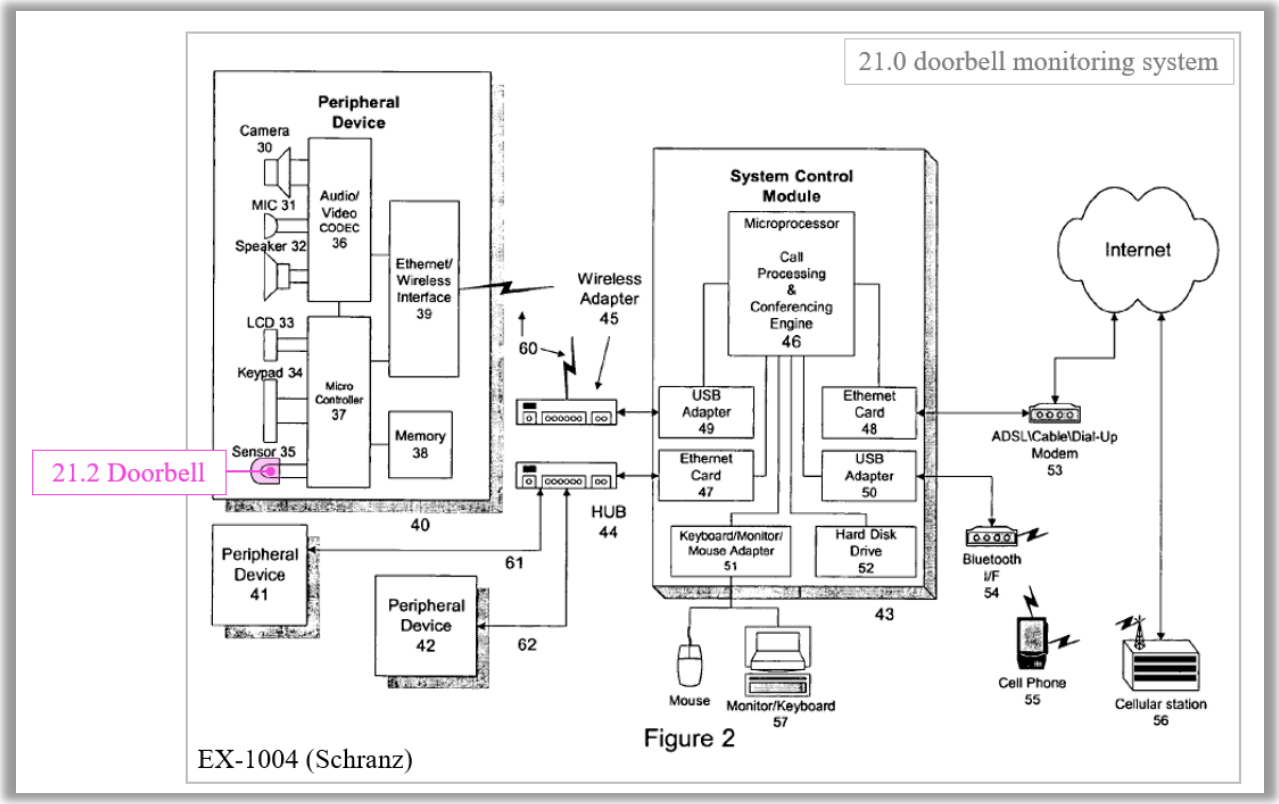
[21.2] a doorbell located in an entry point, activation of the doorbell being a triggering event;

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system utilizes a number of peripheral devices such as "intercoms, doorbell-intercoms or surveillance units." EX-1004, ¶53. In particular and as shown below, one such device, peripheral device 40, includes sensor 35 (pink) which can be "a motion detector, infrared radiation sensor or ***doorbell signal.***" EX-1004, ¶48 (emphasis added). Schranz further discloses that the doorbell is mounted at strategic exterior locations to monitor "entrances to the building such as doors and windows" [*a doorbell located in an entry point*]. EX-1004, ¶53. Schranz explains that the doorbell signal functions in two modes: normal mode and armed mode. EX-1004, ¶58. In normal mode, the doorbell, sensor 35, can simply be used to detect an event and notify that someone is at the door. EX-1003, ¶64.

> In the normal mode, the peripheral devices function as intercoms and doorbells. They can be used to page people in the house, place outgoing or answer incoming VoIP calls and notify that someone is at the door. They still notify the SCM when an event like motion, infrared radiation or vibration detection takes place.

EX-1004, ¶59; EX-1003, ¶64.

In alarm mode, the doorbell, sensor 35, "functions as normal, but in addition to notifying people locally with a chime when pressed, it also places a call to a pre-configured VoIP address." EX-1004, ¶60. In other words, the only difference between the normal and armed modes of Schranz's system is that "[i]n Alarm Mode the SCM will generate an outbound call when a peripheral device notifies it of an event." EX-1004, ¶61. Schranz discloses that the peripheral devices detect an event, called the detected agent, and signals the system control module (SCM) [*activation of the doorbell being a triggering event*]. EX-1004 ¶47. Therefore, a POSITA understood that Schranz discloses that activation of a doorbell is an event that causes the triggering of actions [*a doorbell located in an entry point, activation of the doorbell being a triggering event*]. *EX-1003, ¶65.*



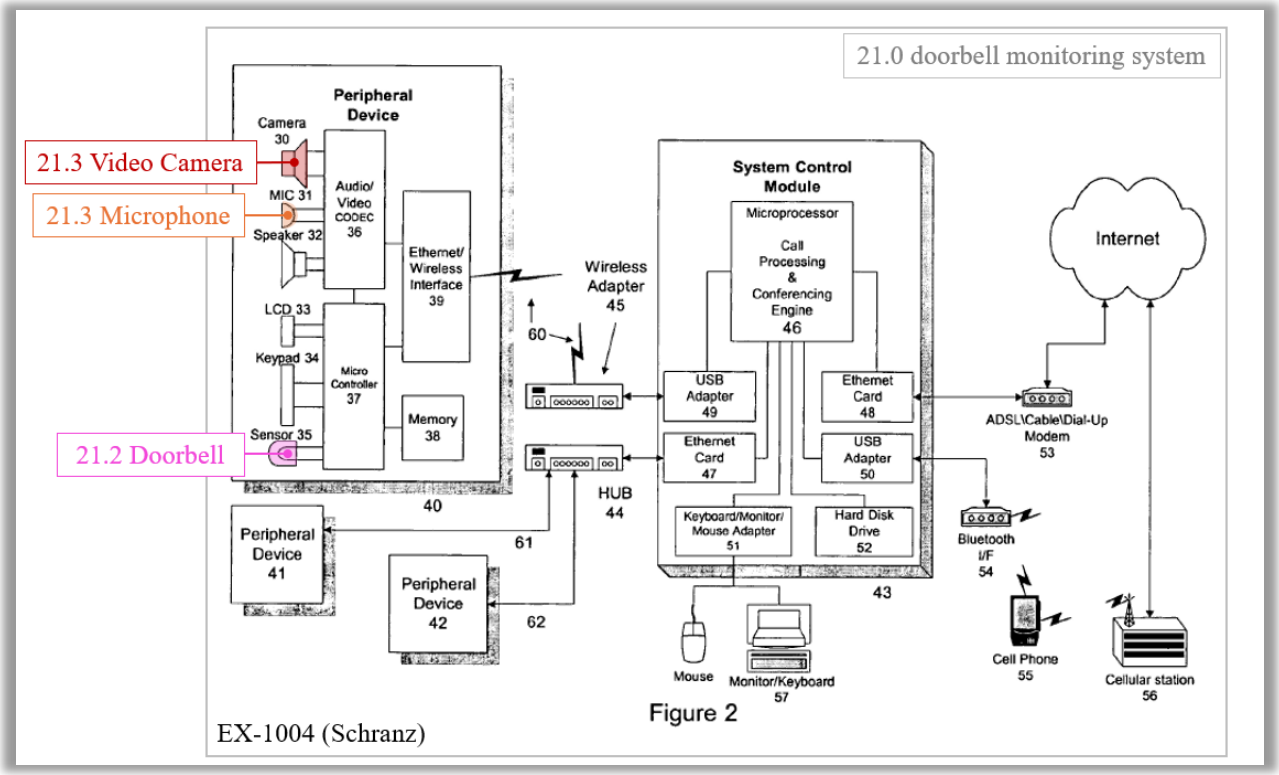
EX-1004, Figure 2 (annotated) ; EX-1003, ¶65.

> ***[21.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;***

Schranz discloses this limitation. Schranz discloses a VoIP security monitoring and alarm system with peripheral devices (*i.e.,* camera 30, microphone 31, speaker 32) situated at doors, windows, hallways or rooms [*a video camera and an external microphone disposed in the entry point*]. EX-1004, ¶47. The peripheral devices, including the doorbell, "detect an event" and notify the system control module. EX-1004, Abstract. The system control module then establishes a

VoIP call with a remote user so that the remote user "will hear ambient audio and see video images from the peripheral device in the location of the alarm" [*for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications*]. EX-1004, Abstract, Claim 1; EX-1003, ¶66.

Specifically with respect to Figure 2 below, Schranz discloses a VoIP security monitoring and alarm system utilizing peripheral device 40 which includes "***camera 30***, ***microphone 31***, speaker 32, LCD 33, keypad 34, sensor 35, audio/video CODEC 36." EX-1004, ¶48 (emphasis added). Schranz states that camera 30 (red) [*video camera*] may be a CCTV board camera that supports both video and audio through CODEC 36. Schranz explains that CODEC 36 "digitizes the analog video signal into a standard digital format." EX-1004, ¶48; EX-1003, ¶67.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶67.

Schranz further explains that the peripheral devices, including the camera 30 (red) [*video camera*] and microphone 31 (orange) [*external microphone*], are typically placed in "a doorbell-intercom located at the main entrance to the premises" [*disposed in the entry point*]. EX-1004, ¶48. Further Schranz states that, in armed mode, the peripheral devices, including the doorbell monitor the environment, and when someone rings the doorbell, in addition to notifying people locally with a chime when pressed, it also places a call to a pre-configured VoIP address via the SCM [*responsive to the triggering event*]. EX-1004, ¶¶60-

61. The SCM then provides a notification to the remote user. EX-1004, ¶¶64, 61. The SCM routes the audio and video data captured from the peripheral device to the remote agent. EX-1004 ¶¶24, 63-64. In other words, the microphone and camera of the peripheral device at the entry point send audio and video data to the SCM which routes the audio and video data to a remote user when a person rings the doorbell [*capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications*]. EX-1003, ¶68.

Schranz's disclosure is consistent with the '191 Patent's disclosure that "a triggering event such as the ringing of a doorbell, initiates the contact of the control unit to the homeowner 16; however, the plurality of video cameras 22 collect video for the homeowner's review irrespective of the occurrence of the triggering event." EX-1001 3:4-8, 4:46-51; EX-1003, ¶69.

