

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EXACQ TECHNOLOGIES, INC.,
Petitioner,

v.

JDS TECHNOLOGIES, INC.,
Patent Owner.

Case IPR2016-00568
Patent 6,891,566 B2

Before JONI Y. CHANG, DAVID C. McKONE, and
ROBERT J. WEINSCHENK, *Administrative Patent Judges*.

McKONE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

Exacq Technologies, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) to institute an *inter partes* review of claims 1–10, 23–28, and 49–54 of U.S. Patent No. 6,891,566 B2 (Ex. 1001, “the ’566 patent”). JDS Technologies, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 6, “Prelim. Resp.”). Upon consideration of the Petition and Preliminary Response, we conclude, under 35 U.S.C. § 314(a), that Petitioner has not established a reasonable likelihood that it would prevail with respect to any of the challenged claims. Accordingly, we do not institute an *inter partes* review of the ’566 patent.

B. Related Matters

The parties indicate that the ’566 patent has been asserted in *JDS Technologies, Inc. v. Avigilon USA Corp., Inc.*, Case No. 2:15-cv-10385-AC-EAS (E.D. Mich.), and *JDS Technologies, Inc. v. Exacq Technologies, Inc.*, Case No. 2:15-cv-10387-AC-EAS (E.D. Mich.). Pet. 1; Paper 5, 1. The ’566 patent also is the subject of three additional *inter partes* review petitions in IPR2016-00520, IPR2016-00522, and IPR2016-00532. Pet. 1; Paper 5, 1.

C. Evidence Relied Upon

Petitioner relies on the following prior art:

U.S. Patent No. 6,166,729, issued Dec. 26, 2000, filed May 7, 1997
(Ex. 1004, “Acosta”);

AXIS Communications AB, *AXIS 2400/2401 Administration Manual*,
Rev. 1.1 (July 1999) (Ex. 1009, “AXIS 2400”);
U.S. Patent No. 5,825,432, issued Oct. 20, 1998 (Ex. 1014,
“Yonezawa”);
U.S. Patent No. 6,583,813 B1, issued June 24, 2003, filed Oct. 7, 1999
(Ex. 1015, “Enright”);
U.S. Patent No. 5,499,180, issued Mar. 12, 1996 (Ex. 1016,
“Ammirato”);
U.S. Patent No. 6,784,925 B1, issued Aug. 31, 2004, filed Mar. 24,
1998 (Ex. 1017, “Tomat”);
U.S. Patent No. 5,822,542, issued Oct. 13, 1998 (Ex. 1018, “Smith”).
Petitioner also relies on the Declaration of Greg Thompson (Ex. 1003,
“Thompson Decl.”).

D. The Asserted Grounds

Petitioner asserts the following grounds of unpatentability (Pet. 4):

References	Basis	Claim(s) Challenged
Yonezawa, Acosta, and AXIS 2400	§ 103(a)	1–3, 5, 7–9, 23, 28, 52, 54
Yonezawa, Acosta, AXIS 2400, and Ammirato	§ 103(a)	4
Yonezawa, Acosta, AXIS 2400, and Smith	§ 103(a)	6
Yonezawa, Acosta, AXIS 2400, and Enright	§ 103(a)	10, 25–27
Yonezawa, Acosta, AXIS 2400, and Tomat	§ 103(a)	24
Yonezawa and Acosta	§ 103(a)	49–51, 53

E. The '566 Patent

The '566 patent describes a system for networking digital video cameras. Ex. 1001, Abstract. Figure 1, reproduced below, illustrates an example:

