Trials@uspto.gov
571-272-7822

Paper: 32
Entered: Nov. 7, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

BT AMERICAS INC.,
Patent Owner.

IPR2023-00889
Patent 7,895,641 B2

Before KARL D. EASTHOM, GEORGIANNA W. BRADEN, and SCOTT RAEVSKY, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge*.

DECISION
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 314

I. INTRODUCTION

Palo Alto Networks, Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–25 (the "challenged claims") of U.S. Patent No. 7,895,641 B2 (Ex. 1001, "the '641 patent"). Paper 2 ("Pet."). BT Americas Inc. ("Patent Owner") filed a Preliminary Response along with Paper 6 ("Prelim. Resp."). The parties filed supplemental briefing (Papers 7, 8) to address claim construction issues prior to the Institution Decision (Paper 10, "Inst. Dec.").

After the Institution Decision, Patent Owner filed a Response (Paper 15, "PO Resp."), Petitioner filed a Reply (Paper 20, "Reply"), and Patent Owner filed a Sur-reply (Paper 22). After the briefing, the Board conducted an Oral Hearing and entered a Transcript thereof in the record. Paper 31 ("Tr.").

Petitioner filed a Declaration by Dr. Jeffay in support of its Petition (Ex. 1003) and a subsequent Reply Declaration by Dr. Jeffay in support of its Reply (Ex. 1040). Patent Owner filed a Declaration by Dr. Lee in support of its Preliminary Response (Ex. 2001) and a subsequent Declaration by Dr. Lee in support of its Response (Ex. 2016).

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner demonstrates by a preponderance of evidence that challenged claims 1–25 of the '641 patent are unpatentable.

II. BACKGROUND

A. Real Parties in Interest

Petitioner identifies itself as the real party in interest. Pet. 2. Patent Owner identifies itself and British Telecommunications PLC as real parties in interest. Paper 4 (Patent Owner's Mandatory Notices), 1.

B. Related Proceedings

The parties identify the following district court cases involving the '641 patent: *British Telecommunications PLC v. Fortinet, Inc.*, 1:18-cv-01018-CFC-MPT (D. Del.) and *British Telecommunications PLC and BT Americas, Inc. v. Palo Alto Networks, Inc.*, 1:22-cv-01538 (D. Del.). Pet. 3; Paper 4, 1. The parties also collectively identify as related matters the following *inter partes* review proceedings: IPR2023-00888 (denying institution with respect to U.S. Patent No. 7,159,237 B2); IPR2019-01325 (denying institution with respect to U.S. the '641 patent); and IPR2019-01325 (denying institution with respect to U.S. Patent No. 7,159,237 B2). Pet. 3; Paper 4, 1.

C. The '641 Patent (Ex. 1001)

The '641 patent, "Method and System for Dynamic Network Intrusion Monitoring, Detection and Response," issued on February 22, 2011 with a possible effective filing date of March 16, 2000 (based on a continuation of a patent and a provisional application). Ex. 1001, codes (45), (54), (60), (63). The '641 patent relates to dynamic network intrusion monitoring, detection, and response. Ex. 1001, 1:18–20. The '641 patent discloses that system administrators normally do not have time, ability, or resources to monitor large amounts of constantly-updated audit information, hacking activities, and new attack tactics, tools, and trends. *Id.* at 1:36–41.

According to the ’641 patent, such limitations point to a need for automatic defenses. *Id.* at 1:44–50. Prior art automatic defenses are at a disadvantage against an intelligent attack. *Id.* at 1:51–53.

To address intelligent attacks, the ’641 patent discloses deploying and providing a managed security monitoring service (“MSM service”) that monitors a customer’s network activity using a probe or sentry system. Ex. 1001, 1:59–63. The MSM service first collects status data from monitored components. *Id.* at 1:63. The MSM service then filters or analyzes the collected data for activity that potentially implicates security concerns. *Id.* at 1:63–65. The MSM service further alerts and transmits information about such activity to trained security analysts working at secure operation centers (“SOCs”). *Id.* at 1:65–67. The MSM service guides the security analysts and customer through an appropriate response and optionally, follow-up. *Id.* at 1:67–2:2. The MSM service may accommodate network-specific needs and provide feedback. *Id.* at 2:32–35.

Figure 1 of the ’641 patent is a diagram of the disclosed system and follows:

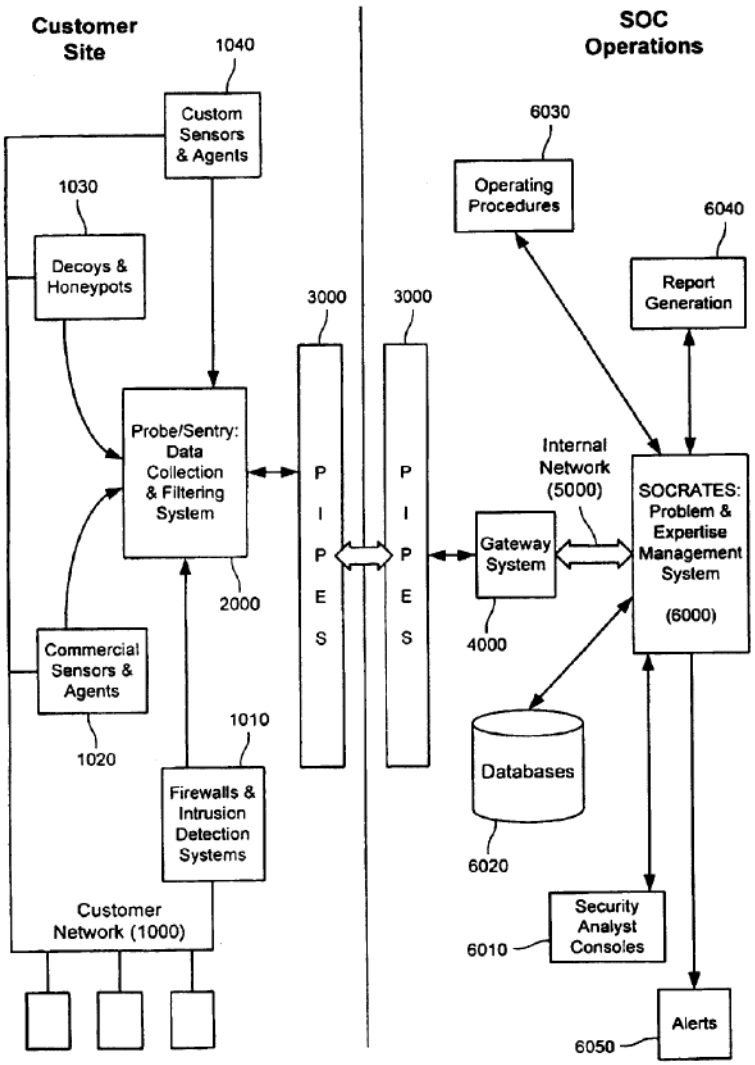


FIG. 1

Figure 1 depicts “an overview of the system architecture of an exemplary embodiment.” Ex. 1001, 3:66–67. Figure 1 illustrates components and systems that operate on the customer site (within the customer’s firewall, on the left), and components and systems that operate within the SOC (within the SOC firewall, on the right). *Id.* at 4:45–49. Pipes 3000 provide an encrypted, secure communications path and message protocol for messages

sent back and forth between probe/sentry system 2000 at the customer site and gateway system 4000 at the SOC. *Id.*at 5:50–54.

Figure 2 of the '641 patent is a diagram of a probe system and follows:

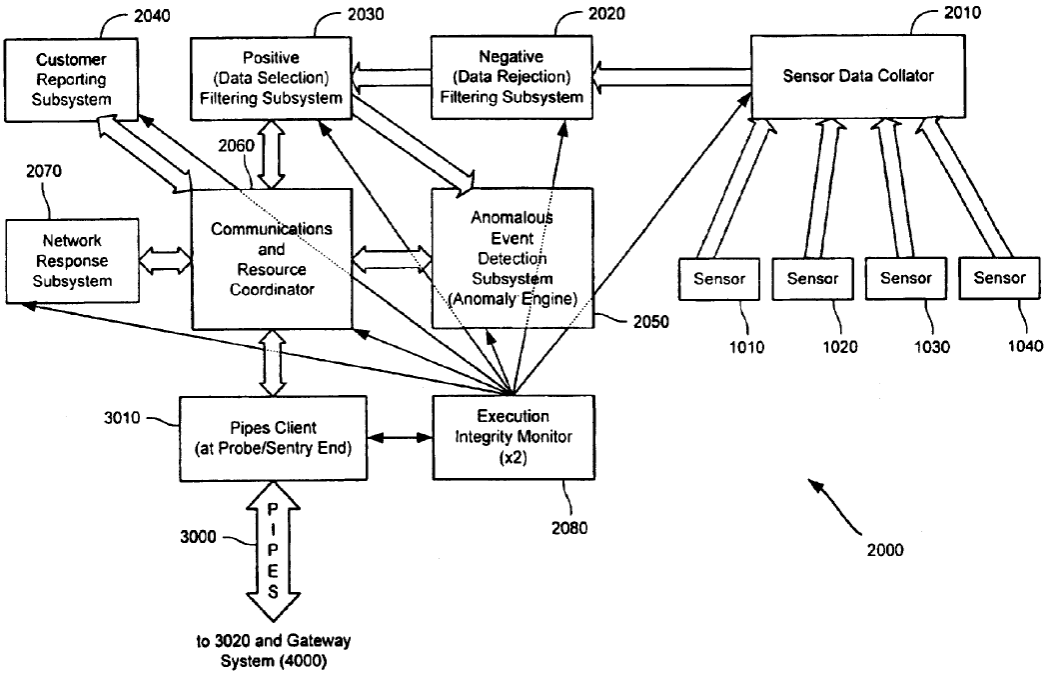


FIG. 2

Figure 2 depicts "a system overview of an exemplary embodiment of a probe/sentry system." Ex. 1001, 4:1–3. Sensors 1010, 1020, 1030, and 1040 collect status data first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then filtered by positive filtering subsystem 2030, which selects potentially interesting information that it forwards to communications and resource coordinator 2060. *Id.* at 8:51–55. Status data that negative filtering subsystem 2020 does not discard and that positive filtering subsystem 2030 does not allow constitutes "residue" that flows to anomaly engine 2050 for further analysis. *Id.* at 8:55–59. Anomaly engine 2050 determines which residue information may be worthy of additional analysis and sends that

residue information to communications and resource coordinator 2060 for forwarding to the SOC. *Id.* at 8:59–62. "Communications and resource coordinator 2060 creates sentry messages out of the interesting status data and forwards those messages on to gateway system 4000 via Pipes 3000." *Id.* at 8:66–9:2.

As part of an SOC, the '641 patent further discloses a Secure Operations Center Responsive Analyst Technical Expertise System ("SOCRATES") for generating "event records" and "problem tickets" for customers experiencing potential security issues that security analysts handle. Ex. 1001, 3:61, 10:11–23. Specifically, "[t]he SOCRATES system is a consolidated system used to manage customers' problems and the supporting data helpful in resolving such problems." *Id.* at 9:56–58. The SOCRATES system "provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools, and installed network components and known vulnerabilities." *Id.* at 9:58–62.