To the extent that Patent Owner asserts that Schranz does not expressly disclose capturing of the video and audio data responsive to the ringing of the doorbell, a POSITA would be motivated to modify the teachings of Schranz to capture video and audio data responsive to the ringing of the doorbell and would have a reasonable expectation of success in doing so. As discussed in the State of the Art section, it was well-known and common at the time of the alleged invention to allow a user to adjust the system parameters, including sensor sensitivities, camera settings, and remote surveillance settings. EX-1008, ¶43. The purpose of

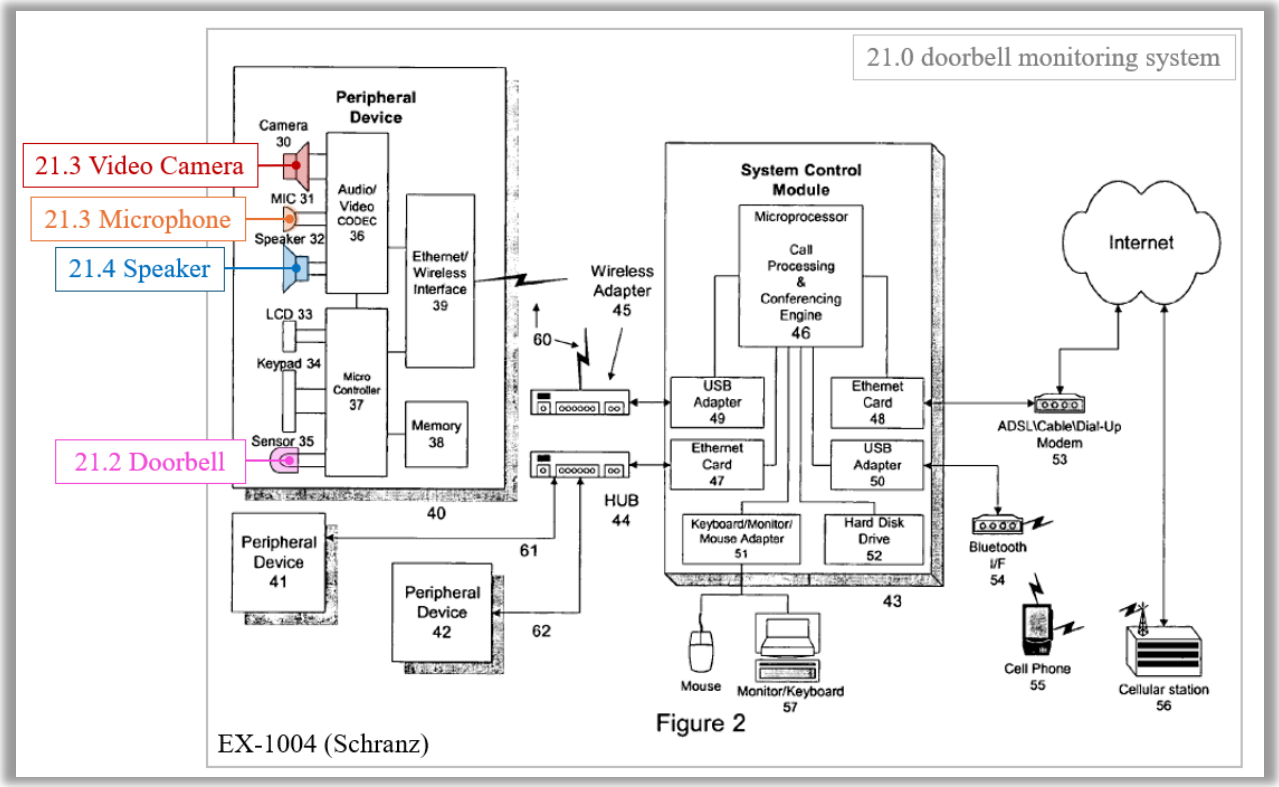
this well-known configurability was to allow for the user to adjust the amount of time to capture the video and audio data from before, during, and after triggering events (pushing of the doorbell button). EX-1003, ¶70.

Schranz itself contemplates this type of user-driven configurability, and specifically discloses that the user sets up system control parameters. EX-1004, ¶¶56, 57. Accordingly, a POSITA would have found it obvious to capture video and audio data responsive to the ringing of the doorbell, with the amount of time defined by the user's system control parameters. Such a modification would have amounted to nothing more than the application of a known technique, configurable capture timing, to improve a similar device in the same, predictable way. EX-1003, ¶71.

[21.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

Schranz discloses this limitation. Specifically with respect to Figure 2 as shown below, Schranz's VoIP security monitoring and alarm system utilizes a peripheral device 40 which includes "a camera 30, microphone 31, ***speaker 32***, LCD 33, keypad 34, sensor 35, audio/video CODEC 36." EX-1004, ¶48 (emphasis added). The speaker 32 (blue) in conjunction with CODEX 36 allows the remote user to play an announcement, prerecorded message, or to enable audio to be sent from the remote location to speaker 32 [*for rendering received audio communications*]. EX-1004, ¶33, 65. In particular, CODEC 36 decodes PCM

samples from the system control module 43 into an analog audio signal to be played by the speaker. EX-1004, ¶48. As explained above, Schranz's peripheral devices, including speaker 32 (blue below), are typically placed in a "a doorbell-intercom located at the main entrance to the premises" [*disposed in the entry point*]. EX-1004, ¶48; EX-1003, ¶72.

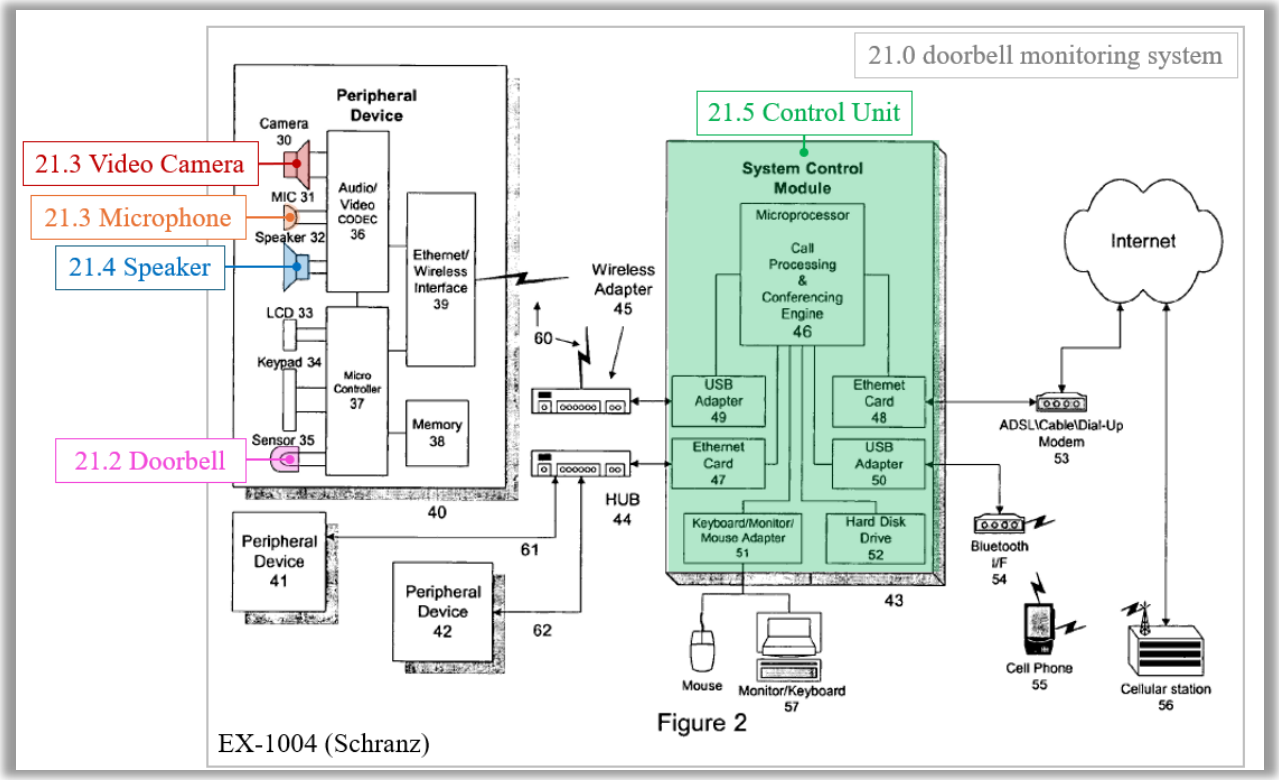


EX-1004, Figure 2 (Annotated) ; EX-1003, ¶72.

[21.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera and the external

microphone, and for communicating the received audio communications to the external speaker; and

Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a system control module 43 (green) [*control unit*] in communication with a set of peripheral devices, including camera 30 (red) [*video camera*], microphone 31 (orange) [*external microphone*], and speaker 32 (blue) [*external speaker*], via either ethernet or wireless connections. EX-1004, ¶48. Schranz explains that the system control module [*control unit*] is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system." EX-1004., ¶49; EX-1003, ¶73.



EX-1004, Figure 2 (Annotated) ; EX-1003, ¶73.

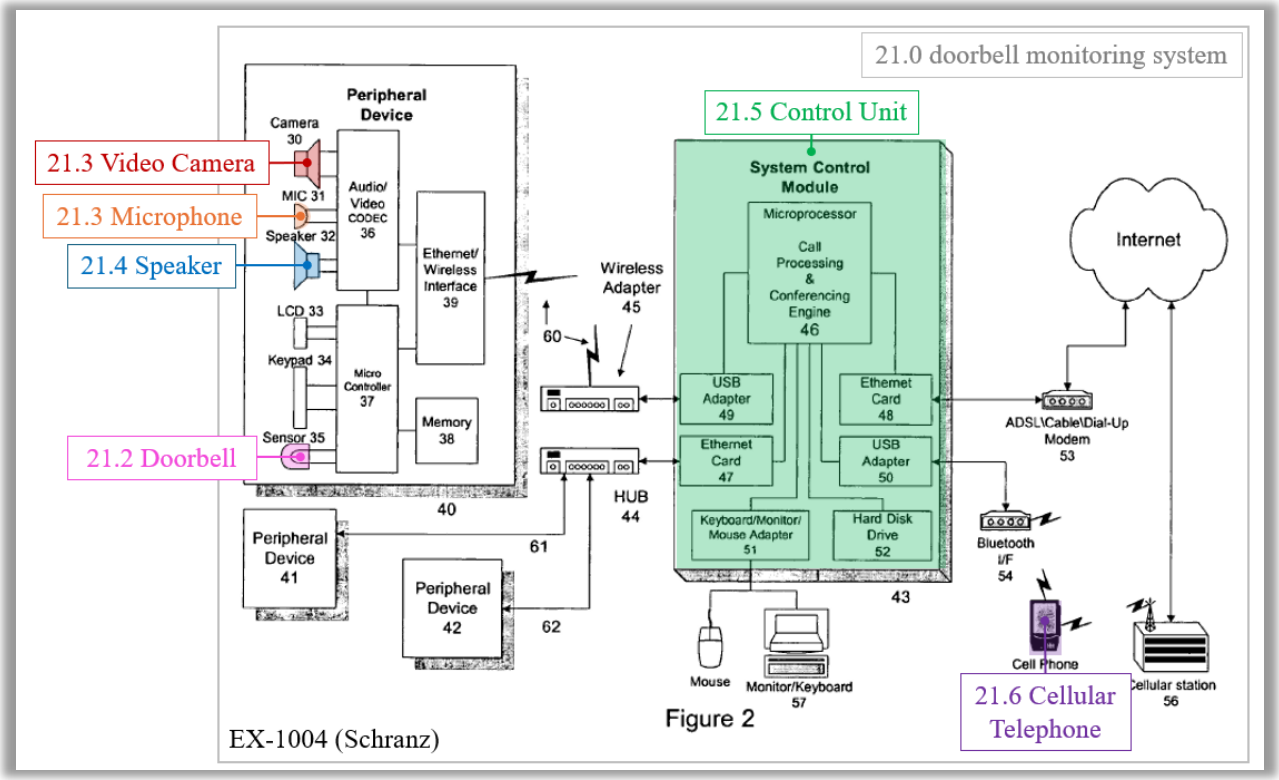
Further, Schranz explains that CODEC 36 "digitizes the analog video signal" from camera 30 and "codes the analog audio signal" from microphone 31 to provide the data to the system control module via wireless or wired channel. EX-1004, ¶48. Upon event detection (*i.e.*, the ringing of the doorbell), the system control module then establishes a VoIP communication call to transmit voice and video information from the peripheral devices (*i.e.,* camera 30 and microphone 31) to the system control module and from the system control module to the remote user. EX-1004, Claim 1. Accordingly, Schranz system control module 43 is *for communicating at least one portion of the visual and audio communications received from the video camera and the external microphone*. EX-1003, ¶74.