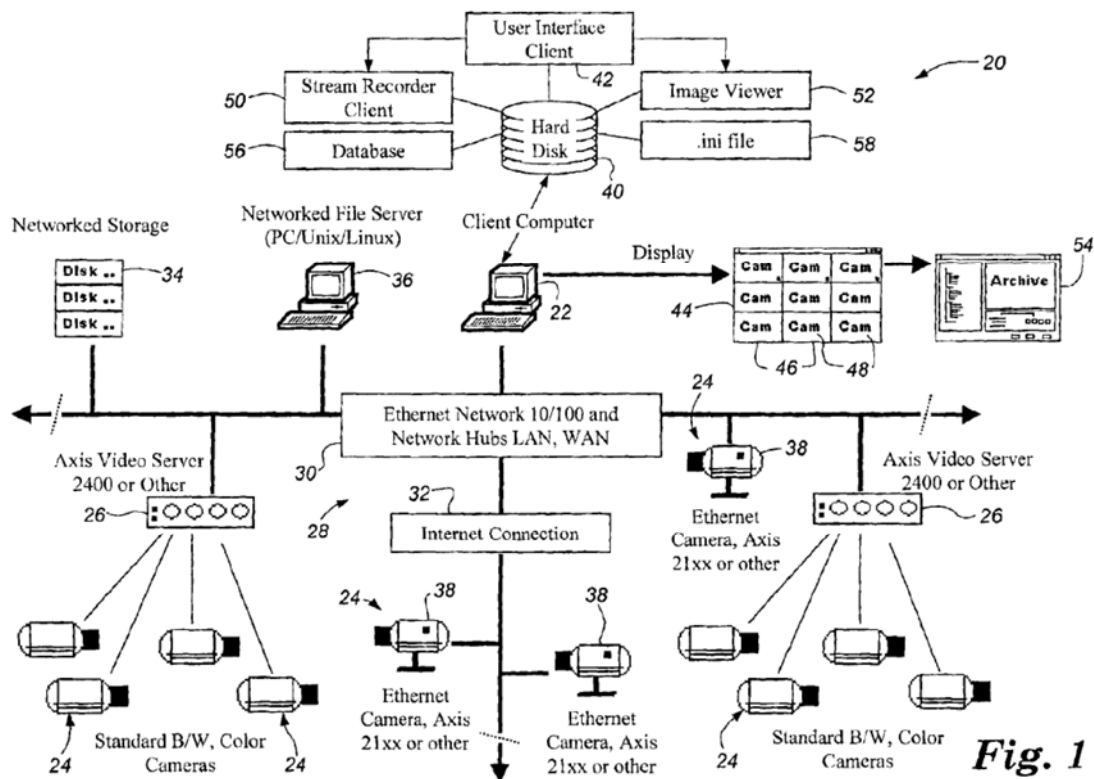


Figure 1 is a block diagram of digital video system 20. *Id.* at 4:20–21.

A plurality of digital video cameras 24 are connected to one or more standalone video servers 26 (which can be Axis 2400, 2401, or 240 video servers). *Id.* at 5:5–6, 5:17–19. Client computer 22 connects to video servers 26 via network 28, which can include private network segment 30 and public network 32 (e.g., the Internet). *Id.* at 5:7–10. Client computer 22 includes a computer readable memory, such as fixed hard drive 40, for storing user interface client application 42. *Id.* at 5:27–30. User interface client application 42 includes a user interface program, in computer readable

form, along with additional software components, such as Web browser extensions, operating system libraries, and compression libraries. *Id.* at 5:30–42.

User interface client program 42 is operable to access locally stored (on hard drive 40) data that uniquely identify cameras 24. *Id.* at 5:51–53. User interface client program 42 then attempts to access those cameras over network 28. *Id.* at 5:53–54. User interface client program 42 is operable to verify access to those cameras 24 that are currently accessible, and to generate user interface display 44 (on the computer’s monitor) including display window 46, for each of cameras 24 accessed over network 28, and to display in each display window 46 image 48 received from the camera associated with that display window. *Id.* at 5:54–61.

In one example, each of video cameras 24 has a unique media access control (“MAC”) address. *Id.* at 6:48–51. To validate access to a camera, user interface client program 42 retrieves MAC addresses from database 56 (stored on hard drive 40), queries the camera for its MAC address (using file transfer protocol (“FTP”)), and compares the camera’s MAC address to the MAC addresses from database 56 to verify that the camera’s MAC address is valid. *Id.* at 6:36–51.

Claim 1, reproduced below, is illustrative of the claimed subject matter:

1. A computer readable medium for use by a computer in providing an interface to multiple cameras via one or more video servers accessible to the computer via a network, comprising:
 - a digital storage device;
 - a user interface program stored on said digital storage

device in computer readable form, said program being operable upon execution by the computer to access server data uniquely identifying each video server and to attempt access to the video servers over the network, said program also being operable to obtain from each of the accessible video servers a hardware address stored in the video server;

wherein said program is further operable to validate the hardware addresses received from the video servers using the server data and, for those video servers having valid hardware address, said program is operable to generate a user interface display on the computer that includes a display window for each of the cameras accessed via the validated servers over the network and to display in each of the display windows an image received from the camera associated with that display window.

II. ANALYSIS

A. *Claim Construction*

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1278 (Fed. Cir. 2015), *cert. granted sub nom. Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 890 (U.S. Jan. 15, 2016) (No. 15-446). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Claim 1 recites a user interface program “operable . . . to attempt access to the video servers over the network, said program also being

operable to obtain from each of the accessible video servers a hardware address stored in the video server.” Patent Owner reads this language to mean that “[o]nly after the video server is accessible, does the user interface program ‘obtain from each of the **accessible video servers** a hardware address stored in the video server.’” Prelim. Resp. 34 (quoting claim 1). According to Patent Owner, “[b]y the plain language of claim, you must have an accessible video server before the program can obtain anything from ‘the accessible video server.’” *Id.* Thus, Patent Owner urges us to read “attempt access to the video servers over the network” and “obtain from each of the accessible video servers a hardware address stored in the video server” together, and in that order. *Id.* at 35–36 (“these limitations . . . require a sequence based on the express language of the claim”).

Despite the requirement that the Petition identify “[h]ow the challenged claim is to be construed” (37 C.F.R. § 42.104(b)(3)), Petitioner does not propose a construction for this term or any other claim term. Pet. 5.

We agree with Patent Owner. Claim 1 recites a user interface program operable to obtain a hardware address from an “accessible” video server. We read this as a reference to the previously recited “attempt access to the video servers over the network.” In other words, the plain language of claim 1 suggests that the user interface software obtains the hardware address from a video server that it has successfully attempted to access. This is consistent with the Specification, which explains that “[user interface] program [42] is operable to verify access to at least those cameras 24 that are currently accessible.” Ex. 1001, 5:54–56. In one embodiment, the hardware address stored on a camera server is a MAC address and the user interface program obtains the MAC address from the camera server by

querying the camera using file transfer protocol (“FTP”). *Id.* at 6:36–38, 6:48–51. A query to the camera server is an attempt to access the camera server.¹

For purposes of this Decision, no other claim term requires express construction.