Figure 4 of the '641 patent is a diagram of SOCRATES and follows:

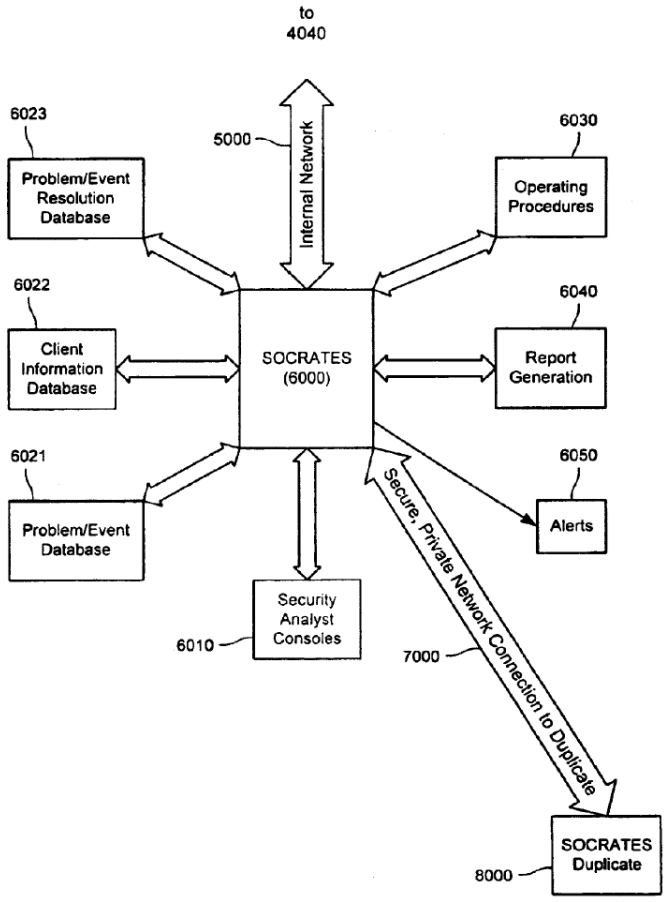


FIG. 4

Figure 4 depicts "a system overview of an exemplary embodiment of a 'SOCRATES' problem and expertise management system." Ex. 1001, 9:54–56. In relation to Figure 4, "[g]ateway messages arrive at SOCRATES 6000 from gateway system 4000 via internal network 5000" and "SOCRATES 6000 first creates from these gateway messages 'event records,' which can be stored in problem/event database 6021." *Id.* at 10:11–16. "Event records may then be linked with other event records stored in problem/event database 6021 and with information from a variety of databases (including customer information from client information database 6022 and problem resolution information from problem/event

resolution database 6023) to form 'problem tickets.'" *Id.* at 10:16–22. The problem tickets "are then opened and displayed on security analyst consoles 6010 to security analysts for handling." *Id.* at 10:22–23.

D. Illustrative Claims 1 and 18

As noted previously, Petitioner challenges claims 1–25 of the '641 patent, of which claims 1 and 18 are independent. Pet. 1; Ex. 1001, 33:25–34:63. Claims 1 and 18 are illustrative of the challenged subject matter and follow:

> 1. A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
>
> a) a sensor coupled to collect status data from at least one monitored component of the network;
>
> b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
>
> c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
>
> d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
>
> e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

> 18. A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:
>
> creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;

correlating the event record with customer information and a symptom record;

using the correlated symptom record to link the event record to problem resolution information;

consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and

providing the problem ticket to a security analyst console for analysis.

E. Asserted Challenges to Patentability and Evidence of Record

Petitioner challenges the patentability of claims 1–25 of the '641 patent based on the following references:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–7, 15–17	103[1]	Duvall[2], Chu[3]
7–13, 16	103	Duvall, Chu, Trcka[4]
14, 15	103	Duvall, Chu, Trcka, Ziese[5]
18–25	103	Duvall, Chu, Cogger[6]

Pet. 6.

F. Claim Construction

A claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA") revised 35 U.S.C. § 103 (effective March 16, 2013). The '237 patent's filing date precedes March 16, 2013. Ex. 1001, code (22). Accordingly, the pre-AIA version of 35 U.S.C. § 103 applies.
[2] US Patent 5,884,033, issued Mar. 16, 1999, filed May 15, 1996. Ex. 1004.
[3] Yang-hua Chu, *Trust Management for the World Wide Web*, M.I.T. (June 13, 1997). Ex. 1005.
[4] US Patent Application Publication No. 2001/0039579 A1, published Nov. 8, 2001, filed May 7, 1997. Ex. 1014.
[5] US Patent 6,484,315 B1, issued Nov. 19, 2002, filed Feb. 1, 1999. Ex. 1015.
[6] US Patent 6,859,783 B2, issued Feb. 22, 2005, filed Sep. 24, 1998. Ex. 1033.

35 U.S.C. [§] 282(b)." 37 C.F.R. § 42.100(b). Under that standard, the "words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

Petitioner asserts that "no claim terms require an explicit construction" and that "the challenged claims are unpatentable under either the ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history, or the district court's previous claim constructions. Pet. 12–13 (citing Ex. 1012 (district court claim construction); Ex. 1013 (same)).

Limitation 1.b recites "a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." Independent claim 18 recites materially the same limitation for purposes of this trial. *Supra* § II.D.

Patent Owner contends that "[a] proper construction of 'post-filtering residue' requires the filtering that creates the 'post-filtering residue' to be distinct from the 'analysis of post-filtering residue.'" PO Resp. 25. According to Patent Owner, "[a]rbitrarily dividing a single filtering subsystem that selects and discards status data cannot satisfy the requirements of limitation 1(b) with respect to 'postfiltering residue.'" *Id.* at 27. In other words, Patent Owner argues that "the analysis of post-filtering residue is a different process than merely selecting or discarding with positive and negative filters." *Id.* Patent Owner adds that "[t]he claims

require this residue to be analyzed further as part of a separate process." *Id.* at 26.

The '641 patent specification and claim language do not support Patent Owner. Limitation 1.b refers to "post-filtering" residue in relation to filtering that occurs prior to arriving at the residue; it does not preclude further filtering of the residue, as we determined preliminarily in the Institution Decision. *See* Inst. Dec. 11–12. Patent Owner agrees: "Respectfully, Patent Owner's 'construction ***does not preclude any filtering in the residue analysis***.'" PO Resp. 26 (quoting Prelim. Resp. 2).

As we also noted in the Institution Decision, the '641 patent specification describes "additional analysis" of "residue information," and implies that "data discrimination analysis," which includes "filtering," is part of such "additional analysis":

> Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC. *Negative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art*.

Inst. Dec. 11 (quoting Ex. 1001, 8:59–65)).

This passage shows that "additional analysis" of "residue information" includes negative and positive filtering. Another passage states that "[p]referably, the system can perform preliminary analysis of the resulting data, either by *simple filtering* . . . or other means to reduce the immense volume of new data into core information worthy of further analysis." Ex. 1001, 3:22–26 (emphasis added).

Therefore, contrary to Patent Owner's arguments, these passages in the '641 patent indicate that the challenged claims allow for further simple

filtering such as negative and positive filtering of data, even though claim 1 also recites positive and negative filtering of status data prior to analysis of the residue data.

Patent Owner also argues that "[a]ny proper construction of 'post-filtering residue' must . . . acknowledge that the filtering of status data (to select or discard status data) is first completed prior to any subsequent analysis, regardless of whether that separate analysis also includes filtering." PO Resp. 29. This argument appears to summarize aspects of limitation 1.b.

As Petitioner shows, claim 1 recites a single filtering subsystem: "*a filtering subsystem coupled to analyze status data* to identify potentially security-related events represented in the status data, *wherein the analysis includes filtering followed by an analysis of post-filtering residue*." Reply 9. Therefore, to the extent the analysis of post-filtering residue is a "separate analysis" from "filtering," which may include selecting (positive filtering) or discarding (negative filtering), the analysis is separate to the extent it occurs at a later time in the same subsystem than the initial "filtering" (as the phrase "filtering followed by an analysis" indicates). *See also* Ex. 1001, Fig 2, 8:51–65 (negative filtering subsystem 2020 first filters data and discards uninteresting data, then positive filtering subsystem 2030 selects interesting information not discarded, then data neither discarded nor selected forms the residue data, which anomaly engine 2050 then analyzes by "well-known" analysis techniques including positive and negative filtering).

In summary, the plain claim language and specification require "analysis of post-filtering residue" to encompass negative and/or positive filtering even if the prior "filtering" also includes negative and positive filtering.

Patent Owner also contends that the parties in prior litigation agreed upon the construction of "post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering" as "status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering." PO Resp. 6 (citing Ex. 1013, 1–4). However, limitation 1.b recites that the "post-filtering residue is data," not "status data," which limitation 1.b introduces earlier ("a filtering subsystem coupled to analyze status data"). In other words, this residue "data" does not refer back to "status data." In any event, even if we were to adopt this construction from the prior litigation, Petitioner shows that it reads on Duvall as modified by Chu, as determined below.

Patent Owner states that "the Board can resolve the controversy in favor of Patent Owner without ever addressing [the prior litigation] constructions." PO Resp. 6. We agree. Apart from our construction of "analysis of post-filtering residue," there is no need to further construe limitation 1.b. We only explicitly construe claim terms "that are in controversy, and only to the extent necessary to resolve the controversy." *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Consequently, we need not explicitly construe limitation 1.b or any other terms and rely on the plain and ordinary meaning of the terms.

G. Principles of Law Regarding Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The obviousness question requires resolving underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence (not here), objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Determining "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue" also helps to resolve the obviousness question. *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result also may weigh in the ultimate determination of obviousness. *See id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

H. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks omitted). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Here, Petitioner asserts a person of ordinary skill in the art at the time of the '641 patent, "would have had a B.S. degree in Computer Science, Computer Engineering, or an equivalent field, as well as at least 2–3 years of academic or industry experience in the design, analysis, and monitoring of computer networks, including issues of network security and network administration, or comparable industry experience." Pet. 11 (citing Ex. 1003 ¶¶ 63–64). Patent Owner does not dispute Petitioner's proposed level of skill. PO Resp. 5.

For the purposes of this Final Written Decision, we adopt Petitioner's level of ordinary skill in the art, because it is consistent with the '641 patent and the prior art of record, except that we delete the qualifier "at least" in the phrase "at least 2–3 years" to eliminate vagueness as to the stated amount of academic or industry experience.

III. ANALYSIS

A. Alleged Obviousness of Claims 1–7 and 15–17 in view of Duvall and Chu

Petitioner contends claims 1–7 and 15–17 would have been obvious to a person of ordinary skill in the art in view of the combined teachings of Duvall and Chu. Pet. 13–49. Patent Owner disputes Petitioner's contentions with respect to independent claim 1 and dependent claims 6 and 15. PO Resp. 6–41.

1. Duvall (Ex. 1004)

Duvall is a U.S. Patent titled "Internet Filtering System for Filtering Data Transferred over the Internet Utilizing Immediate and Deferred Filtering Actions." Ex. 1004, codes (11), (54). Duvall relates to "filtering messages transmitted between the Internet and a client computer." *Id.* at 1:7–8. Duvall discloses a client-based filtering system that compares

portions of incoming and/or outgoing messages with filtering information stored in a filter database to and determine whether to block or allow the incoming and/or outgoing transmissions of messages in response to the comparison. *Id.* at 1:31–35. Duvall explains that in response to a match between certain information in portions of the message and the filtering information, the system can employ one of a number of different specified blocking options, including discarding incoming data, preventing execution of an open command. or replacing parts of received data. *Id.* at 1:35–40.

One embodiment of Duvall, as shown in Figure 1, follows:

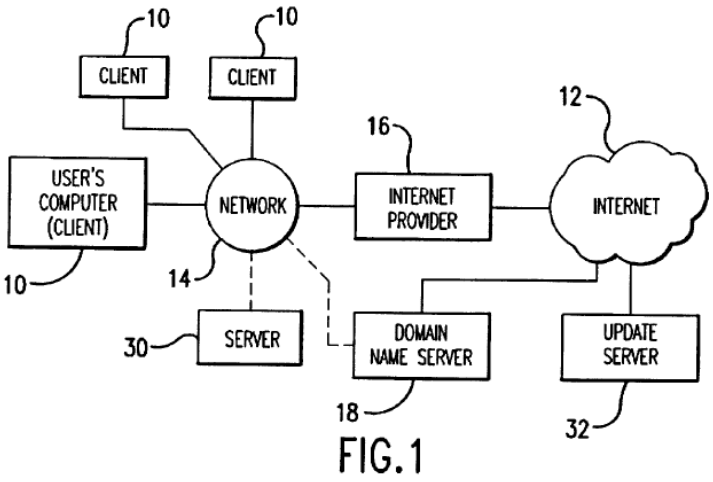


FIG.1

Figure 1 depicts "a block diagram of a network with a client computer for accessing the Internet." Ex. 1004, 2:24–25. The network includes a user with a computer that serves as client computer 10 that communicates with other computers over Internet 12. *Id.* at 2:34–35. According to Internet Protocol version 4, each computer on or connected to the Internet has an IP address that identifies the location of the computer. *Id.* at 2:51–53. Duvall's filter system can filter messages on the basis of IP addresses. *Id.* at 4:5–11, 4:37–39.