Finally, Schranz discloses that the remote user can enable audio to be sent from their location and device to the peripheral devices (*i.e.,* speaker 32). EX-1004, ¶65 ("The remote user can enable audio to be sent from his location to the peripheral device currently sourcing the ambient audio."). In this case, the system control module establishes an audio call with the remote user and provides the data to CODEC 36 which "decodes PCM samples into an analog audio signal to the speaker." EX-1004, ¶¶48, 63. Accordingly, Schranz system control module 43 is *for communicating the received audio communications to the external speaker. EX-1003, ¶75.*

[21.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular

audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit;

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system provides notification of an alarm event to a remote user via the remote user's "***cell phone*** 150, a laptop computer 155, a VoIP phone 160…" EX-1004, ¶62. In refence to Figure 2, Schranz explains that the SCM is connected to the internet via Ethernet Card 48 and ADSL or cable modem 54. Further, Schranz explains that "the cellphone 55 communicates with a cellular station 56" to connect to the internet. EX-1004, ¶49. A POSITA understood that the remote user's cell phone is disposed remotely to the doorway and control unit as shown below in Figure 2. EX-1003, ¶76.



EX-1004, Figure 2 (Annotated) ; EX-1003, ¶76.

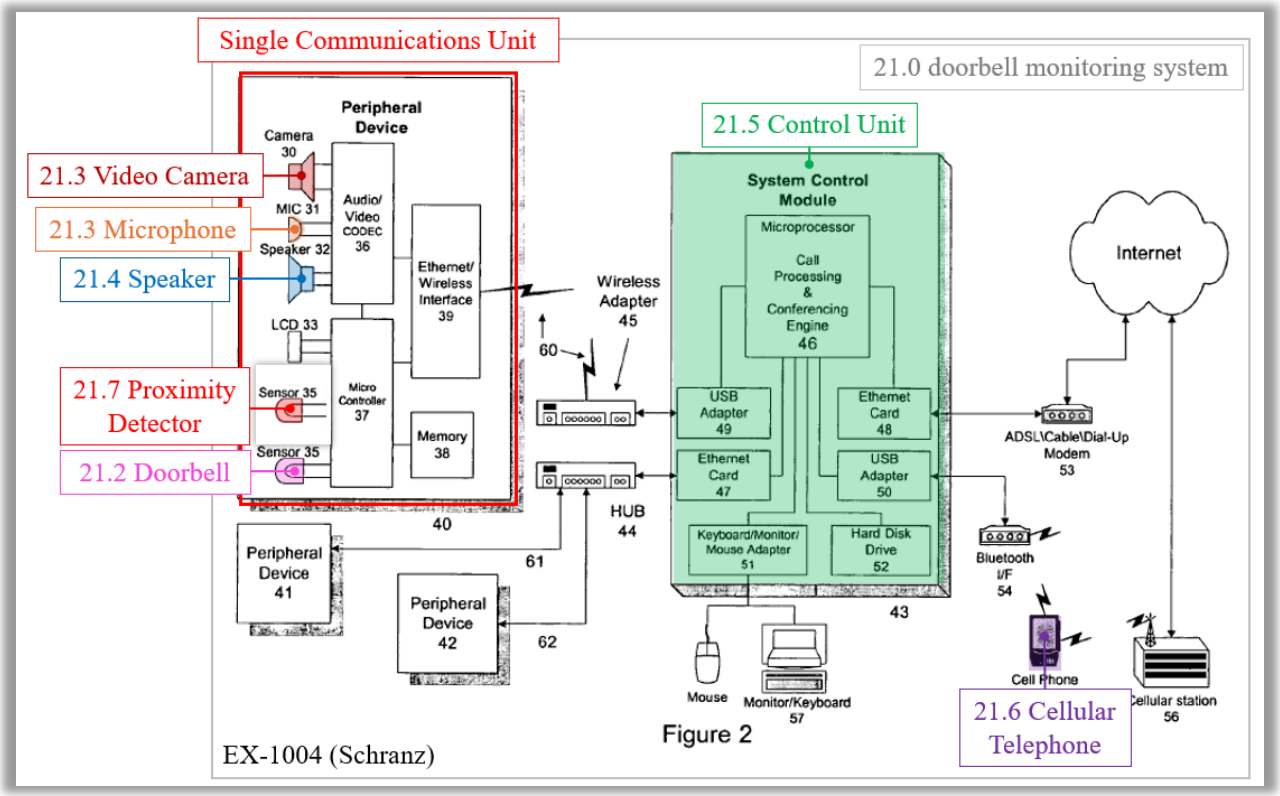
Upon an alarm event, Schranz's system control module establishes a VoIP communication call to transmit voice and video information from the peripheral devices (*i.e.,* camera 30 and microphone 31) to the system control module and from the system control module to the remote user. EX-1004 ¶24, Claim 1. The system control module "knows beforehand which device to contact (work phone, ***cell***, laptop) and what method of message to send (text, voice, ***video***, email)." EX-1004, ¶63 (emphasis added). In other words, the system control module may contact the remote users cell phone with an audio or video message from the alarm

event thereby *rendering the at least one portion of entry point visual and audio communications received from the control unit*. EX-1003, ¶77.

Once the audio call is established, the remote user can "enable audio to be sent from his location to the peripheral device currently sourcing the ambient audio." EX-1004, ¶¶64-65. A POSITA understood that remote user's cellphone disclosed by Schranz is therefore *for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit. EX-1003, ¶78.*

[21.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [*single communications unit*] including sensor 35 (pink) [*doorbell; proximity detector*], camera 30 (red) [*video camera*], microphone 31 (orange) [*external microphone*], and speaker 32 (blue) [*external speaker*]. EX-1004, ¶48. Schranz discloses that sensor 35 "may be different types, such as a ***motion detector***, infrared radiation sensor or ***doorbell signal***." EX-1004, ¶48 (emphasis added). A POSITA would recognize that Schranz's system could easily include both a motion detector (*proximity detector*) and a doorbell signal within peripheral device 40. Schranz therefore discloses a *doorbell*, *video camera, external microphone, external speaker, and a proximity detector*. EX-1003, ¶79.



EX-1004, Figure 2 (modified) ; EX-1003, ¶79.

To the extent Patent Owner asserts that Schranz does not expressly describe a peripheral device with a doorbell and a proximity sensor, it would have been obvious to include both a motion detector (*proximity detector*) and a doorbell signal within peripheral device 40. A POSITA would be motivated by the teachings of Schranz to include both a doorbell and motion detector in a peripheral device at the entrance to a building in order to achieve the express benefits of Schranz, which are to both monitor visitors and track intruders. EX-1004, ¶¶29-30, 58-60. First, as explained above, Schranz expressly teaches that its sensor 35 "may be different types," including both a "motion detector" and a "doorbell

signal," thereby contemplating that peripheral devices may be configured with varying sensor functionality to suit particular security needs. EX-1004, ¶48. Second, Schranz discloses that the system is designed to be installed at the entrance of a building for the purpose of tracking intruders and monitoring visitors. EX-1004, ¶¶29-30, 58-60. A POSITA reading Schranz would thus understand that combining both a doorbell and a motion detector within a single peripheral device 40 would directly advance these objectives: the doorbell enabling communication with expected visitors and the motion detector enabling detection of unexpected intruders. A POSITA would recognize that this modification would provide complementary functionality that serves the purposes of Schranz's system and could be achieved with a reasonable expectation of success. EX-1003, ¶80.

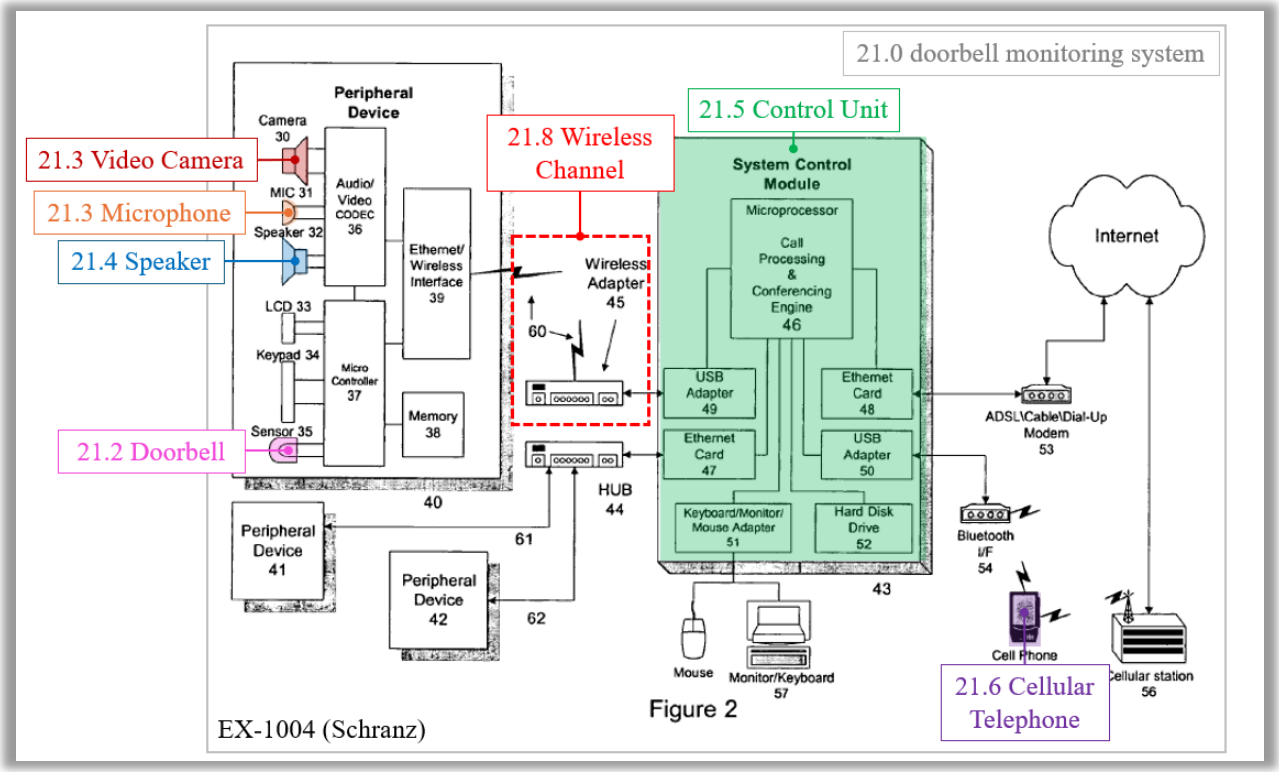
80[21.8] wherein the entry point visual and audio communications are wirelessly streamed to the control unit;

Schranz discloses this limitation. Schranz discloses peripheral devices 40 that include camera 30 (red) [*video camera*] and microphone 31 (orange) [*external microphone*]. EX-1004, ¶48. Camera 30 and microphone 31 transmit analog information to a CODEC 36 which, then, digitizes the information and provides digital data to the system control module 43 (green) [*control unit*]. EX-1004, ¶48. Schranz states that the set of peripheral devices provide digital data to the system control module via a wired or wireless channel [*wirelessly streamed to the control unit*]. EX-1003, ¶81.