B. Asserted Grounds of Unpatentability

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” We resolve the question of obviousness 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) objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In an obviousness analysis, some reason must be shown as to why a person of ordinary skill would have combined or modified the prior art to achieve the patented invention. *See Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008). A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem

¹ We do not reach Patent Owner’s argument (Prelim. Resp. 14–16) that the claim language “to obtain” means “retrieve and receive,” rather than just “receive.”

known in the field of endeavor at the time of invention and addressed by the patent''; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

1. Level of Ordinary Skill

Relying on Mr. Thompson's testimony, Petitioner contends that a person of ordinary skill in the art would have had an undergraduate degree in computer or electrical engineering and two-to-three years of experience in the design and programming of video management software. Pet. 5 (citing Ex. 1003 ¶¶ 27–32). Patent Owner argues that a skilled artisan would have had an Associate's or Bachelor's degree in computer or electrical engineering or would have had one year of experience in the field of computer software. Prelim. Resp. 13. On this record, we credit Mr. Thompson's testimony and adopt Petitioner's statement of the level of ordinary skill.

2. Alleged Obviousness of Claims 1–10 and 23–28

Petitioner contends that claims 1–3, 5, 7–9, 23, and 28 would have been obvious over Yonezawa, Acosta, and AXIS 2400. Pet. 4. Petitioner further contends that claim 4 would have been obvious over Yonezawa, Acosta, AXIS 2400, and Ammirato; that claim 6 would have been obvious over Yonezawa, Acosta, AXIS 2400, and Smith; that claims 10 and 25–27 would have been obvious over Yonezawa, Acosta, AXIS 2400, and Enright;

and that claim 24 would have been obvious over Yonezawa, Acosta, AXIS 2400, and Tomat. *Id.*

a. Overview of Yonezawa

Yonezawa describes a monitor system for displaying images from a plurality of image transmission sources connected to a network. Ex. 1014, Abstract. Figure 1, reproduced below, illustrates an example:

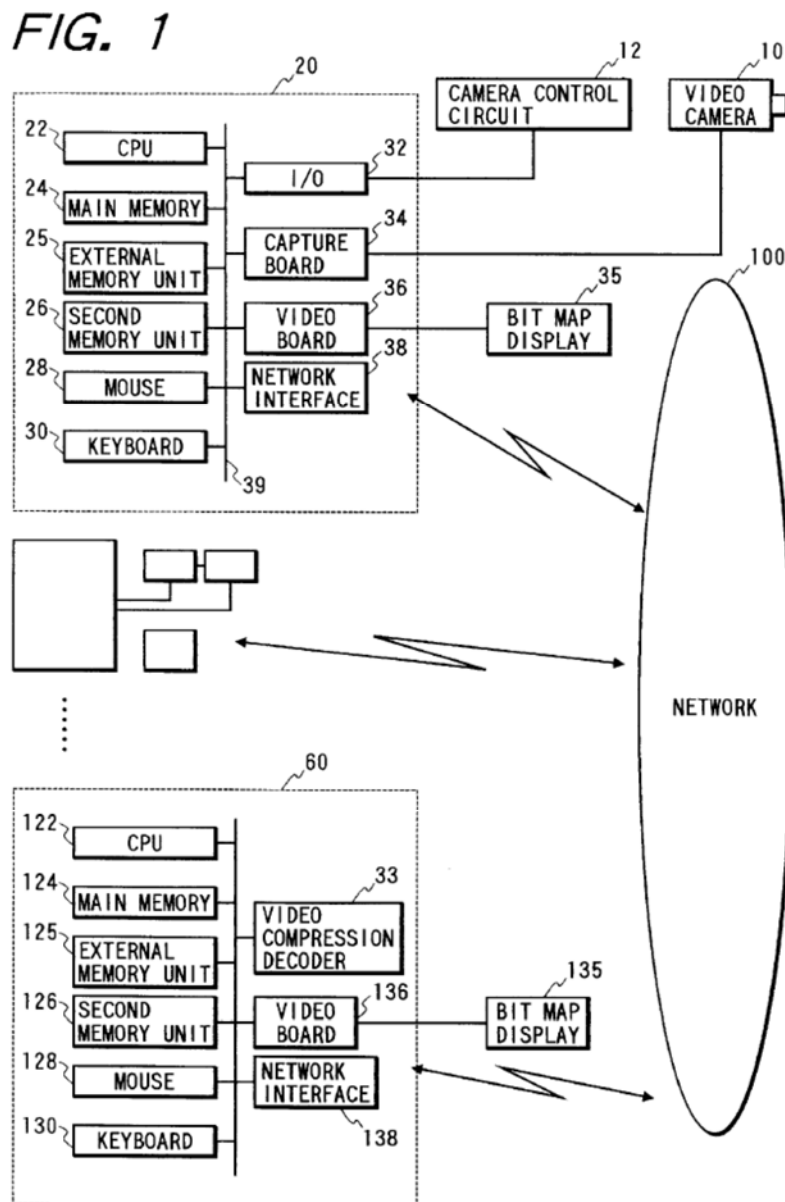


Figure 1 is a block diagram of an image transmission terminal and a monitor terminal. *Id.* at 2:7–9.