Duvall's Figure 2 is a block diagram and follows:

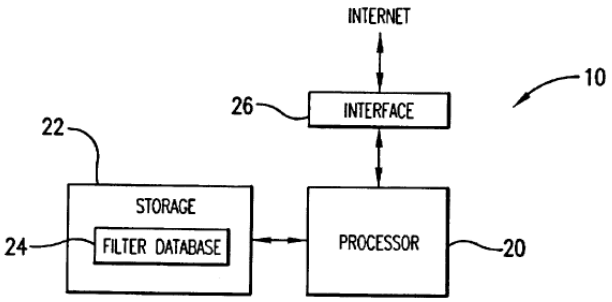


FIG.2

Figure 2 depicts a block diagram of client computer 10 with a filtering system. Ex. 1004, 2:26–27. As shown in Figure 2, "a filtering system resides in client computer 10." *Id.* at 3:43–44. "Processing by the filtering system is carried out by the computer's processor 20, and the system uses the computer's storage 22 to store a filter database 24." *Id.* at 3:44–46. Duvall discloses a related embodiment in which "the filtering system can be provided from a server 30 that is on the client's own network 40." *Id.* at 8:18–21. "This version of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30." *Id.* at 8:23–26.

Duvall discloses a "filter database [that] has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission." Ex. 1004, 3:64–66. "Each filter entry in the filter database also has a field for specifying an action to be taken by the client if that filter were retrieved." *Id.* at 4:12–14. "These actions are essentially divided into two groups, direct action or deferred action." *Id.* at 4:14–15. "Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission." *Id.* at 4:15–17. "If . . . it is determined that no immediate action must be taken,

it is determined whether a deferred action must be taken." *Id.* at 4:65–67. Additionally, a filter can indicate that a deferred action should be taken. *Id.* at 4:65–5:1; 6:19–20.

Duvall discloses filters "stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last." Ex. 1004, 4:27–29. Duvall further discloses, "[i]f there is no deferred action, the system can default to allow the transmission . . . , or it can default to block the transmission." *Id.* at 5:1–3. Deferred filter entries preferably have additional fields, including fields for (1) a keyword, typically a command such as GET; (2) a filter pattern to be compared to data in the message, typically a string of characters; (3) a directional indicator (IN/OUT) for indicating incoming or outgoing transmissions; (4) a compare directive for the type of match; and (5) an action to be taken. typically to allow or block the transmission. *Id.* at 5:8–15.

2. Chu (Ex. 1005)

Chu is a Master's thesis titled "Trust Management for the World Wide Web" submitted to the Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science." Ex. 1005, 3. Chu relates to "trust management . . . in the context of the World Wide Web. *Id.* at 3. For example, Chu discloses sample policies addressing the question of "should I download the active content at this URL." *Id.* at 43–48. Chu discloses policies that employ a "blacklist" and a "whitelist." *Id.* at 44. The blacklist is a list of sites or directories the computer should not download codes from. *Id.* According to Chu, the use of such lists "can be very effective in practice . . . [because] Firewall vendors can compile a blacklist of Web sites that serve potentially dangerous active codes, and place the list in clients' firewalls." *Id.* Chu states that "[t]he blacklist and whitelist ensure good

automation of the trust decision process if the lists are reasonably complete." *Id.* But if the request URL is neither in the blacklist nor the white list, then Chu discloses that the system can return the term "unknown." *Id.*

An example of Chu's policy and description of its code follows:

Policy in English

```
Do not download the code if the URL is served from Harvard or CalTech
Web servers.  Download it automatically if served from MIT.  Prompt me
for my attention otherwise.
```

As the policy description indicates above, Chu's system sends the user an attention prompt to provoke "[u]ser intervention [that] is needed only when the given URL is in neither the blacklist nor the whitelist." Ex. 1005, 44.

3. Analysis of Independent Claim 1

a. "A system for operating a probe as part of a security monitoring system for a computer network"

Petitioner contends that "to the extent the preamble is limiting," Duvall discloses it. Pet. 23. Petitioner reads the preamble onto Duvall's disclosure of "'filtering messages transmitted between the Internet and a client computer' to ensure content that implicates security concerns does not reach recipients." *Id.* at 24 (quoting Ex. 1004, 1:7–24; citing 1:27–29; Ex. 1003 ¶ 113). According to Petitioner, "Duvall's filtering system monitors transmissions for questionable content that should be blocked." *Id.* at 25 (citing Ex. 1004, 3:33–37, 5:8–15, 6:10–42; Ex. 1003 ¶ 119). Petitioner argues that a person of ordinary skill in the art "would have been motivated to block content that may have carried viruses or malware" and that "no modifications would be needed in Duvall's system—domains (e.g., URLs or IP addresses) believed to carry security-implicating content (e.g., viruses) would simply be included in Duvall's blocking filters." *Id.* (citing Ex. 1004, 6:10–27; Ex. 1003 ¶ 119).

Petitioner further contends that Duvall's server 30 is a probe that provides a filtering system. Pet. 25 (citing Ex. 1004, 1:60–64, 8:18–21, Fig. 1; Ex. 1003 ¶¶ 119–20; Ex. 1013 (district court claim construction), 2). According to Petitioner, "Duvall's server 30 collects and analyzes data from other network components to which it is attached, such as clients 10" and that its "filtering system may be part of a firewall." *Id.* at 27–28 (citing Ex. 1004, 1:59–64, 8:21–23).

Patent Owner does not challenge Petitioner's showing regarding the preamble. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

"Whether to treat a preamble term as a claim limitation is determined on the facts of each case in light of the claim as a whole and the invention described in the patent." *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010) (internal quotation marks omitted). "Absent clear reliance on the preamble in the prosecution history, or in situations where it is necessary to provide antecedent basis for the body of the claim, the preamble generally is not limiting." *Symantec Corp. v. Computer Assocs. Int'l, Inc.*, 522 F.3d 1279, 1288 (Fed. Cir. 2008) (internal quotation marks and citation omitted). Additionally, preamble language that merely states the purpose or intended use of an invention generally does not limit the scope of a claim. *See Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345 (Fed. Cir. 2003); *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997). Yet, when the limitations in the body of the claim rely upon or derive essential structure from the preamble, then the preamble acts as a necessary component of the claimed invention and is

limiting. *See Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

A "conclusion that some preamble language is limiting does not imply that other preamble language, or the entire preamble, is limiting." *Cochlear Bone Anchored Sols. AB v. Oticon Med. AB*, 958 F.3d 1348, 1355 (Fed. Cir. 2020); *see also TomTom, Inc. v. Adolph*, 790 F.3d 1315, 1322-23 (Fed. Cir. 2015) (holding the court erred in determining that it had to construe the entire preamble if it construed a portion of it) (citing *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 868 (Fed. Cir. 1985), *overruled in part on other grounds by Nobelpharma AB v. Implant Innovations, Inc.*, 141 F.3d 1059, 1068 (Fed. Cir. 1998) (en banc in part))). Even when a phrase in a preamble provides a necessary structure for a claim, that preamble structure does not necessarily convert the entire preamble into a limitation, particularly one that only states the intended use of the invention. *Cochlear Bone Anchored*, 958 F.3d at 1355.

Based on the entire trial record, we determine that at least part of the preamble is limiting because limitation 1.e recites "the probe," referring to "a probe" in the preamble of claim 1 for antecedent basis. Even if the entirety of the preamble is limiting, as discussed below in connection with a discussion of "security-related events," we determine that Duvall and Chu teach the preamble's "security monitoring system" recitation.

b. "a) a sensor coupled to collect status data from at least one monitored component of the network"

Petitioner contends that Duvall meets limitation 1.a because Duvall's server 30 analyzes (i.e., monitors) status data received from clients 10, which reside on the same network. Pet. 26–29. Specifically, Petitioner argues Duvall's filtering system, which is on a client's network server 30,

"compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken." *Id.* at 29 (quoting Ex. 1004, 4:22–27, citing 2:35–37, 2:42–44, Fig. 1). According to Petitioner, the IP address of a message is "status data" because it is data extracted from network traffic and provides information about the status of the network and its component. *Id.* at 30 (citing Ex. 1004, 4:39–42, 5:66–6:27; Ex. 1013, 1). Petitioner also relies on Duvall's teaching "that information about the data stream can include 'a particular port and IP address' with which a client is attempting to communicate, as well as protocol information, URLs, and associated commands (e.g., an HTTP 'GET command')." *Id.* at 28 (citing Ex.1004, 4:39–42, 5:66–6:27).

As noted below in addressing Patent Owner's arguments related to the status data of limitation 1.b, Patent Owner agrees that IP addresses are status data. *See* Prelim. Resp. 35 ("IP addresses are status data."). Patent Owner does not otherwise challenge Petitioner's showing as to limitation 1.a. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the full record and foregoing discussion, we find that Duvall teaches limitation 1.a.

> *c. "b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering"*

Petitioner contends that Duvall meets claim limitation 1.b. As discussed further below, Duvall discloses the claimed filtering based on comparing an IP address (i.e., "status data") and other information from a message transmission: "When a message is transmitted, whether that

message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken." Pet. 29–30 (quoting Ex. 1004, 4:22–27).

Petitioner generally relies on Duvall's server-based teachings, wherein the server includes the same filter database as Duvall's client. *See* Pet. 30 (citing Ex. 1004, Fig. 2, 8:16–26). Regarding the claim limitation "wherein analysis includes filtering followed by an analysis of post-filtering residue," Petitioner relies on Duvall's teaching that "'[t]he filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last,' where the 'ALLOW' and 'BLOCK' filters are direct action filters." *Id.* (quoting Ex. 1004, 4:27–30; citing Ex. 1003 ¶¶ 126–27). Analyzing Duvall's Figure 3 (see below), Petitioner explains that for the delayed action filters, "immediate action is not required (i.e., data is neither blocked nor allowed at block 104 (i.e., the data is residue data))," and "the data is passed for further analysis." *See id.* at 33–34 (citing Ex. 1004, Fig. 3, 4:50–54). Analyzing Duvall's Figure 3 further, Petitioner reads the claimed "post-filtering residue is data neither discarded nor selected by filtering" onto Duvall's "status data that underwent negative and positive filtering," where Duvall's data "is neither discarded by such negative filtering nor selected by such positive filtering." *Id.* (citing Ex. 1003 ¶ 134).

Petitioner further contends that Duvall teaches "identify[ing] potentially security-related events" because "Duvall's filtering ensures that content implicating security concerns does not reach recipients." Pet. 35 (citing Ex. 1004, 1:7–24; Ex.1003 ¶ 137). Referring to its showing with respect to the preamble, Petitioner contends that "data blocked by Duvall's

filtering system, as well as those not matching any filters, are 'potentially security-related events represented in the status data' because they may relate to requests for, or transmissions of, 'indecent material,' which may be illegal (e.g., 'outlaw[ed]') and/or threaten the security of the requesting user or client device." *Id.* at 35–36 (quoting Ex. 1004, 1:7–24; citing Ex. 1004, 4:61–64 (("[A]dvising the user on how to get back to the state before the user tried to open the stream and send the message.")). Petitioner further argues that the '641 patent does not limit the scope of what "security-related" encompasses, because the '641 patent states that "the present invention is usable generally for [] monitoring of any system." Reply 4 (citing Ex. 1001, 15:63–16:5; Pet. 8).

Petitioner alternatively relies on Chu as teaching determining "potentially security-related events" and suggesting the same in Duvall's system. Pet. 36–37. That is, Petitioner argues that "Chu's blacklists, which contain lists of 'Web sites that serve potentially dangerous active codes,'" suggest the modification. *Id.* at 36 (quoting Ex 1005, 44; citing Ex. 1005, 23 ((discussing virus-ridden downloadable content)). Petitioner relies on Dr. Jeffay's testimony, summarizing his testimony as "explain[ing] that Duvall's and Chu's filtering techniques apply equally well in other security contexts, such as malware or intrusion detection, without needing any modifications." *Id.* (citing Ex. 1003 ¶ 138). In other words, "[f]ilters would include, for example, IP addresses or other criteria (e.g., URLs) associated with malware or potentially security-related content." *Id.* (citing Ex. 1003 ¶ 138). Petitioner contends that "[a]pplying Duvall's techniques in this manner amounts to nothing more than use of known techniques to improve similar devices, methods, or products in the same way (e.g., to detect

malware or a potential intrusion instead of objectionable material)." *Id.* (citing Ex. 1003 ¶ 138; *KSR*, 550 U.S. at 417).