> The peripheral device 40 connects to the SCM 43 via an Ethernet or wireless interface 39. The channel between the peripheral devices 40, 41 or 42 and the SCM 43 may be a wireless channel 60 or wireline channel 61 or 62.

EX-1004, ¶48; EX-1003, ¶81.

As shown below in Figure 2, Schranz discloses wireless interface 39 connected to the peripheral device 40, a wireless channel 60, and a wireless transceiver at the system control module 43 to provide bidirectional communication between the peripheral device 40 and the system control module 50. EX-1004, ¶48. Therefore, Schranz's system discloses that *the entry point visual and audio communications are wirelessly streamed to the control unit*. EX-1003, ¶82.

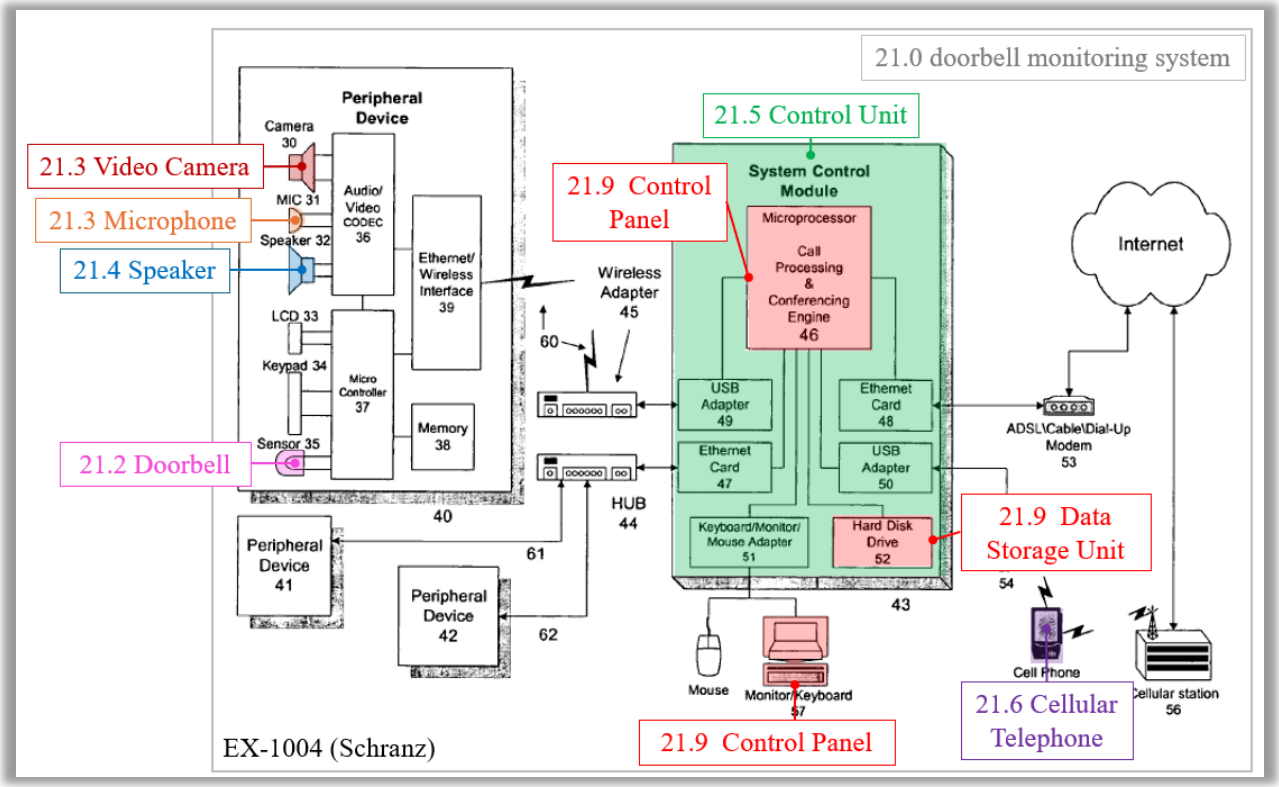


EX-1004, Figure 2 (annotated) ; EX-1003, ¶82.

> ***[21.9] wherein the control unit is configured to store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit wherein a control panel is configured to allow an individual to manage a security system;***

Schranz discloses this limitation. Schranz's system control module (green) [*control unit*] is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system." EX-1004, ¶49. The system control module includes a hard disk drive 52 [*data storage unit*] "to record audio and video data from the peripheral devices during an alarm situation using standard formats." EX-1004, ¶49. Therefore, Schranz discloses a system where the control unit *is configured to*

store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit. EX-1003, ¶82.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶83.

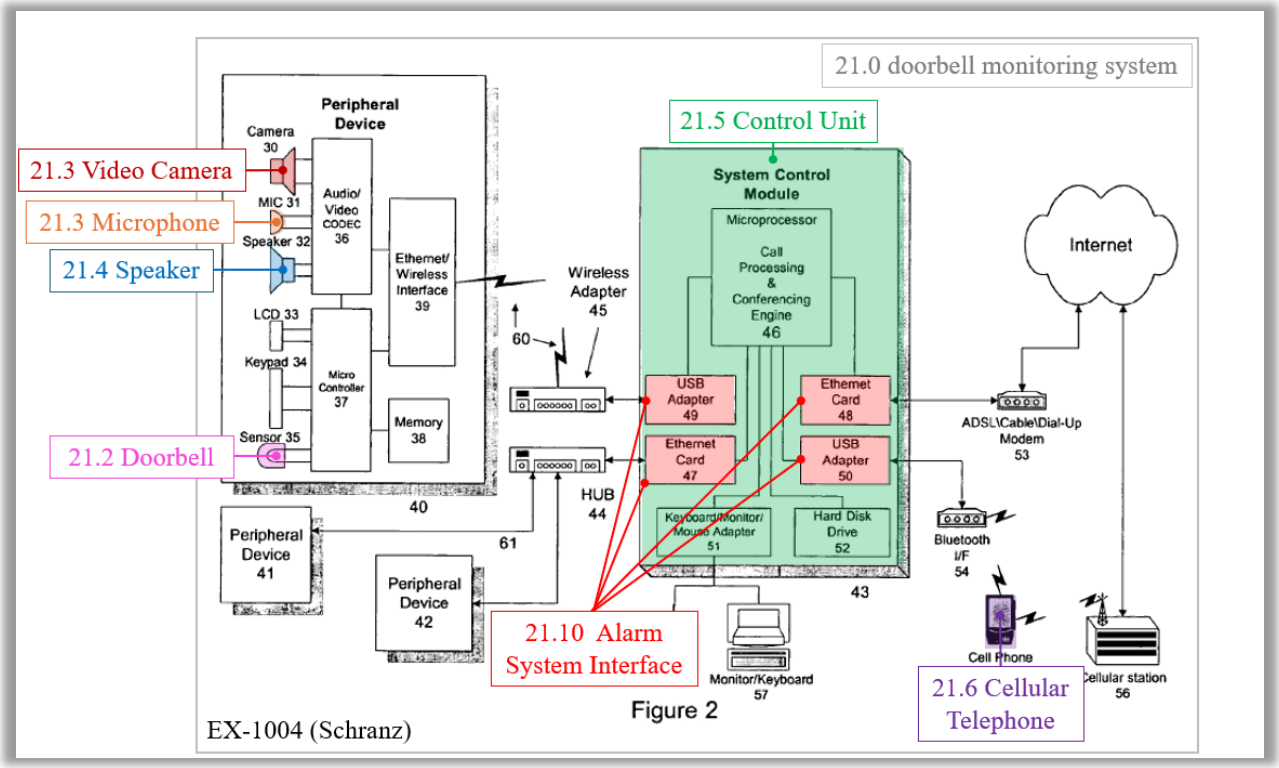
Further, Schranz's system control module 43 [*control unit*] runs a user software application on the operating system which monitors and controls the peripheral devices, event detection, and VoIP call processing. EX-1004, ¶50. The user software application includes a web server and web application that the user can access remotely to "control all aspects of the system." EX-1004, ¶50. Additionally, and as shown above, the system control module 43 includes a keyboard, mouse and monitor 57 "to set up the configurable parameters of the

system." EX-1004, ¶49, ¶56. Schranz explains that keyboard and monitor 57 can be used to define "access codes, the VoIP addresses (URLs) to call during alarm, pre-recorded messages and zone definitions" for the VoIP security monitoring and alarm system. EX-1004, ¶56. The user software application, web server, web application, keyboard, and monitor are collectively a *control panel* that is *configured to allow an individual to manage a security system*. EX-1003, ¶84.

[21.10] wherein an alarm system interface of the control panel is configured to interface with the security system;

Schranz discloses this limitation. As explained above with respect to limitation [21.9] which is incorporated herein, Schranz's system control module 43 [*control unit*] runs a user software application with a web server, web application, keyboard and monitor [collectively the *control panel*]. EX-1004, ¶¶49-50. The system control module 43 includes "10/100BaseT Ethernet cards 47 & 48, two USB ports 49 & 50" [*alarm system interface*]. EX-1004, ¶49. As shown below, Ethernet card 47 and USB adapter 46 are connected to wireless channel 60 and wireline channel 62 which are in turn connected to peripheral devices 40, 41, and 42. Schranz explains that the ethernet card 47 and USB adapter 46 in the SCM allow the SCM to send control packets to and receive status packets from the peripheral devices. EX-1004, ¶48. Likewise, Schranz explains that Ethernet card 48 connects the SCM to modem 53 in order to provide a connection to the internet, and USB adaptor 50 may be used to connect to a Bluetooth enabled cell phone.

EX-1004, ¶49. Schranz further discloses that the packets indicate an alarm detection that is then used by the SCM to locate and connect with the notified agent as quickly as possible using VoIP address resolution and VoIP presence protocols. EX-1004 ¶¶24, 25, 47. Therefore, ethernet card 47 and USB adapter 46 are that *is configured to interface with the security system*. EX-1003, ¶85.

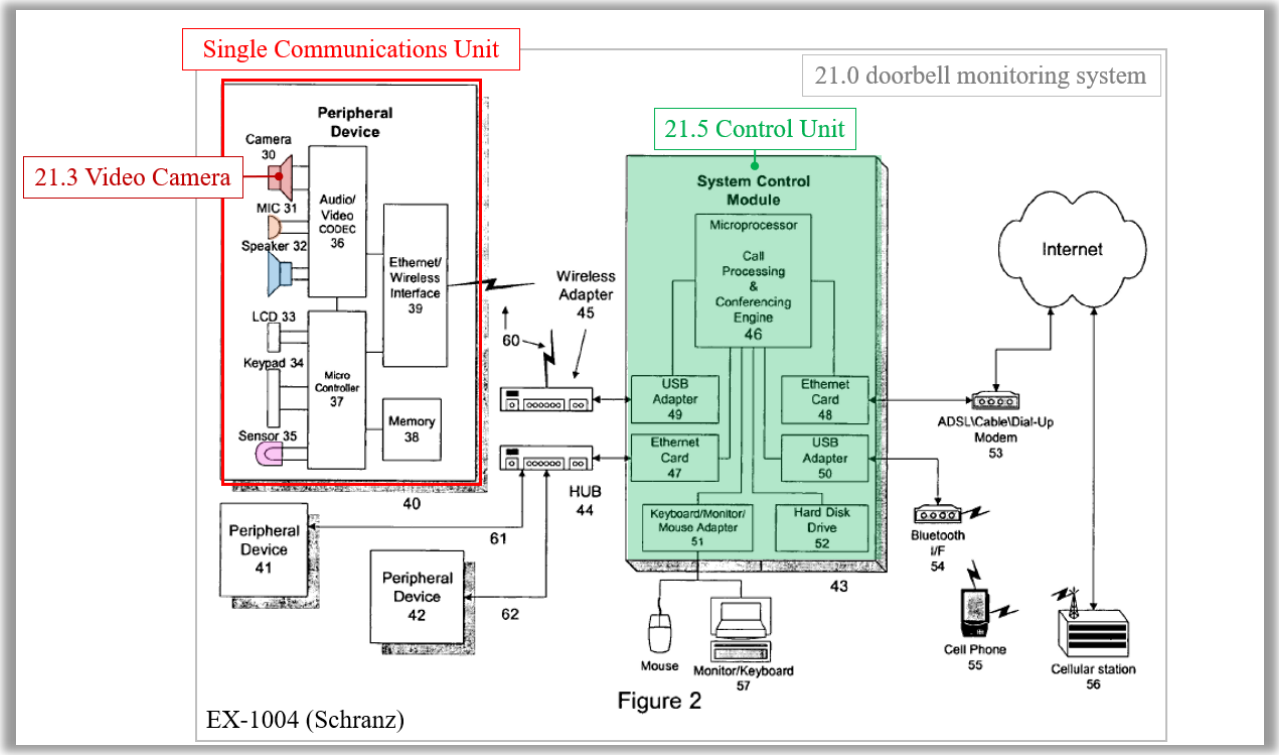


EX-1004, Figure 2 (annotated) ; EX-1003, ¶85.