Image transmission terminal 20 (a workstation or personal computer) controls video camera 10 and transmits an image captured by video camera 10 to network 100. *Id.* at 3:10–25. Monitor terminal 60 sends a control signal for video camera 10 to image transmission terminal 20, which sends a status to monitor terminal 60. *Id.* at 3:62–4:1. Monitor terminal 60 receives, via network 100, image data sent from image transmission terminal 20, decompresses them, and displays the data on bit map display 135. *Id.* at 4:1–6, 4:17–20. As shown in Figure 5, an image display window can include multiple display areas. *Id.* at 5:7–10. As shown in Figure 2, monitor terminal 60 includes software 400, such as camera control client 411 for remotely controlling a camera, image receiving software 412 for decompressing and displaying image data, and map managing software 413 (including a graphical user interface). *Id.* at 4:25–38.

b. Overview of Acosta

Acosta describes a system for viewing digital images of remote locations. Ex. 1004, Abstract. Figure 1, reproduced below, illustrates an example:

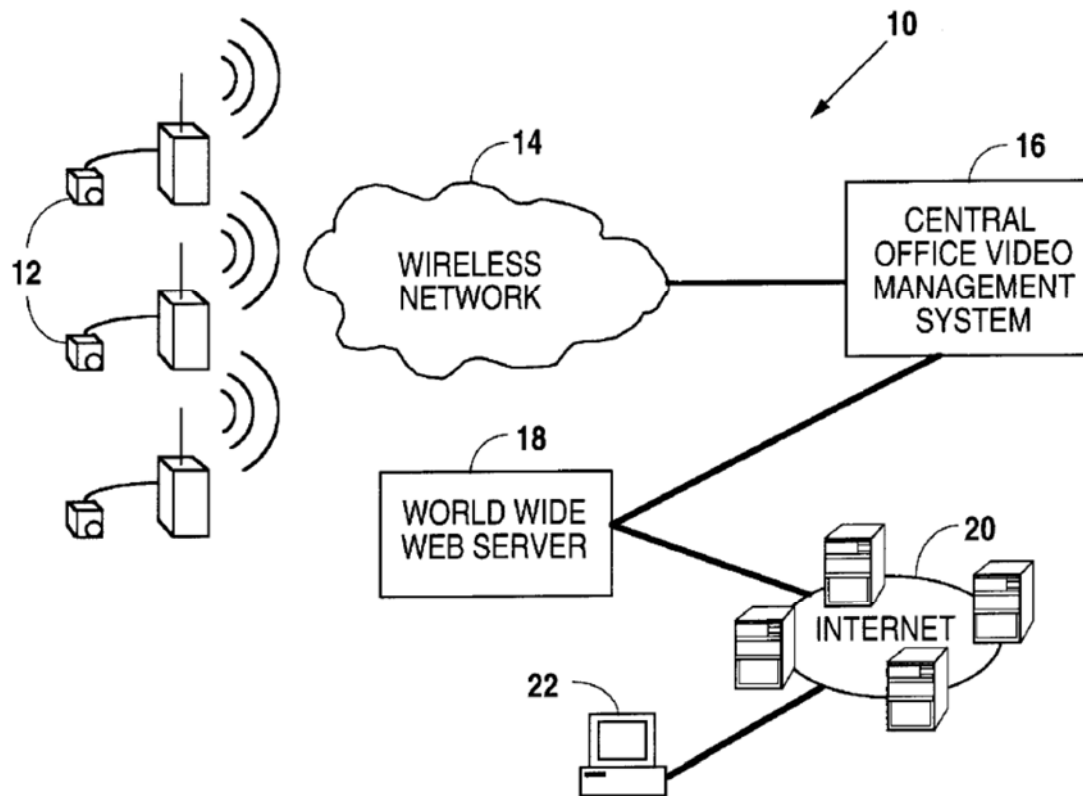


Fig. 1

Figure 1 is a block diagram of a system for viewing live images, in real-time, from multiple remote locations over wireless and wired networks. *Id.* at 2:45–49.

In remote viewing system 10, camera devices 12 are connected, via wireless network 14, to central office video management system (“COVMS”) 16. COVMS 16, in turn, is connected to World Wide Web (“WWW”) server 18 and, via Internet 20, to computer 22. Computer 22 is equipped with a web browser for accessing information available on Internet 20. *Id.* at 4:26–41. COVMS 16 receives images from camera elements 12 over wireless network 14 and decodes the images. *Id.* at 12:57–61. COVMS 16 performs four distinct operations. *Id.* at 12:64–65. Petitioner

focuses, in particular, on the operation of a CommLink Manager process of COVMS 16, depicted in Figure 20, reproduced below:

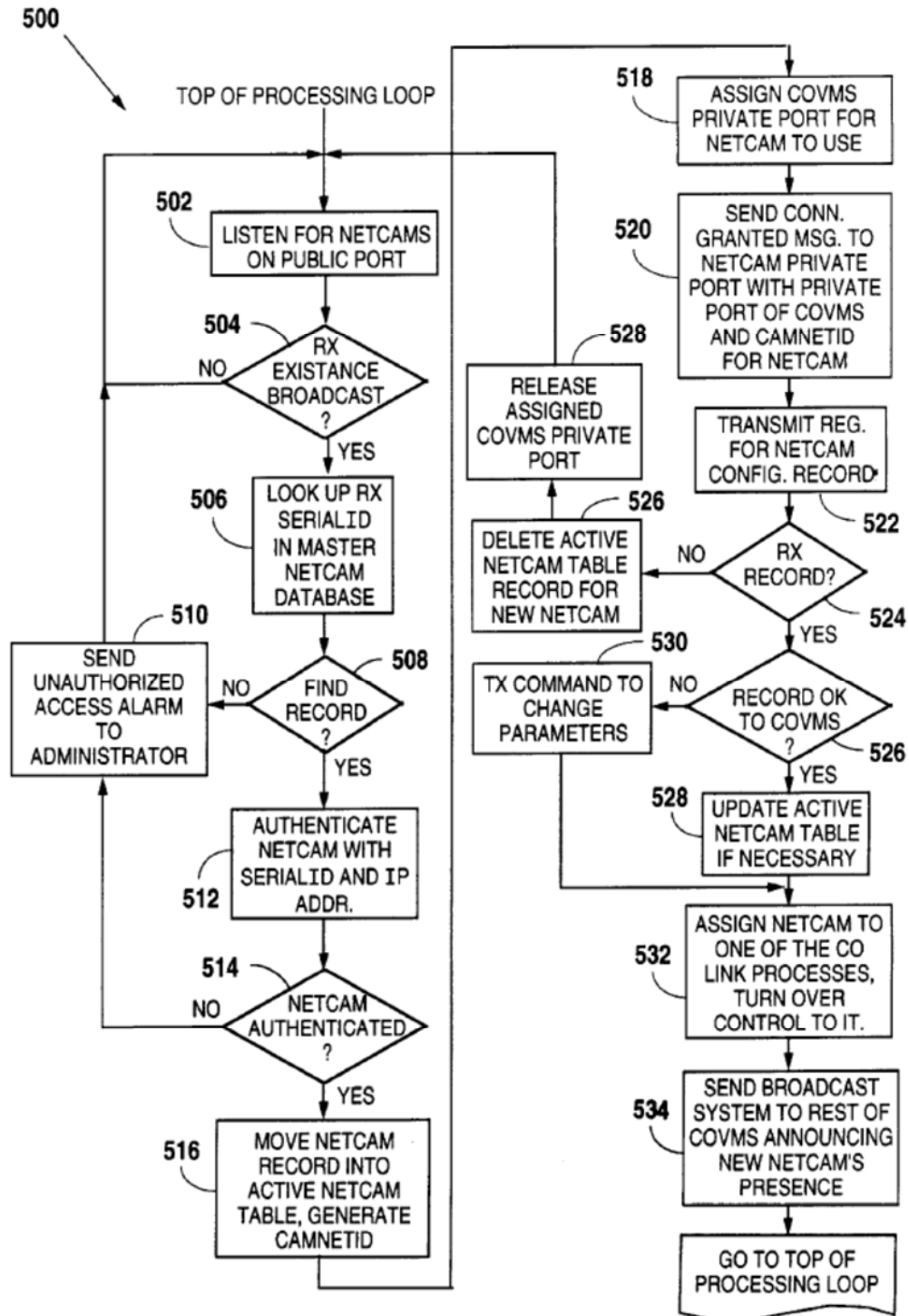


Fig. 20

Figure 20 is a flow chart of a method of operation of a CommLink Manager. *Id.* at 3:44–46.

The process of Figure 20 starts when COVMS 16 listens for and receives a communication request from a camera element 12. *Id.* at 17:35–48 (steps 502, 504). If COVMS 16 detects a broadcast, that broadcast includes a serial ID for the camera element 12. *Id.* at 17:46–48. COVMS 16 looks up, in a database, the serial ID assigned to that camera element and obtains an IP address for that camera element. *Id.* at 17:48–53 (step 506). COVMS 16 determines whether the serial ID and the IP address match and, if so, the camera element 12 is authenticated according to the serial ID and is assigned an IP address. *Id.* at 53–62 (steps 508, 512). COVMS 16 assigns a particular port for use by that camera element 12 in communications with COVMS 16 and communicates that port to the camera element. *Id.* at 18:2–7 (steps 518, 520). COVMS 16 then sends a transmit request to the camera element for its particular configuration record. *Id.* at 18:7–10. If the configuration record is suitable, the camera element is linked to COVMS 16 and COVMS 16 notifies each of the components of system 10 that the camera element is linked to system 10. *Id.* at 18:17–26.

c. Overview of AXIS 2400

AXIS 2400 is a user manual for the AXIS 2400/2401 Video Server. Ex. 1009, 2.² According to AXIS 2400, “Axis’ Video Servers include a built-in Web server that enhances traditional surveillance systems and

² We refer to the page numbers of the document itself, at the top left or right of each page, rather than the page numbers affixed by Petitioner to the bottom right of each page.

provides added networking connectivity for distributing monitored images over a secure intranet network, or even the Internet,” and allow “[v]ideo camera management, configuration, and monitoring - all at your fingertips through a standard Web browser; such as, Netscape Navigator or Microsoft Internet Explorer.” *Id.* at 7. The AXIS 2400 Video Server, for example, connects to Ethernet networks and supports up to four video cameras. *Id.* Relevant to Petitioner’s contentions, the described video server includes a serial number, which is identical to the Ethernet address of the unit. *Id.* at 9.

d. Claims 1–10 and 23–28

Regarding claim 1, Petitioner contends that Yonezawa’s monitor terminal 60 is “a computer.” Pet. 15. Petitioner argues that monitor terminal 60 includes ROM, RAM, an optical disk, or a magnetic disk for storing software 410, disclosure Petitioner maps to a “computer readable medium” and “a digital storage device” of claim 1. *Id.* at 16–17. Although Petitioner does not say so explicitly, it appears that Petitioner contends that Yonezawa’s image transmission terminal 20 is “one or more video servers,” as recited in claim 1. *Id.* at 15, 19–20. Petitioner further contends that Yonezawa’s image receiving software 412 is a “user interface program,” as recited in claim 1. *Id.* at 17. As to the user interface program being “operable to generate a user interface display on the computer that includes a display window for each of the cameras accessed via the validated servers over the network and to display in each of the display windows an image received from the camera associated with that display window,” as recited in claim 1, Petitioner cites to Figure 5 of Yonezawa as showing a user interface

displaying multiple display areas for images from multiple sources. *Id.* at 29–30.