Petitioner also contends that Chu's black and white lists are similar in operation and function to Duvall's BLOCK and ALLOW filters. Pet. 20. Petitioner argues that a person of ordinary skill in the art would have turned to Chu in order to "more accurately resolv[e] residue data to ensure transmissions are correctly blocked or allowed." *Id.* (citing Ex. 1003 ¶ 107). Petitioner also contends that in light of Chu's teachings for a separate analysis (via a user prompt) for data neither allowed nor blocked, a person of ordinary skill in the art "would have recognized that information about data transmissions not matching any of Duvall's filters could be provided to a user with only minor changes to Duvall's overall process." *See id.* at 23 (citing Ex. 1003 ¶ 114), 21 (Chu's policy provides a user prompt for "attention" if the URL is not in a black or white list (reproducing Ex. 1005, 44)).

Patent Owner then contends that Petitioner's expert erred in relying on Duvall's system to identify potentially security-related events. PO Resp. 7–8. Patent Owner contends that "Petitioner's expert only observes a matter of coincidence that, in certain cases, objectionable material may also pose a security risk." *Id.* at 8 (citing Ex 2016 ¶ 35); *accord* Sur-reply 9–10 (similar arguments). Patent Owner also argues that "Petitioner's expert failed to identify any portion of Duvall that discusses computer security, and his testimony made clear that he has no expertise on this issue." *Id.* (citing Ex. 2007, 61:18–62:5, 69:5–8). Patent Owner asserts that Chu does not teach or suggest modifying filters and the motivation proffered by Petitioner is "unrealistic" because, *inter alia*, a "one-off" decision by Chu's user does not suggest such a modification. *See* Sur-reply 11–12.

Patent Owner's arguments do not undermine Petitioner's showing that Duvall and Chu collectively teach identifying "potentially security-related events." The term "potentially security-related events" is broad enough to encompass the objectional material that Duvall monitors and/or those that Chu monitors. Even if objectional material is not "potentially security related" because "non-objectionable material is equally (or even more likely) to raise security concerns" according to Patent Owner, Dr. Jeffay credibly explains that Duvall's and Chu's similar technique for identifying objectionable material identifies potential and virus- and malware-related risks. *See* Ex. 1003 ¶¶ 113–115, 137–138.

For example, the Petition shows that "Chu explains that the user may have 'concerns that prevent her from downloading the game on her machine,' such as '[d]oes this game contain a virus that would erase her hard drive? (security issue).'" Pet. 19 (quoting Ex. 1005, 23). As Petitioner also explains,

> Chu discloses policies addressing the question of "should I download the active content at this URL." EX1005, 43–48. Similar to Duvall, Chu's exemplary policies make use of a "blacklist" (i.e., "sites or directories [the system] should not download codes from") and a "whitelist" (i.e., "sites know[n] to be trustworthy"). *Id.*, 44; EX1003, ¶109. Like Duvall's BLOCK filter, an exemplary Chu policy (shown below) blocks URLs in the blacklist; and like Duvall's ALLOW filter, Chu's policy allows URLs in the whitelist. EX1005, 44; EX1003, ¶109. If a URL is unknown (i.e., it's not in the blacklist or whitelist), the user is prompted for attention. EX1005, 44; EX1003, ¶109.

Pet. 20.

As Petitioner explains, "no modifications would be needed in Duvall's system—domains (e.g., URLs or IP addresses) believed to carry security implicating content (e.g., viruses) would simply be included in Duvall's

blocking filters." Pet. 25 (citing Ex. 1004, 6:10–27; Ex. 1003 ¶ 119). In other words, Petitioner shows that it would have been obvious to include URLs with known or potential malware or viruses in a list of blocked content to ensure security in Duvall's similar system where Duvall's system operates in the materially same way as Chu's system. *See* Pet. 36–37 ("Duvall's and Chu's filtering techniques apply equally well in other security contexts, such as malware or intrusion detection, without needing any modifications," where "[f]ilters would include, for example, IP addresses or other criteria (e.g., URLs) associated with malware or potentially security-related content," and "[a]pplying Duvall's techniques in this manner amounts to nothing more than use of known techniques to improve similar devices, methods, or products in the same way (e.g., to detect malware or a potential intrusion instead of objectionable material)" (citing Ex. 1003 ¶ 138)). Patent Owner's arguments do not address, much less undermine, Petitioner's obviousness showing or Dr. Jeffay's credible testimony supporting the showing as to how and why to implement the combined system based on citations to Duvall and Chu. *See* Ex. 1003 ¶ 138.

As discussed further below in connection with limitation 1.c, Petitioner shows that modifying Duvall's filtering techniques based on Chu's teachings would have improved Duvall's system to include identifying potentially-related security events like viruses or malware by blocking specific IP addresses and/or by further analyzing post-filtering residue data with further keyword and pattern matching search techniques and further using an analyst system as described below in connection with limitation 1.c. *See* Pet. 29–30, 34, 36–40.

Shifting to Duvall's specific system, Patent Owner also contends that Duvall does not teach the "analysis of post-filtering residue" because

Duvall's direct-action filters operate on different data transmissions than those that the deferred-action filters later analyze. *See* PO Resp. 13–14; *see also id.* at 12–25; Sur-reply 12–14 (arguing residue means "left-over" status data). However, as construed above under one interpretation, and as Petitioner argues, claim 1 recites "the post-filtering residue is *data* neither discarded nor selected by filtering," not *status* data, so it need not be part of the same transmission. Moreover, any data as described in the '641 patent and recited in claim 1 that the disclosed filters do not select or discard necessarily is data that is different than the status data that the filters do select or discard. *See* Tr. 44:21–45:1 (Patent Owner agreeing that residue data "doesn't get filtered" prior to becoming residue data).In addition, claim 1 does not refer to "data *transmissions*" or "different data *transmissions*."

In any event, Petitioner shows that Duvall satisfies limitation 1.b even under Patent Owner's claim interpretation. Patent Owner disagrees, arguing that "Petitioner incorrectly presents Figures 3 and 4 as if they were both applied to the same transmission." PO Resp. 13 (citing Pet. 16–19, 32–35). According to Patent Owner, Duvall does not teach that "a single transmission is analyzed according to both processes shown in Figures 3 (direct-action filters) and 4 (deferred-action filters)." *Id.* at 14. Patent Owner bases this argument on the contention that the process shown in Figure 3 applies to transmissions opening a TCP stream, . . . while the process shown in Figure 4 applies to different transmissions sent through the opened stream." *Id.* at 14 (citing Ex. 2016 ¶¶ 83–94). Patent Owner also argues that Petitioner mistakenly treats Duvall as involving transmission of packets. *Id.* at 14–15.

Patent Owner then presents a number of related unavailing arguments based on the unsupported premise that Duvall's Figures 3 and 4 operate on

different transmission streams. PO Resp. 17–25. For example, based on this premise, Patent Owner argues "Duvall clearly does not disclose 'filtering [as described in in Figure 3] followed by an analysis of post-filtering residue [as described in Figure 4], wherein the post-filtering residue is neither discarded nor selected by filtering.'" *Id.* at 25. Patent Owner submits that Duvall's "direct-action filter is never applied to the *same transmission* analyzed by a deferred-action filter," so "Duvall's deferred-action filters cannot analyze 'post filtering residue' as the claimed residue of [the '641 patent] is what is left over after filters have already been applied." *Id.* at 24–25 (emphasis added). Patent Owner contends that "the transmissions in Duvall that are analyzed by the deferred-action filters were never previously filtered, so they could not have been discarded or selected by filtering." *Id.* at 25.

The record does not support Patent Owner's arguments. The filtering subsystem of Duval is remarkably similar to that of the '641 patent. Initially, as noted above, Patent Owner conceded during the Oral Hearing that the '641 patent's residue data "doesn't get filtered" prior to becoming residue data. Tr. 44:21–45:1. Figure 2 of the '641 patent supports this as explained above and further below. Patent Owner's concession during the Oral Hearing contradicts its argument above that Duvall's system must analyze residue data that was "previously filtered" to satisfy the challenged claims.

Moreover, during the Oral Hearing, the Board pressed Patent Owner as to how its disclosed filtering system in the '641 patent differs from Duvall's system. Tr. 46:6–48:5. Patent Owner agreed that the residue data

"doesn't get filtered" prior to becoming residue data. *See id.* at 45:1.[7] Patent Owner ultimately explained that "all the same stuff . . . go[es] through all these filters and get[s] analyzed by the anomalous event detection subsystem or anomaly engine Box 2050, in Figure 2, as one example of volume." Tr. 48:22–25. This argument is beyond the scope of claim 1, because it does not require an anomaly engine or anomalous event detection subsystem. *See* Reply 9–10 ("[C]laim 1 does not recite such an 'anomaly engine,' and it would be 'improper to read a limitation from the specification into the claims.' *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 904 (Fed. Cir. 2004).").

In addition, the '641 patent system clearly creates unfiltered residue data before anomaly engine 2050 analyzes it. *See* Ex. 1001, Fig. 2 (slanted arrow from Positive Filtering Subsystem 2030 to Anomalous Event Detection Subsystem 2050 is residue). Initially, the disclosed probe collects all types of data from at least four sensors 1010, 1020, 1030, and 1040, and then sensor data collator 2010 collates that data and forwards it to resource coordinator 2060. Ex. 1001, 8:47–51. Then, "[d]ata *neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030* form the 'residue,' which is sent to anomaly engine 2050 for further analysis." *Id.* at 8:55–59 (emphasis added).

Moreover, this description does not refer to data forwarded to resource coordinator 2060 as a single transmission of data or residue data. Ex. 1001, 8:47–59. Rather, the data forwarded from the different probes is at most collated into a bulk of data from different sensors and sent to the

[7] Petitioner also agreed. *See* Tr. 11:8–12:25 ("The post-filtered residue doesn't require that data actually be discarded or actually be selected.").

resource coordinator, some of which ultimately may or may not culminate in residue data or residue status data. *See id.* at 8:47–51.[8] The data that negative filter 2020 discards or other data that positive data 2030 accepts is filtered data, and what is left is residue data (i.e., unfiltered data). The '641 patent's filters simply match words or phrases or an IP address in the data (status data), like the direct action filters in Duvall's system. *Compare* Ex. 1001, Fig. 1, *with* Reply 10 (Duvall's filtering operations are based on "the IP address and/or other information in the data stream." (quoting Ex. 1004, 4:23–28)); Pet. 29–30; Ex. 1004, 4:23–28 ("When a message is transmitted, whether that message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some [direct] action needs to be taken."). Then, in Duvall's system, like the '641 patent, an IP address in a single message that the direct action filters do not match is the residue data, which each system later analyzes (e.g., filters). "In other words, both direct- and deferred-action filters are searched for the same message transmitted through the filters checked at step 102–104 data stream." *See* Reply 7–8 (citing Ex. 1040 ¶ 11); Ex. 1004, Figs. 3–4.

Simply put, in both the '641 patent and in Duvall, the residue data is *unfiltered* (unmatched) data and is ultimately different data than the *filtered discarded* (matched) data and *allowed* (matched)) data, but the residue data is the same (i.e., in the same message and same transmission) when the direct action filters do not initially match it so that it becomes residue data (for later filtering/matching and/or analysis).

[8] This passage does not refer to residue data.

In any event, as Petitioner shows, like the '641 patent's probe, Duvall's probe operates on residue data that the system neither discards with negative filtering nor accepts with positive filtering—i.e., status data that the probe does not actually filter with negative or positive filters (initially) but status data that is in the same bulk of data as the filtered status data. *See* Pet. 31–35; Reply 7–8 ("In other words, both direct- and deferred-action filters are searched for the same message transmitted through the Filters checked at step 102-104 data stream." (citing Ex. 1040 ¶ 11)).