[21.11] wherein the video camera is configured to collect the entry point visual communications captured by the single communications unit before the triggering event;

Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [*single communications unit*] including a black

and white or color "CCTV board camera," camera 30 [*video camera*]. The peripheral device 40 [*single communications unit*] may be "located at the main entrance to the premises." EX-1004, ¶47; EX-1003, ¶86.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶86.

A POSITA understood that a CCTV is a "closed circuit" camera that typically records footage continuously, and in many cases records over previous footage periodically in a loop to save storage space. This was a known feature of security cameras as demonstrated in the State-of-the-Art section. *See* §IV.F. Specifically, it was well known to capture and record video continuously in memory, and then based on predefined criteria, discard older video. EX-1008, ¶81. Thus, a POSITA would have understood that Schranz's CCTV would include the

well-known feature of capturing visual communications *before the triggering event.* Schranz's disclosure is consistent with the '191 Patent which itself lacks any detail regarding how its camera captures video before the triggering event, further demonstrating that this feature was well-known and would have been understood by a POSITA without explicit instruction. EX-1003, ¶87.

To the extent that Patent Owner argues that Schranz does not expressly disclose that its camera collects video before a triggering event, a POSITA would be motivated to modify Schranz to incorporate such a feature and would have had a reasonable expectation of success in doing so. First, as discussed in the State-of-the-Art section, it was well-known and common at the time of the alleged invention to capture audio and video in a revolving buffer before saving to more permanent storage based on a triggering event. EX-1008, ¶81 ("video module 620 may buffer video from video cameras 112 in memory.") A revolving buffer was commonly implemented by allowing the user to define the amount of time to retain data from before and after the triggering event. EX-1007, ¶¶43, 81 ("Then, based on predefined criteria, older video that is not considered essential to any alarm signals may be discarded.") The purpose of this well-known technique was to allow for the observer to see and capture data from before, during, and after triggering events (pushing of the doorbell button). EX-1003, ¶88.

Schranz contemplates this type of user-driven configurability, and specifically discloses that the user sets up system control parameters. EX-1004, ¶¶56, 57. Accordingly, a POSITA would have found it obvious to collect video and audio data before the ringing of the doorbell by continuously storing the captured audio and video in a buffer such that context proximate to the triggering event may be collected. Such a modification would have amounted to nothing more than the application of a known technique, revolving buffer storage triggered by a defined event, to improve a similar device in the same, predictable way. EX-1003, ¶89.

Second, a POSITA would be motivated to add such a feature because it provides the additional known benefit of helping identify false alarms as discussed in the State-of-the-Art section. EX-1008, ¶38. A POSITA would have recognized that providing the ability to monitor surroundings even when a triggering event does not occur by using video surveillance was a common capability known as remote surveillance or "lifestyle video," as discussed in the State of the Art. EX-1008, ¶¶43, 82. With lifestyle video, the observer can view the environment and manually verify triggering events thereby enhancing the accuracy of the security system. EX-1003, ¶90. Thus, A POSITA would have been motivated to include "lifestyle video" to limit the number of false alarms and enhance the accuracy of the security system. Moreover, implementing this modification would have been straightforward because it could be accomplished using the existing equipment

already disclosed in Schranz, and hardware storage could be easily expanded if archiving of the video were desired. A POSITA would have had a reasonable expectation of success in making this combination given the well-known nature of continuous video recording in CCTV systems. EX-1003, ¶90.

[21.12] wherein the video camera is configured to collect additional visual communications after the triggering event;

Schranz discloses this limitation. Schranz discloses once a peripheral device detects an event (*e.g.,* the ringing of the doorbell), it notifies the SCM, which then initiates a VoIP call to a remote agent using a pre-programmed VoIP uniform resource locator (URL). This VoIP call can reach a user in the IP network using an IP enabled communication device such as a VoIP phone or multimedia computer, or by going through a gateway it can terminate on a traditional POTS or cellular phone. The SCM then routes the audio and/or video data from the peripheral device to the remote agent as well as storing the data in real-time using standard audio and video formats." EX-1004, ¶¶24, 32. Schranz further explains that the system provides real-time intruder tracking by monitoring the current location of the intruder using the advanced peripheral devices and motion sensors. The notified agent is kept up to date with the current location by periodic announcements from the SCM. EX-1004 ¶29. A POSITA understood that to track an intruder and update the remote users, the peripheral devices, including the camera would continue to capture video data after detecting an event [*configured*

to collect additional visual communications after the triggering event]. EX-1003, ¶91.

[21.13] wherein the doorbell monitoring system is configured to establish communication with the control unit upon activation of the doorbell;

Schranz discloses this limitation. Schranz's VoIP security monitoring system utilizes peripheral devices including a "doorbell signal" to notify the system control module [*control unit*] upon event detection. EX-1004, ¶47, 48. Specifically, Schranz states that "once a peripheral device detects an event it notifies the SCM." EX-1004, ¶24. As explained above in [21.1] and [21.3] and incorporated herein, in both normal or armed mode, the peripheral devices monitor the environment and notify the SCM when an event takes place. EX-1004, ¶¶59-60. Therefore, Schranz's system *is configured to establish communication with the control unit upon activation of the doorbell*. EX-1003, ¶92.

[21.14] wherein at least a portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone; and

Schranz discloses this limitation. Schranz states that during an alarm, such as when a doorbell signal is received, the system sends "some form of VoIP notification" to the remote user's "cell phone 150." EX-1004, ¶¶60-62. In addition, Schranz discloses that the remote person can be notified of the event by the Instant Messaging feature of the Session Initiation Protocol [*wherein at least a*

portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone]. EX-1004, Claim 6. Further, Schranz states that during an alarm "the SCM knows beforehand which device to contact (work phone, cell, laptop) and what method of message to send (text, voice, video, email)." EX-1004, ¶63. The system control module therefore provides *notification sent to the cellular telephone*. EX-1003, ¶93.

[21.15] wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

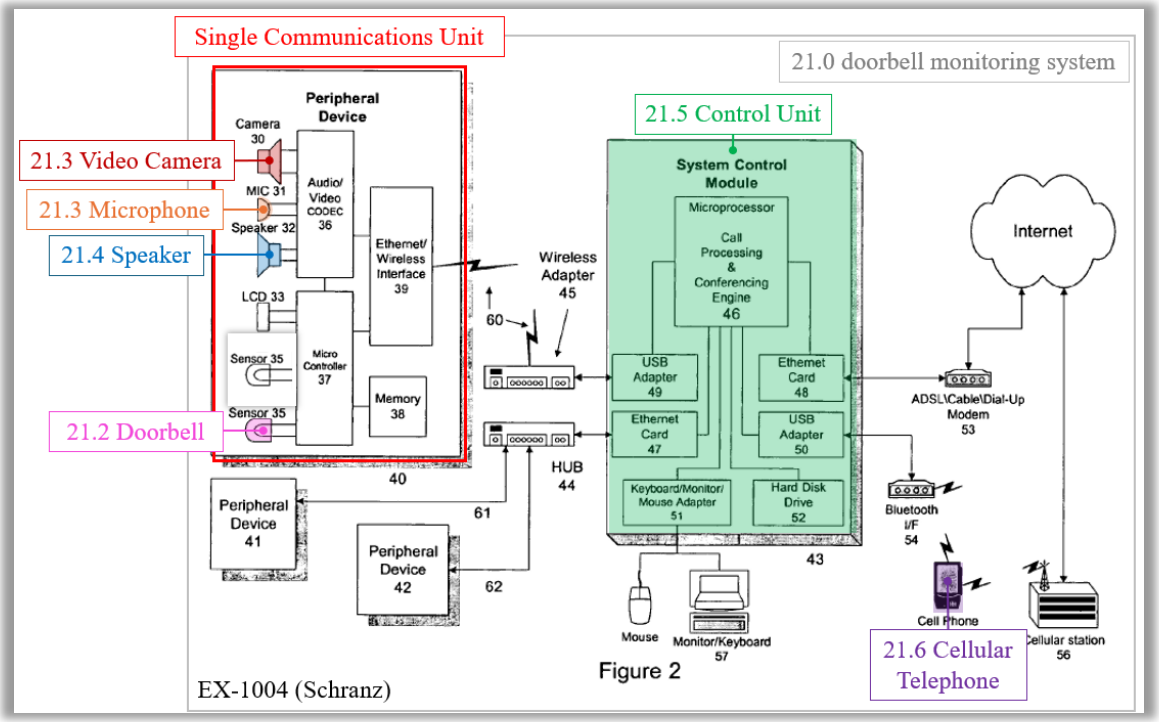
Schranz discloses this limitation. Schranz discloses that system configuration on initial setup requires the user to set "items such as ***access codes***, the VoIP addresses (URLs) to call during alarm, pre-recorded messages and zone definitions." EX-1004, ¶56. Likewise, Schranz discloses that, after system configuration, the user can access the "secure portal" or user web application to control all aspects of the system . EX-1004, ¶¶50, 56. A POSITA understood that a "secure portal" and "access codes" are inherently *configured to authenticate a user of the doorbell monitoring system.* EX-1003, ¶94.

Claim 22

[22] The doorbell monitoring system of claim 21, wherein the single communications unit is configured to stream at least a portion of the captured visual and audio communications.

Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [*single communications unit*] with a camera 30

(red) microphone 31 (orange) connected to system control module 43 (green). EX-1004, ¶48. Schranz explains that CODEC 36 "digitizes the analog video signal" from camera 30 and "codes the analog audio signal" from microphone 31 to provide the data to the system control module via wireless or wired channel. EX-1004, ¶48. The system control module "routes the audio and/or video data from the peripheral device to the remote agent." EX-1004, ¶24. Therefore, Schranz discloses *the single communications unit configured to stream at least a portion of the captured visual and audio communications.* EX-1003, ¶95.



EX-1004, Figure 2 (annotated; EX-1003, ¶95).

Claim 23

[23] The doorbell monitoring system of claim 21, wherein the single communications unit is configured to capture additional video from the video camera after the triggering event.

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12]. EX-1003, ¶96.