Regarding the user interface program “operable upon execution by the computer to access server data uniquely identifying each video server,” as recited in claim 1, Petitioner points to Acosta’s description of COVMS 16 opening a “Master Camera Element Database” for camera elements 12 and creating, in the memory of COVMS 16, an “Active Camera Element Table” of the camera elements 12 that are active in the system. *Id.* at 21 (citing Ex. 1004, 13:44–49).

As to the user interface program “operable upon execution by the computer . . . to attempt access to the video servers over the network,” as recited in claim 1, Petitioner cites to Acosta’s general description of COVMS 16 communicating with camera elements 12 using the TCP/IP protocol suite. Pet. 21–22 (citing Ex. 1004, 7:31–35). Petitioner further cites to Acosta’s description of COVMS 16 sending transmit requests to a camera element 12 after that camera element has been authenticated and COVMS 16 determining whether a record is received from the camera element 12 corresponding to the transmit request. *Id.* at 22–23 (citing Ex. 1004, 18:7–19, Fig. 20 (steps 522, 524, 526)).

Regarding the user interface program “also being operable to obtain from each of the accessible video servers a hardware address stored in the video server,” as recited in claim 1, Petitioner points to Acosta’s description of COVMS 16 listening for camera elements 12 during the authentication process and, upon detection of an incoming broadcast from a camera element, detecting whether the broadcast includes a serial ID for the camera element. *Id.* at 23–24 (citing Ex. 1004, 17:41–48, Fig. 20 (steps 502, 504)).

Petitioner argues that the serial ID necessarily is stored by camera element 12 if camera element 12 is to transmit it. *Id.* at 25. Petitioner further argues that a skilled artisan would have modified Yonezawa's image receiving software 412 to be interoperable with the AXIS 2400 Video Server described in AXIS 2400. Pet. 19. According to Petitioner, a skilled artisan would have done so "to increase the network camera devices supported by the image receiving software 412." *Id.* at 20. Petitioner argues that it would have been "the simple substitution of one known, equivalent element for another to obtain the predictable result of interoperability between the two." *Id.* Petitioner also argues that it would have been a routine design choice to use MAC addresses for server identification, as taught in AXIS 2400. *Id.* at 21 (citing Ex. 1009, 9).

Regarding the user interface program being "further operable . . . to validate the hardware addresses received from the video servers using the server data," Petitioner cites to description in Acosta of COVMS 16 looking up, in a database, the serial ID assigned to a camera element 12 from which COVMS 16 received a broadcast, obtaining an IP address for that camera element 12, and determining whether the serial ID and IP address match. Pet. 26–27 (citing Ex. 1004, 17:48–59, Fig. 20 (steps 506, 508, 512, 514, 516, 518, 520)). Petitioner argues that this is a disclosure of COVMS 16

comparing the serial ID received from the camera element to a serial ID in a database of the COVMS 16. *Id.* at 27.³

Patent Owner contends that the serial ID is an identifier generated by COVMS 16 for a particular communication, rather than a hardware address stored on a camera element. Prelim. Resp. 23. In summarizing the operations of COVMS 16's CommLink Manager, Acosta states that "[i]n general, each communication between any one of the camera elements and the COVMS 16 is assigned an identification (ID)" and that "[t]he ID is used by all the other processes with the system 10." Ex. 1004, 17:30–33. Patent Owner contends that this disclosure makes clear that the serial IDs are not associated with and stored on camera elements 12. Prelim. Resp. 23. Accordingly, Patent Owner argues, Acosta does not teach a "hardware address stored in the video server," as recited in claim 1. *Id.* at 27–28. While we take note of the ambiguity of Acosta's disclosure, Acosta states that the initial broadcast from a camera element "includes the serial ID for the camera 12." Ex. 1004, 17:46–48. On this record, we read Acosta to describe a serial ID as stored on and associated with a camera element,

³ Patent Owner argues that the identifier stored in Acosta's Master Camera Element Database, to which Petitioner cites as teaching "server data uniquely identifying each video server" (Pet. 21), is generated after authentication. Prelim. Resp. 37–38. For purposes of this Decision, and for consistency with Petitioner's position on a user interface operable to validate the hardware addresses received from the video servers using the server data, we proceed as if Petitioner identifies "the serial ID assigned to the camera element 12 making the broadcast [stored] in a database of the COVMS 16 containing the serial ID's for all of the camera elements 12 then operating" (Ex. 1004, 17:48–52) as the "server data uniquely identifying each video server" recited in claim 1.

rather than simply being assigned by COVMS 16 to an individual communication between a camera element and COVMS 16.

Patent Owner also argues that Acosta does not teach a user interface program operable “to attempt access to the video servers” and “to obtain from each of the accessible video servers a hardware address stored in the video server,” as recited in claim 1. Prelim. Resp. 34–35. Patent Owner argues that “the video server must be *accessible* to the user interface program—by IP address (or other mechanism)—before [“said program is further operable to obtain from each of the accessible video servers a hardware address stored in the video server”] can be satisfied.” *Id.* at 34. According to Patent Owner, “Acosta only identifies attempts to access the camera element after an IP address is assigned [to the camera element], which is after the alleged ‘authentication’ process.” *Id.* at 35. Patent Owner further cites to AXIS 2400, arguing that its video server is not accessible without an IP address. *Id.* (citing Ex. 1009, 15 (“To enable access to your video server you must first assign it an appropriate IP Address.”)).