Drilling down further, as Petitioner shows, Duvall's Figures 3 and 4 "are part of the *same* process, which only executes *after* determining that a data stream in opened." Duvall's Figure 3, as annotated by Petitioner, follows:

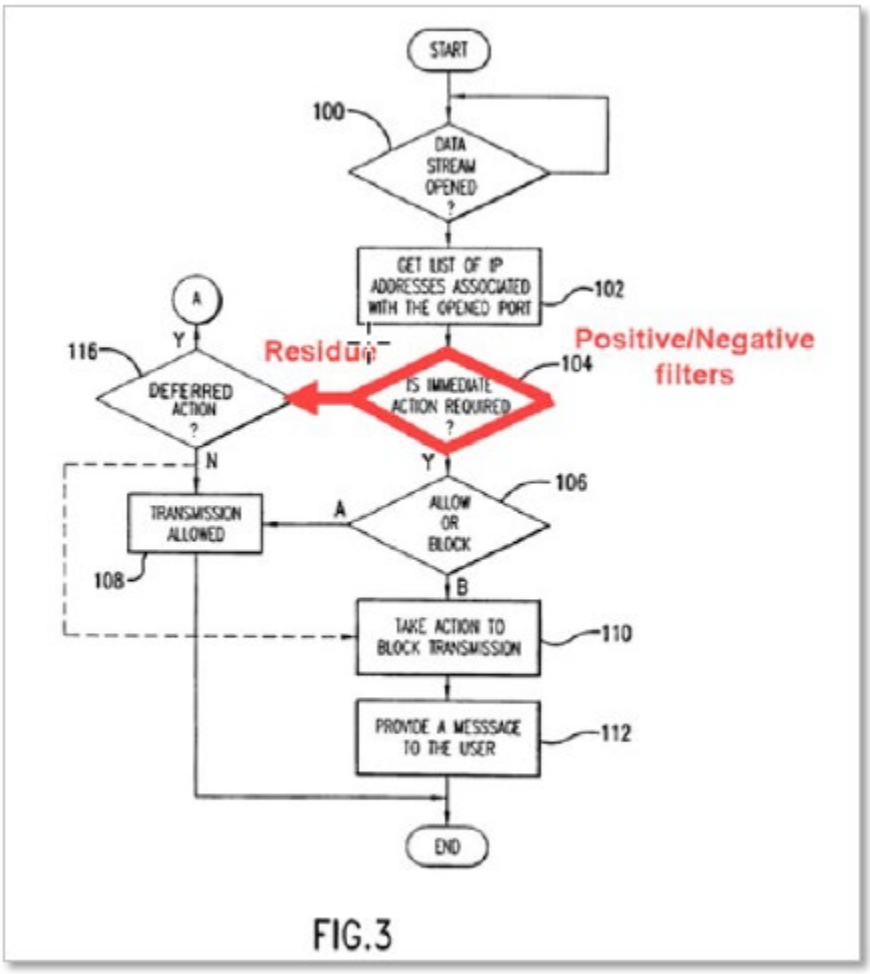


FIG.3

Figure 3, as annotated by Petitioner, shows that Duvall's system first determines if the data stream is open at step 100, and then if so, the process determines if the status data requires direct action in step 104 and if so, the process either applies direct action filters to the data transmission in step 106 or applies deferred action filters to the residue data of that same stream in step 116. *See* Reply 7–8 (citing Ex. 1004, 4:48–55, 4:65–5:1). As Petitioner explains, after the process opens a data stream in Figure 3 and applies direct-action (positive or negative filters), Figure 4 signifies a process to apply deferred-action filters to the residue data of the same transmission stream after step 116 at A in a separate analysis. *See* Reply 9; Pet. 31–35 (relying on Ex. 1004, Fig. 4). That is, Figure 3 joins Figure 4 at junction A of both

figures. *Compare* Ex. 1001, Fig. 3 (A at step 116), *with* Ex. 1001, Fig. 4 (junction A step at step 130).

Petitioner's annotated version of Duvall's Figure 4 follows (Pet. 35):

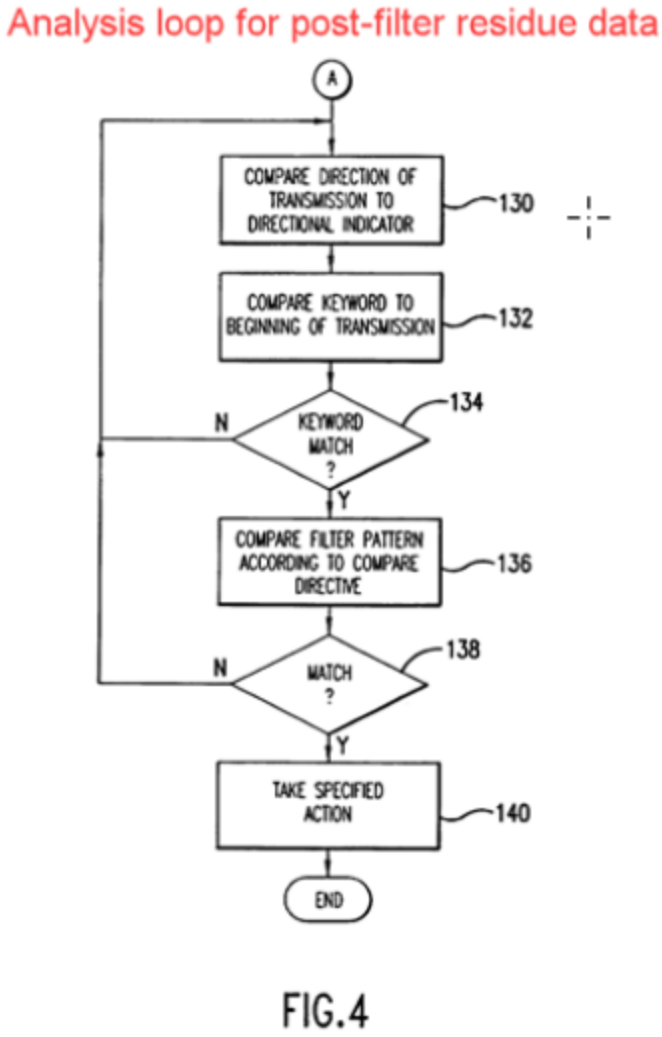


FIG.4

EX1004, FIG. 4 (annotated).

Figure 4 is a flow diagram of Duvall's filtering process that continues after opening the connection at Figure 3's steps 100, 102 and proceeds to junction A at Figure 3's step 116 to junction A at Figure 4's step 116 above. As Petitioner's annotation shows (red), Figure 4 represents an analysis of

post-filter residue data of transmissions in open connections where Figure 3 represents the filtering process before and after opening the connection. This clear showing of the continuing process of Figures 3 and 4 at junction A contradicts Patent Owner's arguments and Dr. Lee's testimony that the two figures represent analysis of different transmission streams, as Dr. Jeffay credibly testifies. *Compare* Ex. 2016 ¶¶ 83–85 (concluding that Duvall's "Figures 3 and 4 do not operate on the same transmissions), *with* Ex. 1040 ¶¶10–11 (testifying that Figures 3 and 4 "expressly show that both direct- and deferred-action filters are searched for the same message transmitted through the data stream, shown by steps 104, 106, and 116, highlighted above" (annotating Ex. 1004, Fig. 4; citing Ex. 1004, 4:48–50, 4:65–5:1), ¶ 12 ("Duvall still discloses that its process depicted in Figures 3 and 4 evaluates messages transmitted through opened data streams against both direct- and deferred-action filters")). As Dr. Jeffay notes in support of his characterization of Figures 3 and 4, Duvall specifically states that

> *[w]hen a message is transmitted*, whether that message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken. *The filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last, and takes action based on the first matched filter*.

Ex. 1040 ¶ 11 (quoting Ex. 1004, 4:23–47). That is, contrary to Patent Owners arguments and Dr. Lee's testimony, a transmission goes to "ALLOW filters first, BLOCK filters next, and deferred actions last (as residue data)," which Figures 3 and 4 show occurs for an open stream. *See* Ex. 1004, 4:26–27, Figs. 3, 4.

In particular, as Petitioner similarly explains with respect to Figure 3,

> If immediate action is not required (i.e., data is neither blocked nor allowed at block 104 (i.e., the data is residue data)), the data is passed for further analysis. This residue data is status data that underwent negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering—i.e., "post-filtering residue." EX1003, ¶134.

Then, as Petitioner similarly explains with respect to Figure 4,

> This "post-filtering residue" is subject to analysis by Duvall's deferred action filters. EX1004, 4:27–30 ("The filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last, and takes action based on the first matched filter."); 4:65–5:7. *This post-filtering residue analysis includes keyword and pattern matching, as depicted in FIG. 4*. *Id.* at 5:8–29; EX1003, ¶135.

Pet. 34 (emphasis added). This analysis further demonstrates that Figures 3 and 4 filter the same message transmission, as Dr. Jeffay testifies.

Contrary to Patent Owner's arguments that Duvall's system does not filter status data (PO Resp. 29–30), as Petitioner argues, Duvall's system filters "the IP address and/or other information in the data stream." Reply 11 (quoting Ex. 1004, 4:23–28; citing Pet. 29–30). In other words, as Petitioner shows, Duvall's filters at Figure 3 (direct action) and Figure 4 (deferred action) essentially perform keyword and pattern matching on information in the same data stream that includes status data such as the IP address. *See* Reply 10; Pet. 29–30, 34; Ex. 1004, 4:23–28; Ex. 1003 ¶ 135.

As Petitioner further shows, "Duvall analyzes other forms of "status data" in addition to IP addresses. These other forms of 'status data[]' . . . include 'protocol information, URLs, and associated commands (e.g., an HTTP 'GET command')."" Reply 12 (citing Pet. 28–29; Ex. 1004, 4:39–42, 5:66–6:27; Ex. 1003 ¶ 123).

As noted above, Patent Owner agrees that "IP addresses are status data." Prelim. Resp. 35. Similarly, as Petitioner shows, Patent Owner's declarant in a related IPR trial involving the '641 testified that Table 6 of the '641 patent lists types of status data information. *See* Reply 11 (citing Ex. 1048 ¶¶ 65–66). Table 6 includes IP addresses. Ex. 1001, App'x B (Table 6). Petitioner also cites prior litigation that shows that a magistrate in a related case involving the '641 patent and a related patent found that the parties agreed that Table 6 includes status data. *See* Reply 11 (citing Ex. 1034, 13 n. 37); Ex. 1034, 13 ("Based on the evidence presented, the court finds BT did not unambiguously disclaim IP addresses as 'status data.'").

The record also does not support Patent Owner's implied argument based on its claim interpretation that Duvall's post-filtering analysis is not a "distinct" analysis from that of the direct action filters (which create the post-filtering residue). *See* PO Resp. 25 (arguing that "[a] proper construction of 'post-filtering residue' requires the filtering that creates the 'post-filtering residue' to be distinct from the 'analysis of post-filtering residue'"); Sur-reply 16–19 (similar argument). As Petitioner shows and as outlined above, even if this claim interpretation is correct,

> Duvall includes direct-action filters, Pet., 29–31 (relying primarily on Duvall's Figure 3), which filter status data, and deferred-action filters, which analyze the post-filtering residue, *id.* at 31–35 (relying primarily on Duvall's Figure 4). Clear from Figures 3 and 4, *Duvall's deferred-action filters are not a continuation of the direct-action filters but come afterwards as their own discrete set of analyses*.

Reply 10 (emphasis added).

Patent Owner advances similar unavailing arguments that are materially similar to the argument addressed above but stated in another

way. *See* PO Resp. 25–29. For example, Patent Owner argues that "there is no basis for artificially breaking Duvall's system in half to suggest that only certain block/allow filters in Duvall's filtering subsystem select and discard, while the other filters (which also block and allow) are performing a distinct analysis." PO Resp. 28. The record does not support this argument. As set forth above and as Petitioner shows, Duvall's system performs a distinct analysis on residue status data in the same message in a transmission after not blocking and not allowing a message in that transmission, or after blocking or allowing other status data in the bulk data stream. Even if part of the residue analysis involves the same types of positive or negative filters as the allowed or blocked data, claim 1 does not preclude using the same or similar filters for analysis of status data in different stages of the filtering process. And as Petitioner shows, Duvall's system performs other analysis on the residue status data, using deferred action filters, which involves keyword and pattern matching, as Figure 4 shows. *See* Pet. 33–34 (citing Ex. 1004, 4:27–30; 4:65–5:29, Fig. 4; Ex. 1003 ¶ 135).