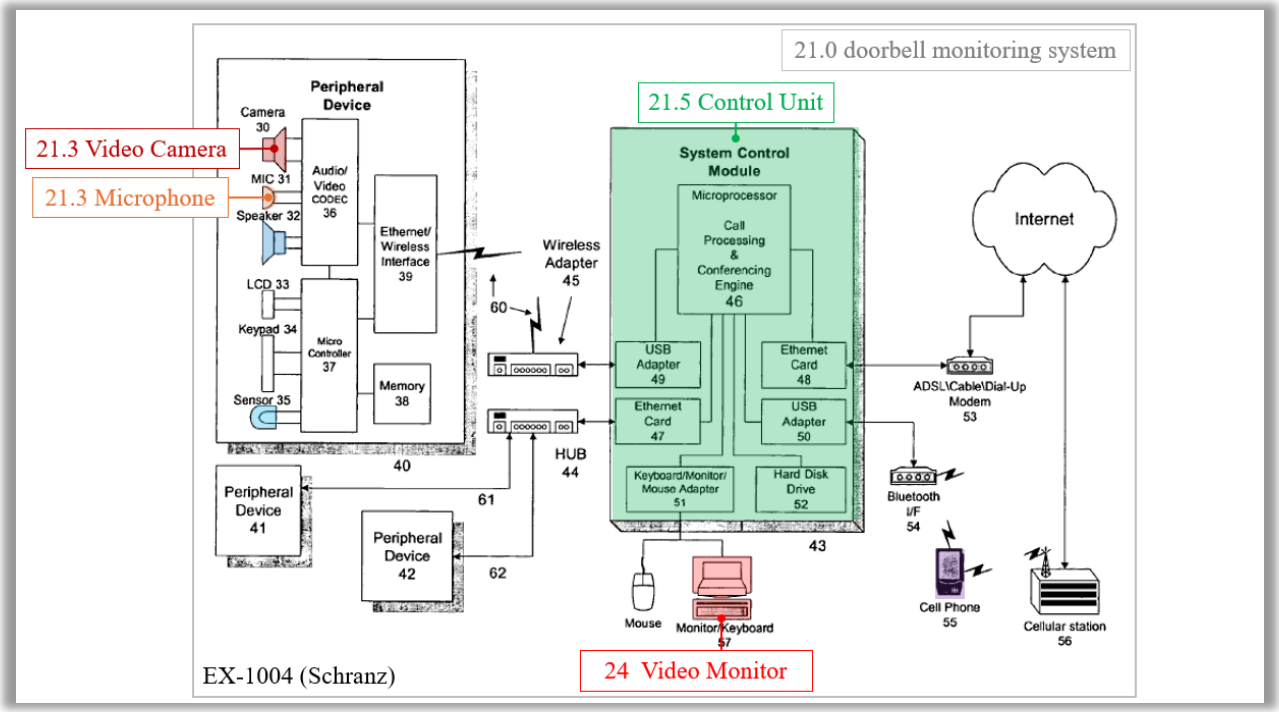
Claim 24

[24] The doorbell monitoring system of claim 21, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor.

Schranz discloses this limitation. Schranz's discloses a system control module 43 (green) [*control unit*] that is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system" and typically is an "off the shelf computer." EX-1004, ¶49. As shown below, the system control module 43 or off the shelf computer includes a keyboard, mouse and monitor 57 (red) [*video monitor*] "to set up the configurable parameters of the system." EX-1004, ¶¶49, 56. Further, the system control module runs a web server and website where "[t]he user can visually see the current configuration and the status of all peripheral devices." EX-1004, ¶50. As shown below, the system control module 43 is in communication with a set of peripheral devices, including camera 30 (red) [*video camera*] and microphone 31 (orange) [*external microphone*]. EX-1004, ¶48. The system control module 43 receives audio and video communication from camera 30 and microphone 31 via CODEC 36 which "digitizes the analog video signal into

a standard digital format, codes the analog audio signal from the microphone into PCM samples." EX-1004, ¶48. Therefore, the user can see the audio and visual data from camera 30 and microphone 31 through the webserver and website on the system control module 43. EX-1003, ¶97.

Schranz further explains that the user can access the website to see the audio and video data from "any Internet browser that supports the https protocol." EX-1004, ¶50. As discussed above, the system control module 43 is typically an off the shelf computer and therefore has an internet browser that supports the https protocol. EX-1004, ¶49. A user can thereby access the website to see the audio and video data on the system control module 43 itself through a keyboard, mouse and monitor 57. Therefore, Schranz's system control module 43 [*control unit*] is *configured to display the entry point visual and audio communications on the video monitor. EX-1003, ¶98.*



EX-1004, Figure 2 (annotated) ; EX-1003, ¶98.

Claim 25

[25] The doorbell monitoring system of claim 24, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime.

Schranz discloses this limitation. As explained above with respect to Claim [24] and incorporated herein, Schranz systems operates as follows: (1) Camera 30 and microphone 31 capture audio and visual information from the entry point (EX-1004, ¶48); (2) CODEC 36 digitizes the audio and video data and transmits the digital data to the system control module via wireless channel 60 (EX-1004, ¶48); (3) The system control module 43 website or "graphical monitor and control

program" displays the audio and video data to allow the user to "visually see the current configuration and the status of all peripheral devices" (EX-1004, ¶50). Furthermore, Schranz's system allows the user to access the "graphical monitor and control program" through "any Internet browser" such as by using the system control module and monitor 57 [*video monitor*]. EX-1004, ¶48. Moreover, Schranz contemplates the bandwidth requirements of real-time bidirectional transmission of audio and video data and explains the "preferred method to connect [the SCM] to the Internet is by ADSL or Cable modem since their bandwidth capabilities are the best." EX-1004, ¶49. Schranz explains that "Dial-Up modems may be used for audio only applications." EX-1004, ¶49. A POSITA understood that Schranz discloses communications protocols that allow for real-time bidirectional transmission of audio and video data including Voice over Internet Protocol data information, used to deliver voice and/or video information between the peripheral devices, the computing platform including the video monitor and the remote person's device using Real-Time Transport Protocol (RTP) or Session Initiation Protocol (SIP) [*visual and audio communications on the video monitor in substantially realtime*]. EX-1004, Claims 2-4; EX-1003, ¶99.

Claim 26

[26] The doorbell monitoring system of claim 21, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime; and wherein the doorbell monitoring system is

configured to authenticate a user of the doorbell monitoring system.

Schranz discloses this limitation for the same reason as discussed with respect to limitations [25] and [21.15]. EX-1003, ¶100.

Claim 27

[27] The doorbell monitoring system of claim 21, wherein the control unit is configured to generate a file that includes at least a portion of the entry point visual and audio communications captured by the single communications unit.

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system includes system control module 43 [*control unit*] with a hard disk drive 52 that is "used to record audio and video data from the peripheral devices during an alarm situation using standard formats." EX-1004, ¶50. The audio and video data are sourced from camera 30 and microphone 31 contained within peripheral device 40 [*single communications unit*]. EX-1004, ¶48. A POSITA understood that the "standard formats" contemplated by Schranz include a file that contains a portion of the audio and video captured at by the single communications unit. For example, A POSITA would have understood that, at the time of the invention, common standard formats include MP4 files which store both audio and video data. EX-1003, ¶101. Therefore, Schranz discloses a *control unit configured to generate a file that includes at least a portion of the entry point*

visual and audio communications captured by the single communications unit.

EX-1003, ¶101.

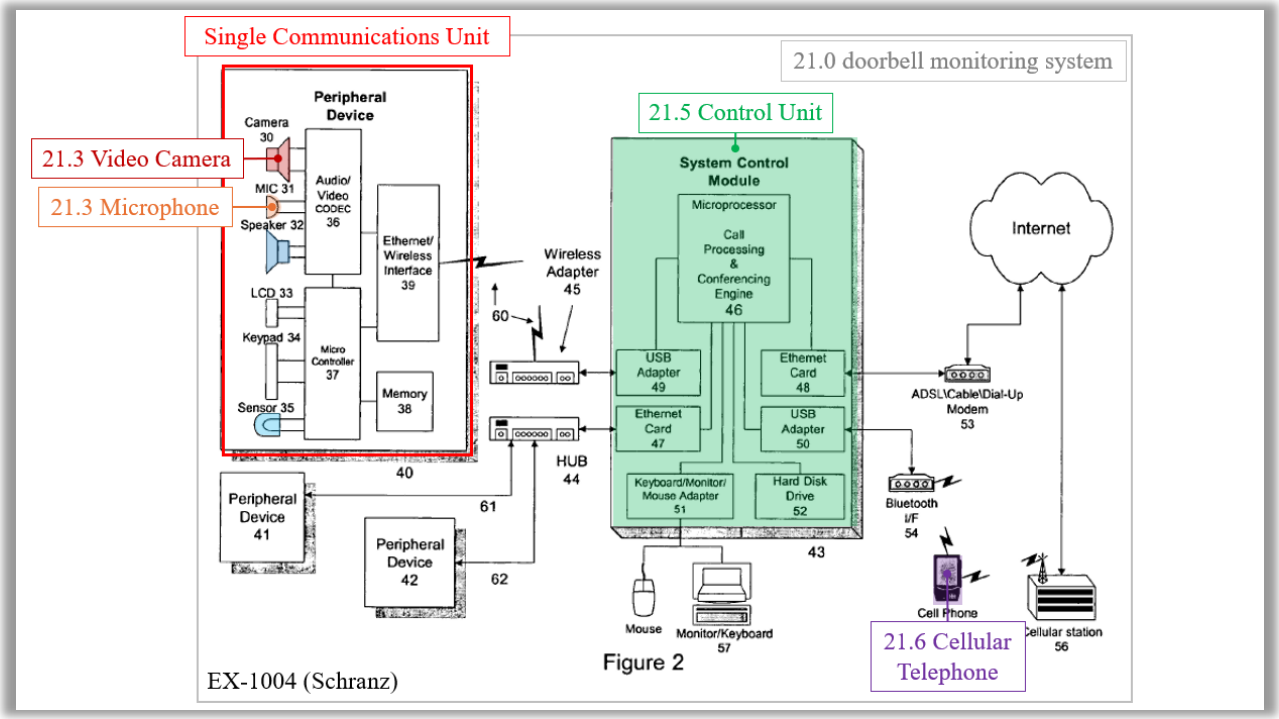
Claim 28

[28] The doorbell monitoring system of claim 21, wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit.

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system utilizes peripheral devices to detect an event and a system control module to establish a VoIP call to a remote user via cellular networks. EX-1004, Abstract. The remote user will "will hear ambient audio and see video images from the peripheral device in the location of the alarm." The remote user can then issue "DTMF commands to the SCM to control the audio, initiate conference calls and other functions" [*wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit*]. EX-1004, Abstract; EX-1003, ¶102.

Specifically with respect to Figure 2 (below), Schranz's system includes camera 30 and microphone 31 disposed within peripheral device 41 [*single communications unit*] to capture audio and video data at "the main entrance to the premise." EX-1004, ¶48. Once peripheral device 41 detects an event, the device

notifies the system control module 43 which initiates a VoIP notification to a remote agent. EX-1004, ¶24, 60, 62. The VoIP notification may be sent to the remote user's cell phone 150 [*cellular telephone*], laptop computer 155, or multimedia computer 170. EX-1004, ¶62. The remote user can then send "a text message commanding the SCM to make an ***audio and video call*** to the same device." EX-1004, ¶63 (emphasis added). When the audio and video call is established, the remote user will hear the audio from microphone 31 and video from camera 30 at the location of the alarm. EX-1004, ¶¶64, 24, Abstract. The user can then "issue commands to the SCM" using the cell phone's keypad [*user interface*] to issue DTMF commands. EX-1004, ¶64. The remote user can issue a variety of commands including "increase and decrease the volume of the audio path," "play an announcement over the speaker," and "initiate a conference call to a third-party." EX-1004, ¶¶65-66. Therefore, Schranz discloses a *cellular telephone* with a *user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit. EX-1003, ¶103.*



EX-1004, Figure 2 (annotated) ; EX-1003, ¶103.