As Patent Owner points out (*id.* at 35), Petitioner cites to Acosta’s disclosure of COVMS 16 using the TCP/IP suite to communicate with a camera element after that camera element has been authenticated as disclosing “to attempt access to the video servers over the network.” Pet. 21–22 (citing Ex. 1004, 18:7–19, Fig. 20 (steps 522, 524, 526)). As explained above, for the claim limitation “said program also being operable to obtain from each of the accessible video servers a hardware address stored in the video server,” as recited in claim 1, Petitioner (Pet. 24–25) cites to Acosta’s authentication process (specifically, Fig. 20, steps 502, 504), which

occurs before the camera element is accessed (at Fig. 20, steps 522, 524, 526).

We agree with Patent Owner. As explained in Section I.A above, according to the plain language of claim 1, the user interface software obtains a hardware address from a video server that it has successfully attempted to access. According to the evidence cited by Petitioner, COVMS 16 does not first attempt to access a camera element 12 before authenticating it. Rather, COVMS 16 listens for a camera element 12 sending a broadcast and authenticates the camera element based on information (serial ID) received from the broadcast. Ex. 1004, 17:41–52. Only after the camera element 12 is authenticated does the COVMS 16 take action to communicate with camera element 12, assigning it an IP address, assigning it a particular port on COVMS 16, sending it a connection granted message, and sending a request to camera element 12 to transmit a record. *Id.* at 17:50–18:16, Fig. 20 (steps 512, 518, 520, 522). On this record, we agree with Patent Owner that “there are no disclosed ‘accessible video servers’ when a communication serial ID . . . is broadcast in Acosta.” Prelim. Resp. 35. Accordingly, Petitioner’s evidence does not support a finding that Yonezawa, Acosta, and AXIS 2400 teach “a user interface program . . . operable . . . to attempt access to the video servers over the network, said program also being operable to obtain from each of the accessible video servers a hardware address stored in the video server,” as recited in claim 1.

Petitioner also does not demonstrate that a skilled artisan would have combined the teachings of Yonezawa and Acosta. Petitioner argues that a skilled artisan would have modified Yonezawa’s image receiving software 412 to incorporate the network camera validation technique described in

Acosta. Pet. 18–19. Petitioner argues that both Yonezawa and Acosta are directed to networked camera systems and that Yonezawa’s image receiving software 412 and Acosta’s COVMS 16 “relate to managing connections to network camera devices, and are thus similar components of similar systems.” *Id.* According to Petitioner, a skilled artisan “would be motivated to modify the image receiving software 412 to improve its management of network camera devices by limiting it to receiving images from validated network camera devices only.” *Id.* at 19. Relying on Mr. Thompson’s testimony, Petitioner argues that this would have been the use of known validation techniques to improve a similar network camera system in the same way. *Id.* (citing Ex. 1003 ¶ 55). The testimony of Mr. Thompson to which Petitioner cites (Ex. 1003 ¶¶ 54–55) merely repeats, nearly verbatim, the arguments in the Petition, without providing additional explanation or citing to evidence.

We are not persuaded that Petitioner’s evidence will show that a skilled artisan would have had reason to combine Yonezawa and Acosta in the proposed manner. Petitioner points to no persuasive evidence (in Yonezawa or elsewhere), and we find none, that suggests that Yonezawa’s system suffers from an inability to distinguish between valid and invalid camera servers. Indeed, it appears that Yonezawa’s system’s map managing software 413 includes the capability to track and control cameras by identification number. Ex. 1014, 5:32–45. Petitioner’s statement (repeated by its expert) that Yonezawa’s system would be improved by receiving images only from validated camera devices is not supported by persuasive evidence.

Petitioner's evidence also does not show that Acosta's system is similar to Yonezawa's or that Acosta's validation technique would have improved Yonezawa's system in a similar way. Acosta's COVMS 16 is a device for interfacing between cameras on commercial wireless networks and web servers on wired networks such as the Internet. Ex. 1004, 7:29–8:27. Yonezawa describes using software at a monitor terminal to communicate with and control camera software at an image communication terminal over a network. Ex. 1014, 4:25–38. Petitioner has not introduced persuasive evidence or argument regarding how a technique for validating cameras at an interface between wired and wireless networks (Acosta) would have improved a system in which a monitor terminal communicates with and controls an image communication terminal and attached camera (Yonezawa). Petitioner does not cite to the teachings from either Acosta or Yonezawa as providing reasons to combine. Simply stating that the combination “would merely be the use of known validation techniques to improve a similar network camera system in the same way,” Pet. 19, without evidence, is not sufficient. Petitioner's expert does not add materially to Petitioner's attorney argument, as he merely repeats the Petition's argument nearly verbatim, without citation to the evidence that serves as the basis for his opinion. *See* 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

Because the evidence in the Petition does not support a finding that Yonezawa, Acosta, and AXIS 2400 teach each limitation of claim 1 or that a skilled artisan would have had reason to combine the references as argued

by Petitioner, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claim 1 would have been obvious.

Claims 2–10 and 23–28 depend, directly or indirectly, from claim 1. Petitioner’s evidence regarding these claims does not remedy the deficiency in its evidence for claim 1. *See* Pet. 30–45. Accordingly, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 2–10 and 23–28 would have been obvious.

3. Alleged Obviousness of Claims 49–54

Petitioner contends that claims 49–51 and 53 would have been obvious over Yonezawa and Acosta. Pet. 4. Petitioner further argues that claims 52 and 54 would have been obvious over Yonezawa, Acosta, and AXIS 2400. Claim 49 is independent.