Patent Owner's argument that Duvall's system does not operate on packets also does not undermine Petitioner's showing. PO Resp. 21–23 ("Petitioner is relying on an imaginary implementation of Duvall . . . that performs deep packet inspection to filter packets rather than the application-level transmissions as actually disclosed."). Patent Owner presents a number of unavailing arguments related to Duvall's patching code as it relates to packets and/or opening TCP/IP sockets. But as Petitioner argues, this line of argument is irrelevant to the claim language, because claim 1 recites "residue data" and "data" and neither requires nor precludes packet analysis. *See* Reply 8–9. Moreover, to the extent relevant, Petitioner shows that Duvall's TCP/IP process analyzes messages in the form of "network

packets [that] include application-level data (e.g., message content)." *Id.* (citing Ex. 1004, 2:42–44; Ex. 1040 ¶¶ 13–15). Patent Owner agrees with Dr. Jeffay that Duvall's system analyzes multiple packets of a message. PO Resp. 23–24 ("As Petitioner's expert recognized, the deferred action filter's keyword and filter pattern analysis would need to be conducted 'over multiple packets' rather than just individual packets." (citing Ex. 2007, 107:17–19; Ex. 1004, 6:10–27, 5:66–67)).

Patent Owner also argues that "it would not make technical sense to force Duvall's direct-action filters to apply to packets in an already opened stream," where "matching keywords (cf. Fig. 4, 134) and filter patterns (cf. Fig. 4, 136) would be entirely pointless because there is no payload to match against." *Id.* at 24 (citing Ex. 2016 ¶ 105). But Patent Owner agrees with Dr. Jeffay that a "single HTTP transmission may require multiple packets to send the data over the network." *Id.* at 24 (citing 2016 ¶ 103). Patent Owner also notes that "Duvall's direct-action filters can already filter based on an IP address and port and Petitioner's own expert admits that the 'connection establishment packet does not have a payload.'" *Id.* at 23–24 (citing Ex. 2007, 94:15–16; Ex. 2016 ¶ 104).

These arguments do not undermine Petitioner's showing. As discussed above, Duvall's Figure 3 contradicts Patent Owner's arguments, because it clearly shows applying direct action filters to an open stream. As Petitioner explains, even if Duvall describes using direct action filters as a way to open a stream in some embodiments (or under some circumstances), Duvall clearly shows applying direct action filters to an open stream. *See* Reply 8 ("That Duvall discloses one way to block transmissions by 'not executing the open command,' EX1004, 4:56–58, does not negate Duvall's disclosed process for evaluating messages transmitted through opened data

streams. EX1040, ¶12.”). That is, with respect to Figure 3, Duvall states that after the “filtering system detects when the client opens the stream for a particular port and IP address (step 100),” it “searches the filter database for matching filters” that have the IP addresses associated with “meta value ANY PORT and also with the particular opened port (step 102).” Ex. 1004, 4:39–46. Then the filtering system “retrieves any filters that match the particular IP address,” and checks those “to determine if any require immediate action. i.e., if unconditional allowing or blocking is required (steps 104, 106).” *Id.* at 4:46–50. Duvall’s system then processes residue status data as outlined above with respect to Figure 4 and as Petitioner shows. And as Dr. Jeffay credibly testifies, Figures 3 and 4 operate on the same transmission with Duvall’s TCP/IP messages transmitted as “IP datagrams,” “often referred to simply as ‘packets’,” which include “‘application-level’ data (e.g., message content) that Dr. Lee attempts to distinguish,” so that Patent Owner’s arguments and Dr. Lee’s testimony that Dr. Jeffay advances an alleged “deep packet inspection” theory are unavailing. *See* Ex. 1040 ¶ 14 (citing Ex. 1047, 1–2; Ex. 2016 ¶ 96).

Moreover, regarding Patent Owner’s relied-upon blocking action, Duvall shows it is merely a preferred embodiment: “When blocking is done on the basis of the IP address of the outgoing message, such blocking is *preferably* accomplished by simply not executing the open command.” Ex. 1004, 4:56–58. Patent Owner relies on this statement in an effort to effectively delete the passages quoted above that describe the general operation of filtering an open stream via Figures 3 and 4. As Petitioner essentially argues and as Dr. Lee testifies, this disclosed preference in Duvall as one way to block an outgoing message does not eliminate what Figures 3 and 4 generally teach as outlined above, contrary to the testimony

of Dr. Lee that Duvall's Figures 3 and 4 do not operate on the same message. *See* Reply 8; Ex. 2016 ¶ 12 ("Although Duvall discloses one way to block transmissions by 'not executing the open command,' Duvall still discloses that its process depicted in Figures 3 and 4 evaluates messages transmitted through opened data streams against both direct- and deferred-action filters." (quoting Ex. 1004, 4:56–58; citing Ex. 1004, 4:23–37, 4:48–50, 4:65–5:1)).

Even if, as Patent Owner argues, Duvall's system blocks all unwanted messages by using a blocking filter and not executing the open command, as described above, the system still allows some status data messages in a data stream that it does not block by filtering and it creates residue data on other status data in the same open stream. Claim 1 does not require the system to block status data and also allow status data by filtering. Rather it recites "the analysis includes filtering [that may simply allow some status data] followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." Therefore, Duvall's system satisfies claim 1 even if Patent Owner is correct in characterizing Duvall's filter system as always using blocking filters on unwanted IP addresses to facilitate the next step of not opening a connection.

Based on the full record, we find that Duvall teaches limitation 1.b.

d. "c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system"

Petitioner contends that Duvall and Chu collectively teach limitation 1.c. According to Petitioner, a person of ordinary skill in the art would have looked to Chu to optimize the handling of unresolved residue data in order to avoid "filtering too much or too little" in Duvall." Pet 37 (citing Ex. 1004,

8:6–8; Ex. 1003 ¶¶ 140–141). Petition argues that "[i]n the case of unresolved data, Chu prompts for human intervention," which "would take the form of an analyst system having people trained to manage Duvall's corporate network." *Id.* at 37–38 (citing Ex. 1004, 8:18–23; Ex. 1005, 44 ("Prompt me for my attention"); Ex. 1003 ¶ 137).[9]

Petition further argues that Duvall's use of a "***uniform set of filters for many users***" for "a corporate network" suggests that "the decision of how to handle unresolved data would not be left to each user individually, but rather, to a group of people trained in making such decisions, such as analysts at a network-security service." Pet. 39 (quoting Ex. 1004, 8:18–23; citing Ex. 1003 ¶¶ 138–139). Petitioner also asserts that Duvall discloses a "password protected" "editing manager," which suggests that persons editing filters in a corporate network are trained professionals. *Id.* at 38 (quoting Ex. 1004, 8:8–10; citing Ex. 1003 ¶ 139). Therefore, Petitioner contends that "in the Duvall-Chu combination, information about the unresolved residue data would be sent to a trained network analyst for handling of the unresolved residue data." *Id.* at 39–40.

Petitioner further explains that "[t]his group of trained professionals responsible for maintaining uniformity of the filters is 'an analyst system . . . associated with said security monitoring system,'" and a person of ordinary

[9] Patent Owner contends that an "'analyst system' denotes a technological system that is used by analysts." PO Resp. 31. Patent Owner also contends that "[t]he use of the term 'analyst system' in [] claim [1] refers to a technological system capable of assisting an analyst in his role." *Id.* at 31–32. It is not necessary to decide if an "analyst system" requires human intervention because even if it does, based on Petitioner's showing, we find that Duvall discloses it or determine that it would have been obvious over Duvall and Chu.

skill "would have been motivated to assign the role of managing and editing filters to a group of people having the expertise to properly evaluate whether 'the filtering system is filtering too much or too little,' rather than the individual receiving the illicit content." Pet. 39–40 (quoting Ex. 1004, 8:6–8; Ex. 1003 ¶ 144).

Dr. Jeffay supports Petitioner by citing to several prior art analyst systems that suggest similar systems would have been advantageous in Duvall's system: "[T]he responsibility for editing the filters in a corporate network would have been advantageously outsourced to a third-party network-security service because each individual corporation would not likely be able to staff and maintain its own center of network security competency." Ex. 1003 ¶ 142 (citing Ex. 1037, 224 (explaining that IBM previously provided an outsourced network-security service); Ex. 1038, 1:49–60 (explaining that "network management systems," like Duvall's "editing manager," "collect[ ] large volumes of information); Ex. 1039, 2:16–20 (explaining that "network management systems," like Duvall's "editing manager," "typically operated by collecting large volumes of information which then required evaluation by . . . a highly-skilled network administrator")); Pet. 38 (citing Ex. 1003 ¶ 142).

Patent Owner argues that Petitioner fails to show that the combination of Duvall and Chu teaches an analyst system. PO Resp. 33; Sur-reply 19–20 (also alleging Chu "leads away from an analyst system—and even an analyst" by allowing a single "end-user to make an individualized trust decision"). Patent Owner maintains that "[e]ven if Petitioner could show that Duvall-Chu included a group of analysts, there is still no disclosure of any analyst system used by those analysts." PO Resp. 34. Patent Owner also argues that "neither Duvall nor Chu even discloses a system that could

receive transmissions (*i.e.*, prompt) sent from Duvall's probe." *Id.* (citing Ex. 2016 ¶ 129). Patent Owner then contends that "Duvall's editing manager is only capable of editing filters using known database techniques," and "Chu merely displays a prompt on the device of the same user attempting to download the file," which is not an analyst system. *Id.* at 35 (citing Ex 1004, 8:11–12; Ex. 1005, 44). Patent Owner further argues that "Petitioner's expert [does not] explain why it would be obvious to add an analyst system to Duvall-Chu, or how it could even be accomplished." *Id.* at 34; *see also id.* at 11 (similar arguments, arguing "Chu only prompts the same user that was originally trying to download the file").

Patent Owner also argues that Dr. Jeffay improperly relies on prior art to show that analyst systems employing outsourcing were well known and obvious to implement in Duvall-Chu's system. *See* PO Resp. 34 (citing Ex. 1037). According to Patent Owner, "[t]he mere fact that outsourcing is possible does not mean that it would be either obvious or inherent to incorporate such undisclosed systems (presumably used by third-party analysts) into Duvall-Chu," and Exhibit 1037 "provides no actual disclosure of how such outsourcing was accomplished, nor any disclosure of the systems used by the third parties." *Id.* (citing Ex. 1037; Ex. 2016 ¶¶ 127, 129).

Patent Owner's arguments based on Dr. Lee's similar testimony are unavailing. Patent Owner largely attacks Duvall and Chu separately without addressing Petitioner's showing based on the combined teachings of the references and the knowledge of an artisan of ordinary skill. *See* PO Resp. 33–35 (citing Ex. 2016 ¶¶ 127, 129).

As Petitioner argues, "in the Duvall-Chu combination, information about the residue data would be sent to an analyst system having trained

professionals for handling the unresolved residue data," which would reduce the chance of the system "filter[ing] too much or too little." Reply 13 (citing Pet. 38–39; Ex. 1003 ¶¶ 142–143). As outlined above, the Petition shows that in addition to Duvall's "password protected" "editing manager" for editing filters by an analyst, Duvall also describes "a corporate network" having "a uniform set of filters for many users," thereby suggesting that in light of Chu's teaching of providing feedback about residue data to a human operator (analyst), the combination suggests that "information about the residue data would be sent to an analyst system having trained professionals for handling the unresolved residue data." Pet. 38–39 (quoting Ex. 1004, 8:8–9; citing Ex. 1004, 18–23; Ex. 1003 ¶ 142). Petitioner also shows that Duvall's editing manager and filtering system is part of the claimed probe, which further shows the relied-upon analyst system is capable of receiving residue and other information at the probe. *See id.* at 40 (citing Ex. 1004, 8:2–5, 8:18–21; Ex. 1003 ¶ 148). Neither Patent Owner nor Dr. Lee addresses Petitioner's specific showing, which is persuasive. *See* PO Resp. 31–35, Ex. 2016 ¶¶ 122–133.