Claim 29

[29] The doorbell monitoring system of claim 28, wherein the two or more actions are at least one of (1) play a pre-recorded greeting, (2) request additional video and/or audio communications, (3) institute two-way video communications between the user and the person at the entry point, (4) notify an alarm company, or (5) selection of no action.

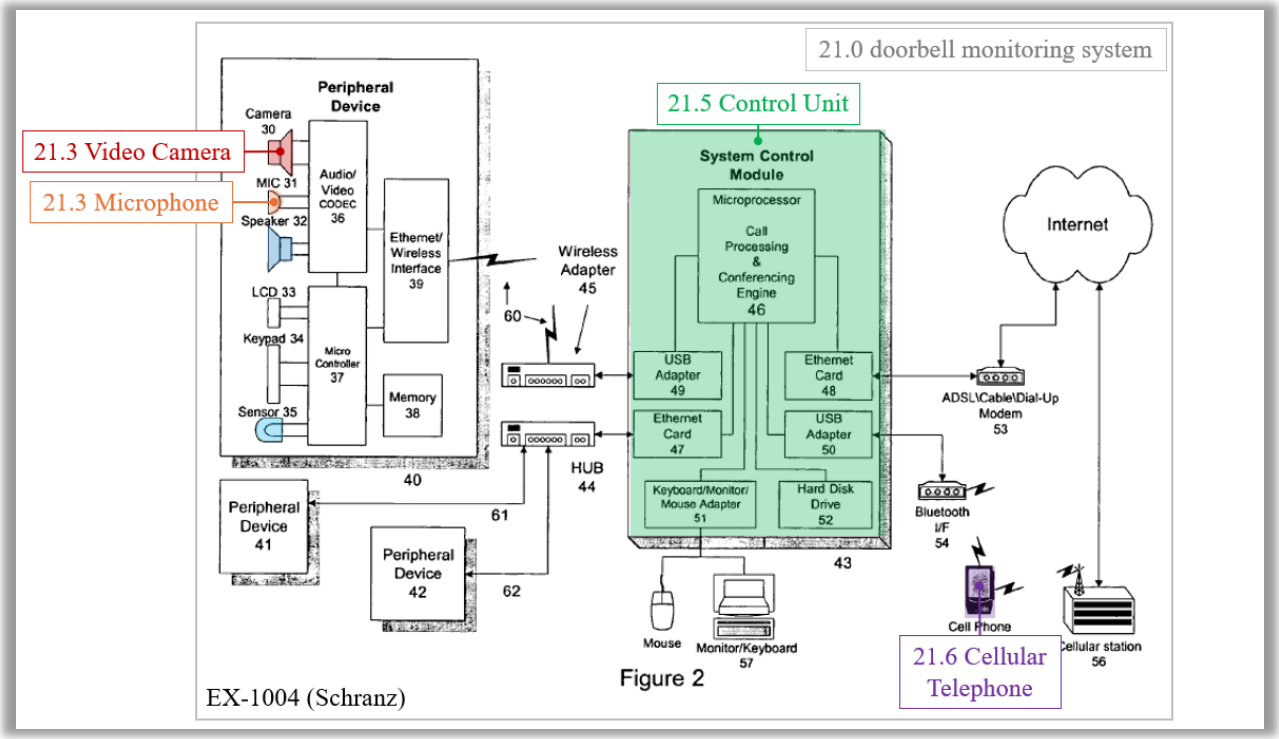
Schranz discloses this limitation. As explained with respect to Claim [28], upon event detection, Schranz's system control module 43 establishes a VoIP audio and video call between the peripheral device (*i.e.*, peripheral device 40) and the remote user's cell phone (*i.e.*, cell phone 150). EX-1004, Abstract, ¶60, ¶62. During the call, the remote user can use the keypad on the cellphone to send

DTMF tones which tell the system control module to perform a specific action. EX-1004, ¶64. Schranz explains that "[s]everal commands are available to the user, some of which are described." EX-1004, ¶64; EX-1003, ¶104.

First, Schranz expressly discloses that the user "can direct the SCM to play an announcement over the speaker" [*(1) play a pre-recorded greeting*]. EX-1004, ¶65. Schranz explains that during initial system configuration the user can set-up configurable parameters including a "pre-recorded message." EX-1004, ¶56. A POSITA understood that Schranz's system allows the announcement requested by the remote user to be one of the pre-recorded messages set-up during initial system configuration. Therefore, Schranz discloses that one of the actions requested by the remote user may be to (*1) play a pre-recorded greeting*. EX-1003, ¶105.

Second, Schranz expressly discloses that the user can "command a call transfer to a particular peripheral device" [*(2) request additional video and/or audio communications*]. EX-1004, ¶31. As shown in Figure 2, Schranz's system control module 43 is connected to multiple peripheral devices including device 40, 41, and 42. In one instance, the user may be receiving audio and video information from peripheral device 40 over the VoIP call. The user may then request a transfer to peripheral device 41 to receive additional video and or audio communications from the scene. In another instance, when receiving audio and video information from peripheral device 40 over the VoIP call, Schranz discloses that the user can

request additional information from the SCM "by querying the SCM using DTMF commands." EX-1004, ¶29. Therefore, Schranz discloses that one of the actions requested by the remote user may be to *(2) request additional video and/or audio communications*. EX-1003, ¶106.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶106.

Third, Schranz discloses that once peripheral device 41 detects an event, the device notifies the system control module 43 which initiates a VoIP notification to a remote agent. EX-1004, ¶24, 60, 62. The VoIP notification may be sent to the remote user's cell phone 150 and the remote user can then send "a text message commanding the SCM to make an ***audio and video call*** to the same device." EX-1004, ¶62, 63 (emphasis added). When the audio and video call is established, the

remote user will hear the audio from microphone 31 and video from camera 30 at the location of the event [*(3) institute two-way video communications between the user and the person at the entry point*]. EX-1004, ¶64, ¶24, Abstract. Further, Schranz discloses a VoIP communication call such that "voice and/or video information is exchanged between the said peripheral device… and the remote person" [*(3) institute two-way video communications between the user and the person at the entry point*]. EX-1004, Claim 1; EX-1003, ¶107.

Fourth, Schranz discloses that the remote user "can initiate a conference call to a third-party, such as his neighbor or the police." EX-1004, ¶66. Schranz identification of "the police" as an exemplary third party demonstrates that the system was designed to facilitate emergency security communications in response to a detected event. A POSITA would have understood that *an alarm company* is similarly a third-party resource for emergency security communications in response to a detected event. Indeed, contacting an alarm company in response to a security event was a well-known and routine practice in the home security field at the time of the alleged invention, and Schranz's open-ended reference to "a third-party" plainly encompasses such a contact. EX-1003, ¶108. A POSITA would have found it obvious to modify Schranz's system to include the ability to initiate a conference call to an alarm company, as doing so merely applies Schranz's own disclosed functionality, initiating a conference call with the police, to an additional,

predictable recipient, *an alarm company*. Such a modification would have required no change to the underlying architecture of Schranz's system and would have yielded nothing more than the predictable result of expanding the set of third parties available for a conference call to include an alarm company. Therefore, Schranz discloses that one of the actions requested by the remote user may be to *(4) notify an alarm company*. EX-1003, ¶108.

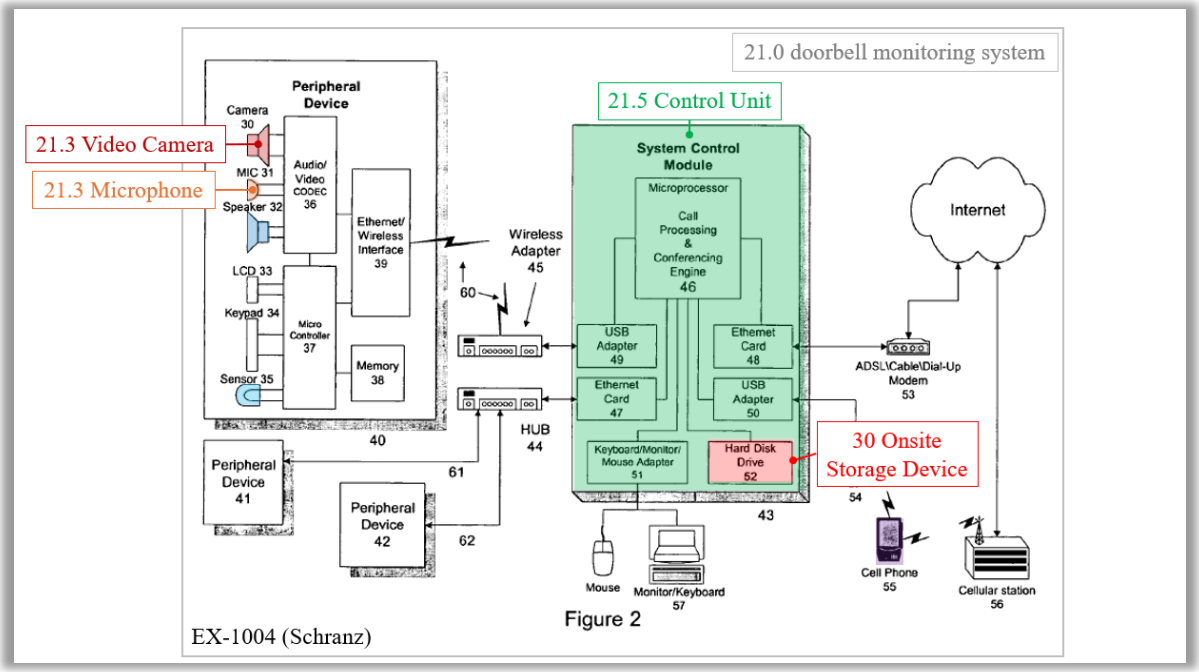
Finally, Schranz discloses the remote user may elect to send DTMF commands to the system control module, and includes the user electing not to send a DTMF a command [*(5) selection of no action*]. EX-1003, ¶109.

Claim 30

> ***[30] The doorbell monitoring system of claim 21, wherein the control unit further communicates captured visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications.***

Schranz discloses this limitation. Schranz system control module 43 [*control unit*] is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system." EX-1004, ¶49. As shown below, the system control module 43 (green) [*control unit*] is connected to hard disk drive 52 (red) [*onsite storage device*] which is designed "to record audio and video data from the peripheral devices during an alarm situation using standard formats" [*communicates captured visual and audio communications to an onsite storage*

device and wherein the storage device stores the captured visual and audio communications]. EX-1004, ¶49. Therefore, Schranz system control module 43 [*control unit*] *communicates captured visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications*. EX-1003, ¶110.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶110.

Claim 31

[31] The doorbell monitoring system of claim 30, wherein the stored video and audio communications are accessible by an additional device apart from the control unit.

Schranz discloses this limitation. As explained above with respect to Claim [30], Schranz system control module includes a hard disk drive 52 that "record[s] audio and video data from the peripheral devices during an alarm situation using

standard formats." EX-1004, ¶49. Additionally, Schranz system control module 43 runs a user software application with a web server and web application that the user can access remotely to "control all aspects of the system." EX-1004, ¶50. Schranz explains that the user may access the "website remotely and securely using any Internet browser that supports the https protocol." EX-1004, ¶50. A POSITA understood that in order to control all aspects of the system, the user web application must allow the user to view and manage the audio and video data storage on hard drive 52. Moreover, as the user can access the website from any internet browser, a POSITA understood the *stored video and audio communications* are accessible from any device with an internet browser and is therefore *accessible by an additional device apart from the control unit.* EX-1003, ¶111.