Regarding claim 49, Petitioner’s allegations are not entirely clear. On one hand, Petitioner cites Yonezawa as teaching a “digital video system,” as recited in claim 49. Pet. 45–47. On the other (and inconsistently with its position as to claim 1), Petitioner cites only to Acosta as teaching “a client computer” and “one or more video servers accessible by the client computer over a network,” as recited in claim 1. *Id.* at 47. In contrast to its arguments for claim 1 (which identify Yonezawa’s image transmission terminal 20 as the “one or more video servers”), Petitioner contends that Acosta’s camera elements 12 include both “a plurality of cameras” and “the video server(s), said video server(s) providing an interface between the cameras and client computer” of claim 49. *Id.* at 47–49. In contrast to Petitioner’s arguments for claim 1 (which identify Yonezawa’s monitor terminal 60 as the “computer”), Petitioner maps Acosta’s COVMS 16 to the “client computer”

of claim 49. *Id.* Aside from noting that a camera element 12 includes a video digitizer, processor card, remote communications link module, and antenna (*id.* at 48 (citing Ex. 1004, 4:43–45)), Petitioner does not explain how a camera element 12 is a video server. Petitioner’s citation to Mr. Thompson’s testimony is not helpful, as it merely repeats the argument from the Petition. Ex. 1003 ¶¶ 119–20.

Claim 49 recites “the video server(s) including a unique number that is stored in memory within the video server(s) and that is accessible to the client computer over the network.” Petitioner contends that the serial ID described in Acosta is a “unique number”⁴ stored in memory within camera element 12 (the alleged “video server(s)” of claim 49). *Id.* at 49.⁵ In arguing that the serial ID is “accessible to the client computer,” Petitioner cites to description in Acosta of COVMS 16 listening for broadcasts from camera element 12, the broadcasts including serial IDs. *Id.* at 49–50 (citing Ex. 1005, 17:41–48, Fig. 20 (steps 502, 504)). In contrast to Petitioner’s arguments as to claim 1 (which identify Yonezawa’s network 100 as the network), Petitioner refers to Acosta’s wireless network 14 as the “network” recited in claim 49. *Id.* at 50 (citing Ex. 1004, 7:43–44). According to Petitioner, “Acosta discloses the COVMS 16 accessing the serial ID from camera element 12 over the network.” *Id.*

⁴ We do not reach Patent Owner’s claim construction arguments regarding a “unique number,” as recited in claim 49 (Prelim. Resp. 17–18), or that Acosta’s serial ID is not a unique number (*id.* at 38).

⁵ For the reasons given for claim 1, above, we are not persuaded by Patent Owner’s arguments (Prelim. Resp. 38–39) that the serial ID is not stored on a camera element and, instead, is assigned by COVMS 16 to a communication.

For reasons similar to those given for claim 1, Petitioner does not present evidence sufficient to find that Yonezawa and Acosta teach “the video server(s) including a unique number that is stored in memory within the video server(s) and that *is accessible* to the client computer over the network.” Specifically, Petitioner states, in conclusory fashion, that Acosta discloses “COVMS 16 accessing the serial ID from camera element 12” (Pet. 50) without explaining adequately why simply listening for a broadcast (including a serial ID) from a camera element 12 is a teaching of accessing the serial ID stored in the camera element’s memory over the network. Petitioner cites to Mr. Thompson’s testimony, which, again, merely repeats the Petitioner’s argument verbatim. *Id.* (citing Ex. 1003 ¶ 123). We are not persuaded, by this evidence, that Petitioner is likely to show that the serial ID stored in memory on a camera element 12 is accessible to COVMS 16. On this record, we are not persuaded that Yonezawa and Acosta teach “the video server(s) including a unique number that is stored in memory . . . that *is accessible to the client computer*” over the network, as recited in claim 49.

Moreover, Petitioner has not shown that a skilled artisan would have had reason to combine Yonezawa and Acosta. In explaining why a skilled artisan would have combined Yonezawa and Acosta, Petitioner states that it “would have been obvious to modify Yonezawa’s image receiving software 412 to incorporate the network camera device validation described in Acosta.” Pet. 47. Petitioner argues that a skilled artisan would have done so for the reasons Petitioner gives for claim 1. *Id.* Repeating the Petition verbatim, Mr. Thompson also refers back to his analysis regarding claim 1. Ex. 1003 ¶ 117.

We note above how Petitioner's allegations as to claim 49 differ from those directed to claim 1. Nevertheless, assuming Petitioner proposes combining Yonezawa and Acosta in the same manner, and for the same reasons, as given for claim 1, Petitioner cannot show that claim 49 would have been obvious. As explained above for claim 1, the evidence presented in the Petition is not sufficient to find that a skilled artisan would have combined Yonezawa and Acosta. Accordingly, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claim 49 would have been obvious.

Claims 50–54 depend, directly or indirectly, from claim 49. Petitioner's evidence regarding these claims does not remedy the deficiency in its evidence for claim 49. *See* Pet. 50–60. Accordingly, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 50–54 would have been obvious.

III. CONCLUSION

Petitioner has not established a reasonable likelihood that it would prevail with respect to any of claims 1–10, 23–28, and 49–54. Accordingly, we do not institute an *inter partes* review of the '566 patent.

IV. ORDER

Accordingly, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is not instituted for claims 1–10, 23–28, and 49–54 of U.S. Patent No. 6,891,566 B2.

IPR2016-00568
Patent 6,891,566 B2

PETITIONER:

Steven M. Bauer
Joseph A. Capraro, Jr.
Gerald Worth
Micah Miller
Proskauer Rose LLP
PTABMattersBoston@proskauer.com
jcapraro@proskauer.com
gworth@proskauer.com
mmiller@proskauer.com

PATENT OWNER:

Marc Lorelli
Matthew M. Jakubowski
Adam R. Southworth
Brooks Kushman P.C.
JDSC0109IPR4@brookskushman.com