Petitioner also notes that Dr. Jeffay "explains that Duvall already discloses the hardware required to receive information about data transmissions." Reply 13 (citing Ex. 1003 ¶ 114 ("Duvall already suggests reviewing system activity to determine whether "the system is filtering too much or too little," and further "provides a screen on the user's display" for viewing information about data transmissions." (quoting Ex. 1004, 4:61–64, 8:5–7; Pet. 22–23)); *see also* Pet. 38 ((Duvall's "editing Manager" "allows the user to make custom changes [to the filters] if the user believes that the filtering system is filtering too much or too little."(quoting Ex. 1004, 8:3–10). Accordingly, as Petitioner shows, and artisan of ordinary skill "would

have recognized that modifying Duvall's system to provide information to a user about data transmissions not matching any of Duvall's filters would require only minor changes to Duvall's overall process." Reply 13 (quoting Ex. 1003 ¶ 114).

Dr. Jeffay's testimony, including citations to prior art analyst systems, supports Petitioner's showing that such analyst systems would have involved minimal modifications to Duvall's system with well-known security system techniques providing the advantage of trained security analysts to analyze data, including large volumes thereof, to resolve residue data as suggested by Chu. *See, e.g.,* Pet. 38 (citing Ex. 1003 ¶ 142); Ex. 1003 ¶ 114 (implementing human intervention as Chu suggests would have involved incorporating known techniques and minor changes to Duvall's overall process), ¶ 142 (analyst systems provide expert analysis on large volumes of data (citing Ex. 1037, 224; Ex. 1038, 1:49–60; Ex. 1039, 2:16–20)). As Petitioner argues, a person of ordinary skill readily "would have understood how to use third-party security-monitoring services," where in addition to the above examples of prior art analyst systems, "the 1997 NetRanger User's Guide provides a detailed communications architecture in which a 'Director provides monitoring and analysis services to NetRanger, and communicates . . . via the communication system.'" Reply 14 (quoting Ex. 1049, 021).

Dr. Jeffay credibly supports Petitioner, contrary to Dr. Lee's testimony that it would not have been obvious to implement such a system, because, *inter alia*, "EX1037 provides no actual disclosure of how such outsourcing was accomplished, nor any disclosure of the systems used by the third-party." Ex. 2016 ¶ 128. Specifically, Dr. Jeffay credibly testifies that a person of ordinary skill in the art

> would have understood how to use third-party security-monitoring services, including, for example, how to transmit data to the third-party service for analyst review and response. The 1997 NetRanger User's Guide, for example, provides a detailed communications architecture in which a "Director provides monitoring and analysis services to NetRanger, and communicates . . . via the communication system." EX1049, 021; *see also id.*, 020 ("The NSX is the sensing and management component of the NetRanger System that resides on a corporate network. It communicates with one or more remote Director systems via the Post Office network communications system.").

Ex. 1040 ¶ 17. In other words, as Dr. Jeffay's testimony implies, Dr. Lee takes an overly narrow view of how an artisan of ordinary skill would have interpreted documents describing well-known third-party security systems, including how to implement them in other security monitoring systems such as Duvall-Chu.

Contrary to Patent Owner's argument that Chu allows the user to avoid security by choosing to access sites with malware, Petitioner persuasively explains that "a POSA would have been motivated to assign the role of managing and editing filters to a group of people having the expertise to properly evaluate whether 'the filtering system is filtering too much or too little,' *rather than the individual receiving the illicit content*." Pet. 39 (quoting Ex. 1004, 8:6–8; citing Ex. 1003 ¶ 144) (emphasis added).

Patent Owner acknowledges that Chu's system "alerts the end-user of the lack of any determination." Prelim. Resp. 45–46. Patent Owner similarly acknowledges that Chu's "'user intervention' teaches prompting the end-user for attention at the original application." *Id.* at 46. Chu's alert system provides information to a user about an identified problem, thereby further suggesting feedback with respect to Duvall's filtering analysts using an editing function on a corporate network. *See* Ex. 1004, 8:1–25, Ex. 1005,

44. And as noted above, Duvall's system explicitly provides feedback regarding blocked messages to a user's screen. Ex. 1004, 6:62–65.

Specifically, this alert informs the user/analyst system as suggested by the combination of Duvall and Chu that the previous filtering operations (ALLOW/BLOCK in Duvall or white list/black list in Chu) are unable to render a decision regarding a specific website, thereby suggesting further analysis as occurs in Duvall's system and raising the issue of whether that website is potentially unsafe, as Petitioner argues. *See* Pet. 37–40.

Patent Owner also argues that "Duvall explicitly discloses that a 'user [can] make custom changes' using the editing manager to resolve that very problem" of "filtering too much or too little." PO Resp. 9 (alteration in original) (quoting Ex. 1004, 8:6–7). Therefore, according to Patent Owner, there is no reason "why a POSA would be motivated to look for Chu," where Dr. Jeffay testified during cross-examination that "nothing more is needed" in Duvall's system. *Id.* (quoting Ex. 2007, 133:10–22).[10] This line of argument appears to admit that Duvall already discloses an analyst system (e.g., a system with human intervention according to Patent Owner).

The record also does not support Patent Owner's argument that the Reply raises a new untimely argument by focusing on "*when*" to modify

[10] As we noted in the Oral Hearing, Patent Owner's cross-examination of Dr. Jeffay assumes at the outset of the questioning that Duvall's system includes an analyst. *Compare* PO Resp. 9 (quoting Ex. 2007, 133:17–22), *with id.* at 133:1–5 (Patent Owner setting the parameters of the questioning of Dr. Jeffay at the outset, as follows: "Okay. Could the person who is authorized to adjust the filters see what content is allowed and blocked and use the editing manager to tune the filters?"), and Tr. 33:19–35:15 (The Board noting and asking as follows: "So your [deposition] question already pre-supposes there's a person there. So if there's a person in Duvall, maybe you don't need a person, another person?").

Duvall's system. *See* Sur-reply 7–8. This argument is semantical. Patent Owner's related arguments characterizing the Petition's motivation as faulty also do not undermine the Petition because they fail to address Petitioner's full showing and mischaracterize it. *See id.* at 8–12. As outlined above, the Petition relies on Chu as further suggesting to decide if or when to modify Duvall's system so that the system does not ultimately filter too much or too little, thereby improving the filter system by using a group of analysts to obtain a uniform decision with respect to a corporation's filters as to a security/trust decision.

In other words, Patent Owner's arguments do not undermine Petitioner's showing that an artisan of ordinary skill would have looked to Chu's similar system to address similar problems and to address security issues with human intervention such as malware, as outlined above. *See* Pet. 19–23. As Petitioner shows and as outlined above, the modification of Duvall's similar system "amounts to nothing more than incorporating well-known techniques (providing information to human users for analysis) into Duvall's known system" "with only minor changes to Duvall's overall process" "to properly address Duvall's residue data," such that "the results of the combination would have been predicable." *Id.* at 22–23 (citing *KSR*, 550 U.S. at 419–21). Under these circumstances, "where the prior art was so similar, and the choice of elements readily predictable, [Petitioner] did not need to show . . . a particular benefit" in modifying the prior art. *See Cisco Sys., Inc. v. K.Mizra LLC*, No. 2022-2290, 2024 WL 3841809, slip op. at *3 (Fed. Cir. Aug. 16, 2024) (holding that "the Board ran afoul of *KSR* and *Intel* by ignoring Cisco's non-benefits-based, first and second motivation to combine rationales" (citing *KSR*, 550 U.S. at 419; *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373 (Fed. Cir. 2023) ("[C]ontrary to the Board's

suggestion, Intel never had to show that replacing Kabemoto's secondary cache with Bauman's secondary cache was an 'improvement' in a categorical sense.")).

Therefore, Petitioner shows that it would have been obvious to implement Chu's similar system and notify a security analyst (or a group thereof) "to optimize the handling of unresolved residue data in order to avoid 'filtering too much or too little' in Duvall." Pet 37 (citing Ex. 1004, 8:6–8; Ex. 1003 ¶¶ 140–141). And as noted above, Petitioner further explains that in light of the knowledge of an artisan of ordinary skill about known systems at the time, the combined teachings suggest employing trained network security analysts to handle a group of corporate filters in Duvall's system, which would further optimize and uniformly handle unresolved data as opposed to leaving decisions about individual filters and associated websites to untrained single operators whose decisions may not be uniform (i.e., contradict each other). *See id.* at 37–40. Therefore, Petitioner also articulates benefits such as uniform decision making in filter editing and the ability to detect malware in modifying Duvall's system based on the collective teachings of Chu and Duvall.

Accordingly, as summarized above and contrary to Patent Owner's arguments, Petitioner's showing as outlined above also demonstrates "how" and "why" to modify Duvall's system. Patent Owner's arguments support this finding as to "how" by recognizing that "the administrator that handles filters [e.g., using Duvall's editing manager] do[es] double-duty to analyze security-related events." *See* Prelim. Resp. 46. And as noted above, limitation 1.c is broad and does not require the "analyst system" to actually analyze information. Even if claim 1 does require such an analysis, Petitioner's showing covers that interpretation as explained above.

Based on the record and foregoing discussion, we determine that the combination of Duvall and Chu teaches limitation 1.c.

> *e. "d) a receiver for receiving feedback at the probe based on empirically derived information reflecting operation of the security monitoring system"*

Referring to its showing for limitation 1.c, Petitioner contends that the combined teachings of Duvall and Chu teach this element, asserting that "information about residue data is sent to an analyst for handling." Pet. 40. Petitioner also contends that Duvall "discloses feedback in the form of an 'editing Manager' that allows 'edit[ing] the database to add, delete, or modify filters in the database." *Id.* at 41 (alteration in original) (quoting Ex. 1004, 8:2–5).[11] According to Petitioner, a person of ordinary skill in the art would have recognized that

> Duvall's editing manager provides "*a receiver for receiving feedback . . . based on empirically-derived information reflecting operation of said security monitoring system*" because the information is only provided to the trained professional if the data is residue data—meaning that the data did not match any allow/block filters and passed through subsequent analysis (e.g., keywords and pattern matching) without any resolution.

Id. (citing Ex. 1004, 5:8–18; Ex. 1003 ¶¶ 146–147). As indicated above in connection with limitation 1.c, Petitioner relies on Chu's teaching of providing "[u]ser intervention [to a user/analyst]. . . only when the given URL is neither the blacklist nor the whitelist" to suggest providing feedback information arising from the analyst's receipt of information about the filtering process and including residue data, where Chu also teaches

[11] The term "empirically derived information" as recited in limitation 1.d does not refer back to, or further limit, the recited "information" in limitation 1.c.

prompting the user/analyst when there is neither blocking nor allowing of status data. *See id.* at 39 (quoting Ex. 1004, 44 ("Prompt me for my attention otherwise.").

Petitioner contends that "decisions made by the trained professional (e.g., whether the filters should be modified) would be based on observable information about the data (e.g., transmission path, URL, etc.)." Pet. 40 (citing Ex. 1003 ¶ 147). Petitioner adds that "[f]eedback is received '*at the probe*' because Duvall's editing manager is part of the filtering system implemented on server 30." *Id.* (citing Ex.1004, 8:2–5, 8:18–21; Ex. 1003 ¶ 148).

Patent Owner does not directly address Petitioner's showing for limitation 1.d. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. To the extent Patent Owner's arguments that address Petitioner's showing with respect to limitations 1.c and 1.e, we address those above and in the next section.

Based on the record and foregoing discussion, we determine that the combination of Duvall and Chu teaches limitation 1.d.

> *f. "e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback"*

Referring to its showing for limitations 1.c and 1.d, Petitioner contends that the combination of Duvall and Chu teach limitation 1.e because, *inter alia*, the combination teaches "'*receiving feedback*' from an analyst via Duvall's 'editing Manager,' which 'allows the user to edit the database to add, delete, or modify filters in the database.'" Pet. 41 (non-

emphasized quotes quoting Ex. 1004, 8:2–5; citing Pet. § VI.A.2(e); Ex. 1003 ¶ 149).