Claim 32

[32] The system of claim 30, wherein the onsite storage device is configured to provide the additional device with access to the stored video and audio communications in substantially realtime.

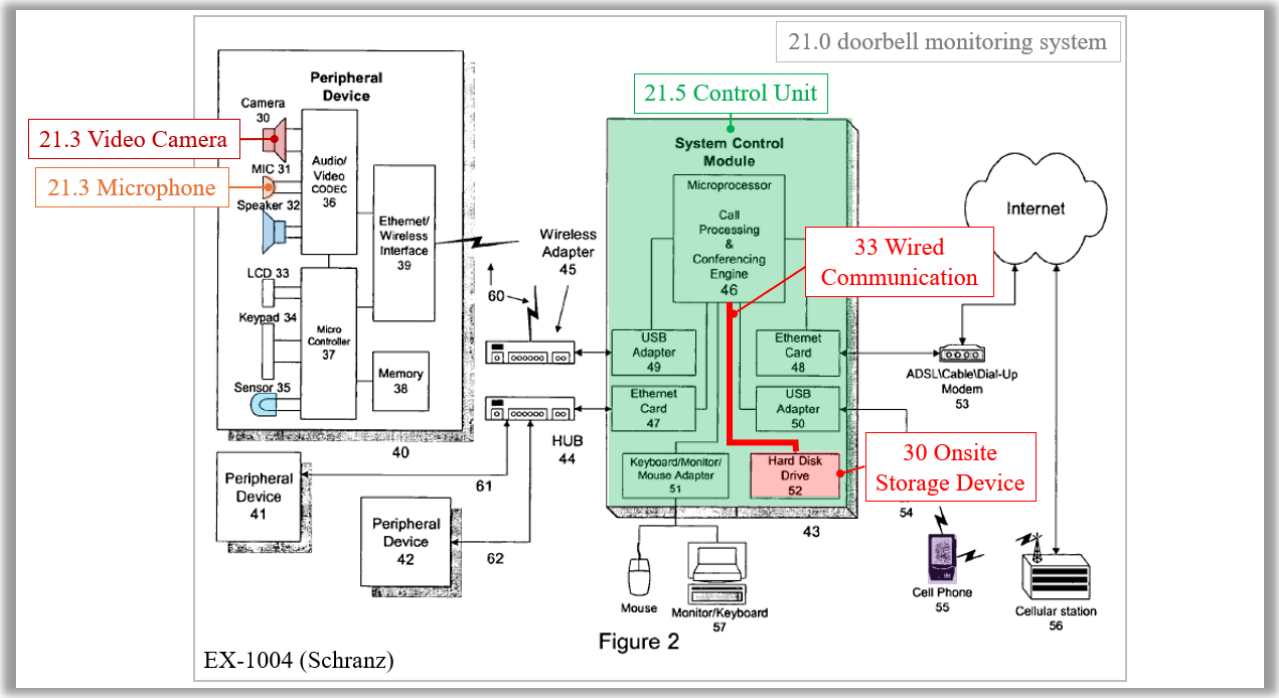
Schranz discloses this limitation. Schranz discloses that its onsite storage devices records video and audio communications in substantially real-time, e.g. "an audio and video recording mechanism that uses a hard disk drive to store the data in real-time using standard audio and video formats." EX-1004, ¶32. Schranz's further discloses that a user can remotely access the security system

through a web portal to control all aspects of the system which a POSITA understood would include access to the stored real-time audio and video data. EX-1004 ¶50, 56. Schranz explains that the user connects to the website via an internet browser that supports the "https protocol," and a POSITA understood that the user is thereby provided access to the stored real-time audio and video data in *substantially realtime*. Therefore, Schranz's user monitor and keyboard 57 with web interface or website provides *access to the stored video and audio communications in substantially realtime*. EX-1003, ¶111.

Claim 33

[33] The system of claim 30, wherein the control unit communicates the captured visual and audio communications to the onsite storage device via wired communication.

Schranz discloses this limitation. As shown below in Figure 2, Schranz system control module 43 [*control unit*] provides audio and video data to hard drive 52 [*onsite storage device*] *via wired communication*. EX-1003, ¶113.



EX-1004, Figure 2 (annotated) ; EX-1003, ¶113.

Claim 34

[34.0] A doorbell monitoring system comprising:

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.0]. EX-1003, ¶114.

[34.1] a doorway having an environment;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.1]. EX-1003, ¶115.

[34.2] a doorbell located in an entry point, activation of the doorbell being a triggering event;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.2]. EX-1003, ¶116.

[34.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.3]. EX-1003, ¶117.

[34.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.4]. EX-1003, ¶118.

[34.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera and external microphone, and for communicating the received audio communications to the external speaker;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.5]. EX-1003, ¶119.

[34.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit; and

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.6]. EX-1003, ¶120

[34.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.7]. EX-1003, ¶121

[34.8] wherein the single communications unit is configured to play a pre-recorded message to a visitor at the entry point and wirelessly streaming at least a portion of the captured visual and audio communications to the control unit;

Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system is designed to play a "pre-recorded audio playback at a peripheral device with an announcement stored on the SCM." EX-1004, ¶33. Schranz explains that the peripheral devices [*single communication unit*] are often located "at the main entrance to the premises" and typical examples of the pre-recorded message "include a doorbell chime, attack dogs barking or the speech of a person." EX-1004, ¶48, ¶33. Therefore, Schranz discloses a *single communications unit configured to play a pre-recorded message to a visitor at the entry point*. Moreover, for the same reasons as described with respect to limitation [21.8], Schranz's system discloses that *the entry point visual and audio communications are wirelessly streamed to the control unit*. EX-1003, ¶122.

[34.9] wherein the video camera is configured to collect the entry point visual communications before the triggering event; and

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.11]. EX-1003, ¶123.

[34.10] wherein the video camera is configured to collect additional visual communications after the triggering event.

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12]. EX-1003, ¶124.

Claim 35

[35] The doorbell monitoring system of claim 34, wherein the single communications unit is configured to stream at least a portion of the captured visual and audio communications.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [22]. EX-1003, ¶125.

Claim 36

[36] The doorbell monitoring system of claim 34, wherein the single communications unit is configured to capture additional video from the video camera after the triggering event.

Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12]. EX-1003, ¶126.

Claim 37

[37] The doorbell monitoring system of claim 34, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [24]. EX-1003, ¶127.

Claim 38

[38] The doorbell monitoring system of claim 37, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [25]. EX-1003, ¶128.

Claim 39

[39] The doorbell monitoring system of claim 34, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime; and wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [25] and limitation [21.15]. EX-1003, ¶129.

Claim 40

[40] The doorbell monitoring system of claim 34, wherein the control unit further comprises a data storage unit wherein the control unit is configured to store the entry point visual and audio communications in the data storage unit of the control unit.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [27]. EX-1003, ¶130.

Claim 41

[41] The doorbell monitoring system of claim 34, wherein the control unit is configured to generate a file that includes at least a portion of the entry point visual and audio communications captured by the single communications unit.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [27]. EX-1003, ¶131.

Claim 42

[42] The doorbell monitoring system of claim 34, wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [28]. EX-1003, ¶132.

Claim 43

[43] The doorbell monitoring system of claim 42, wherein the two or more actions are at least one of (1) play a pre-recorded greeting, (2) request additional video and/or audio communications, (3) institute two-way video communications between the user and the person at the entry point, (4) notify an alarm company, or (5) selection of no action.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [29]. EX-1003, ¶133.

Claim 44

[44] The doorbell monitoring system of claim 34, wherein the control unit further communicates captured visual and audio communications to an onsite storage device and wherein the

storage device stores the captured visual and audio communications.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [30]. EX-1003, ¶134.

Claim 45

[45] The doorbell monitoring system of claim 44, wherein the stored video and audio communications are accessible by an additional device apart from the control unit.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [31]. EX-1003, ¶135.

Claim 46

[46] The system of claim 44, wherein the onsite storage device is configured to provide the additional device with access to the stored video and audio communications in substantially realtime.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [32]. EX-1003, ¶136.

Claim 47

[47] The system of claim 45, wherein the control unit communicates the captured visual and audio communications to the onsite storage device via wired communication.

Schranz discloses this limitation for the same reasons as discussed with respect to Claim [33]. EX-1003, ¶137.

VI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Party-in-Interest Under 37 C.F.R. §42.8(b)(1)

Petitioner certifies that the real party-in-interest in this Petition is Vivint LLC.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

1. Judicial Matters

To Petitioners' knowledge, the '191 Patent is involved in the following pending litigation:

Case Heading	Number	Tribunal	Date
Duke W. Zinser v. Vivint, LLC and Vivint, Inc.	4:25-cv-01030	EDTX	September 18, 2025

2. Administrative Matters

As of this Petition's filing and to the best knowledge of Petitioner, the '191 Patent has not been subject to any *inter partes* reviews or reissues. The '191 Patent was subject to Reexamination No. 90/019,542.

3. Related Patents

To the best knowledge of Petitioner, there are no patents related to the '191 Patent.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Back-Up Counsel
Patrick D. McPherson Reg. No. 46,255 PDMcpherson@duanemorris.com DUANE MORRIS LLP 901 New York Avenue NW Suite 700 East Washington, D.C. 20001 T: (202) 776-7800	Patrick C. Muldoon Reg. No. 47,343 PCMuldoon@duanemorris.com DUANE MORRIS LLP 901 New York Avenue NW Suite 700 East Washington, D.C. 20001 T: (202) 776-7800 Gilbert A. Greene, Reg. No. 48,366 BGreene@duanemorris.com DUANE MORRIS LLP Terrace 7, 2801 Via Fortuna, Suite 200 Austin, TX 78746 T: 512-277-2246 Joe Powers Reg. No. 47,006 japowers@duanemorris.com DUANE MORRIS LLP 30 South 17th Street Philadelphia, PA 19103 T: 215-979-1000

D. Service Information 37 C.F.R. §42.8(b)(4)

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioner consents to electronic service at the email addresses above as well as to our docketing department at the following address: DC_IPDocketing@duanemorris.com..

E. Payment of Fees – 37 C.F.R. §42.103

The required fee is being paid using the Patent Review Processing System.

VII. CONCLUSION

Petitioner requests the Board institute an IPR and cancel the Challenged Claims.

Respectfully submitted,

DUANE MORRIS LLP

Dated: March 16, 2026

/s/Patrick D. McPherson/
Patrick D. McPherson
USPTO Reg. No. 46,255
DUANE MORRIS LLP
901 New York Avenue NW
Suite 700 East
Washington, D.C. 20001

LEAD COUNSEL FOR PETITIONER

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. §42.24 *et seq*., the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,233 words as calculated by the "Word Count" feature of Microsoft Word 365, the word processing program used to create it.

Dated: March 16, 2026

/s/Patrick D. McPherson/
Patrick D. McPherson
Reg. No. 46,255
Lead Counsel for Petitioner

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on March 16, 2026, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent 7,583,191 and all supporting exhibits were served via Federal Express, postage prepaid, to the correspondence address of record for the '191 Patent:

Kirby Drake Law PLLC
2550 Pacific Avenue
Suite 700
Dallas, TX 75226
UNITED STATES

Courtesy copies of the Petition and supporting exhibits were sent by email to the litigation Counsel below:

Gary R. Sorden
gsorden@coleschotz.com
Aaron Davidson
adavidson@coleschotz.com
Brian A. Carpenter
bcarpenter@coleschotz.com
Timothy J.H. Craddock
tcraddock@coleschotz.com
Brian L. King
bking@coleschotz.com
Jeffrey M. Saltman
jsaltman@coleschotz.com

/s/Patrick C. Muldoon/
Patrick C. Muldoon
Reg. No. 47,343
Counsel for Petitioner