According to Petitioner, "[e]diting the filters in Duvall's filter database '*modif[ies] an analysis capability of said probe . . . based on said feedback*' because Duvall operates by comparing 'information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.'" Pet. 41 (second quote quoting Ex. 1004, 4:22–27; citing Ex. 1004, 4:27–30, 4:40–43). According further to Petitioner, "Duvall's system searches filters in the database when determining whether to allow or block a data transmission." *Id.* (citing Ex. 1003 ¶ 150). "As filters are added, deleted, or modified, Duvall's analysis would reflect these updates." *Id.* (citing Ex. 1004, 8:3–16; Ex. 1003 ¶ 150).

Petitioner also contends that "Duvall's filtering system accommodates dynamic updates because it searches 'filter entries stored in the database' when performing its analysis, . . . which would reflect [prior] changes to filters as they are edited." Pet. 42 (quoting Ex. 1004, 4:25–26; citing Ex. 1004, 4:22–43, 8:3–16; Ex. 1003 ¶ 152).

To further show that Duvall's system is capable of dynamic modification, Petitioner refers to Duvall's "Updating Mechanism" as follows:

> Duvall recognizes that "[b]ecause Internet sites are being added to the Internet at a fast rate . . . the filtering system preferably also has an *updating mechanism* to keep filters current" and that "the system can adapt as new sites and servers are added to the Internet." EX1004, 7:18–21; 2:16–18. Given the rapidity of updates, a POSA would have recognized that Duvall's "*analysis capability of said probe*" is "*dynamically modified . . . during operation thereof*" because taking the system offline each time an update was required would be disadvantageous. EX1003, ¶151. To avoid this disadvantage, Duvall "provid[es] updates

> online" so that "the system can adapt as new sites and servers are added to the Internet." EX1004, 2:16–18.

Pet. 41–42.

Petitioner asserts that "[a] main benefit of databases is that entries can be edited or added without taking the system offline, which prevents the filtering system from being down during updates." Pet. 42 (citing Ex. 1003 ¶ 153). Petitioner contends that "[s]ince Duvall's system 'searches the filter database for matching filters' when opening a new data stream, the 'analysis capability of said probe' always reflects the latest and current set of filters." *Id.* (quoting Ex. 1004, 4:40–43; citing Ex. 1003 ¶ 153).

Patent Owner argues that "Petitioner does not sufficiently demonstrate that Duvall-Chu is 'reasonably capable' of dynamic modification." PO Resp. 35 (citing *ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1361 (Fed. Cir. 2018)). That is, Patent Owner agrees that claim 1 only requires that the modification control system *is capable of* "dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback." *See ParkerVision*, 903 F.3d at 1361 ("[A] prior art reference may anticipate or render obvious an apparatus claim—depending on the claim language—if the reference discloses an apparatus that is reasonably capable of operating so as to meet the claim limitations, even if it does not meet the claim limitations in all modes of operation.").[12]

[12] *ParkerVision* notes that previous Federal Circuit "cases distinguish between claims with language that *recites capability*, and those that *recite configuration*," and "where claim language recites 'capability, as opposed to actual operation,' *an apparatus that is 'reasonably capable' of performing the claimed functions 'without significant alterations' can infringe those claims*." *Id.* at 1362 (quoting *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (emphasis added)).

Here, claim 1 recites "a modification control system *for* dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback," which is the same as citing mere "capability" under *ParkerVision*. *See id.* at 1362 (holding that claims reciting "[a]n apparatus *for frequency up-conversion*" (claim 4) or "[a]n apparatus *for communicating*" merely recite a capability). "As a result, '[a]n invention need not *operate* differently than the prior art to be patentable, but need only *be* different'—or, rather, '*unobviously* different.'" *Id.* at 1361 (quoting *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464 & n.2, 1468 (Fed. Cir. 1990)); *see also In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable."); *In re Anderson*, 662 F. App'x 958, 963 (Fed. Cir. 2016) (nonprecedential) ("We also agree with the Board that the 'for use' claim language is a statement of intended use. The 'for use' language does not add a structural limitation to the claimed system or method.").

As noted above, Petitioner's contends that "the analysis capability of Duvall is modified dynamically 'because taking the system offline each time an update was required would be disadvantageous.'" Pet. 41. Petitioner also contends that Duvall's system updates its filters by editing them on-line and that "[a] main benefit of databases is that entries can be edited or added without taking the system offline, which prevents the filtering system from being down during updates. *Id.* (citing Ex. 1003 ¶ 153).

Dr. Jeffay's cited testimony credibly supports Petitioner. As Dr. Jeffay testifies, "Duvall explains that the 'implementation and use of the editing manager are generally based on known database editing techniques,'" and that "a main benefit of databases is that entries can be

edited or added without taking the system offline, which prevents the filtering system from being down during updates." Ex. 1003 ¶ 153 (quoting Ex. 1004, 8:10–11); *accord* Reply 16 (citing Ex. 1003 ¶ 153).

Based on the foregoing, Duvall implicitly discloses or renders obvious the limitation based on what a skilled artisan would have known about existing database techniques, which Duvall specifically references for its editing manager. A "prior art reference must be 'considered together with the knowledge of one of ordinary skill in the pertinent art.'" *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (quoting *In re Samour*, 571 F.2d 559, 562, 197 USPQ 1, 3–4 (CCPA 1978); citing *DeGeorge v. Bernier*, 768 F.2d 1318, 1323 (Fed. Cir. 1985) (a reference "need not, however, explain every detail since [it] is speaking to those skilled in the art)). As Petitioner argues, Duvall's system implements its "editing manager generally based on known database editing techniques." Ex. 1004, 8:10–11. Petitioner explains that "at the time of the '641 patent, almost every commercially-available database-management system implemented multi[-]version concurrency control (MVCC), which allowed a database to be queried (i.e., remain online) while simultaneously being written to." *Id.* at 17 (citing Ex.1040 ¶¶ 19–23).

Supporting Petitioner, Duvall discloses the following:

> In addition to an initial filter database and future updates, the filtering system has an [E]diting Manager *that allows the user to edit the database to add, delete, or modify filters in the database. The editing filter allows the user to make custom changes if the user believes that the filtering system is filtering too much or too little*. The editing manager is preferably separately password protected. The system allows each filter to be examined individually
>
> The *implementation and use of the editing manager are generally based on known database editing techniques*. In

> addition, during a session over the Internet, a user can copy URLs for later editing. The user can then copy those URLs for inclusion in the database, or can edit the entry, e.g., to change the action from allow to block or vice versa.

Ex. 1004, 8:11–16 (emphases added).

Based on Duvall's disclosure that ties its editing manager database functionality to known commercial databases and evidence describing same, as Petitioner shows, prior art databases, such as Duvall's, were not only at least capable of, but configured to, perform dynamic modification via online editing where "techniques for solving this problem were well known in the art and already incorporated into commercially available database-management systems." *See* Reply 17–18 ("Nothing more than use of a standard commercial database system at the time of the '641 patent would be necessary to enable the claimed dynamic modification in Duvall-Chu's system." (citing Ex. 1040 ¶¶ 19–23). At the cited declaration paragraphs, Dr. Jeffay cites record evidence, including a textbook (Ex. 1051) and other evidence (Exs. 1041–1043, 1045) to support his conclusion that "the use of a standard commercially available database-management system at the time of the '641 patent would have enabled a database entry to be queried (i.e., read) while simultaneously being written to." Ex. 1003 ¶¶ 19–23.

Petitioner also contends that such a system would have been obvious for providing a "main benefit" that "prevents the filtering system from being down during updates." *See* Pet. 42 (citing Ex. 1003 ¶ 153); PO Resp. 35 (referring to Petitioner's "motivation").

Patent Owner argues that "nowhere does Duvall or Chu suggest this capability would occur even some of the time or in certain modes of operation" because "the Duvall-Chu system must be significantly altered to perform this claimed functionality." PO Resp. 37 (citing Ex. 2016 ¶ 134–

141 (discussing cache coherency issues)). Patent Owner cites to Dr. Jeffay's deposition testimony as allegedly "recognizing dynamic modification could create problems with cache consistency but providing no evidence of prior art solutions available at the time." *Id.* (citing Ex. 2007, 164:20–165:13).

This line of argument and evidence does not undermine Petitioner's showing. Nor does it address Dr. Jeffay's Reply declaration testimony, supported by cited record evidence, that any modification to Duvall's database would have been implicit or routine given that dynamic modification was a common database feature at the time of the invention, including via "Oracle 8i." *See* Reply 17 (citing Ex. 1003 ¶ 153; Ex. 1040 ¶¶ 19–24; Ex. 1044, 1–29, 1–30); PO Resp. 37 (citing 2016 ¶¶ 134–141) (testifying that dynamic modification in Duvall is not inherent and raising cache coherency and other issues)).[13]

Moreover, as Petitioner argues, the '641 patent does not describe any detail for the claimed "dynamically modifying" functionality. Reply 18 (citing Ex. 1001, 5:32–35 ("The software and filters of probe/sentry system 2000, in a preferred embodiment, may be adaptive or, alternatively, may be manually updated offline or dynamically (that is, during actual operation)."')). As Petitioner argues, "[t]his lack of detail demonstrates that the claimed 'dynamic modification' would have been well within the capability of a POSA." *Id.* (citing *Uber Techs., Inc. v. X One, Inc.*, 957 F.3d 1334, 1339 (Fed. Cir. 2020) (noting that when a patent specification "is entirely silent on how to" perform a claimed feature, it "suggest[s] that a

[13] Petitioner does not rely on inherency contrary to Dr. Lee's testimony and Patent Owner's characterization.

person of ordinary skill in the art was more than capable of" performing that claimed feature)). *See* Ex. 2016 ¶¶ 134–141.

This lack of detail also undercuts Dr. Lee's testimony that cache consistency and other alleged problems associated with using RAM prevents the dynamic database functionality with respect to Duvall's known database techniques. That is, the '641 patent does not address any of the alleged known problems with respect to dynamic updates that Dr. Lee raises. Rather, it simply states that the filter database "may be manually updated offline or dynamically (that is, during actual operation)" without more description, as noted above. *See* Ex. 1001, 5:32–35. Therefore, this lack of detail also implies that the challenged claims neither preclude nor require known techniques raised by Dr. Lee and/or Dr. Jeffay, including, for example, re-booting the database or running cache protocol updates. *See* Ex. 2016 ¶¶ 134–141 (discussing Dr. Jeffay's solutions).

Patent Owner also argues that "Petitioner never identifies any analyst systems in the prior art capable of receiving whatever was transmitted by its probe." PO Resp. 34. Patent Owner further argues that Petitioner fails to show dynamic modification of the probe as opposed to the database. Sur-reply 22. This line of argument is unavailing. As discussed in connection with limitation 1.c above, Petitioner relies on the combined teachings of Chu and Duvall to suggest an analyst system that receives residue feedback data at the probe, which in turn, serves to facilitate dynamic modifications to Duvall's probe's filters via the probe's editing manager's analysts based further on Duvall's corporate filter teachings and Chu's analysis teachings. *See* Reply 13; Pet 38–39 (analyst system) 40 (tying analyst system editing manager and filters to Duvall's receiver at probe). Any updates by either the user analyst ("custom changes") at the probe's editing manager or automatic

updates at the probe by the server are ultimately updates based on prior feedback at the probe. *See* Pet. 41–42 (citing Ex. 1004, 5:18–18; 7:18–21, 8:2–5, 18–21; Ex. 1003 ¶¶ 146–147). That is, as Petitioner explains, current dynamic update decisions by the user analyst reflect previous filter updates based on residue feedback by a user analyst who had customized the filters as a result of having previously analyzed residue data "if the user believes the filtering system is filtering too much or too little," (*see* Ex. 1004, Fig. 4, 8:1–9), whereas, similarly, an automatic update from the server "preferably causes some or all of the existing filters [as previously customized based on residue feedback] in the filter database to be replaced" (*id.* at 7:27–29). *See* Pet. 40–42 (citing Ex. 1004, 2:16–18, 4:22–43, 7:18–21, 8:2–16; Ex. 1003 ¶¶ 150–153).

Regarding capability during operation, claim 1 does not require modifying an analysis capability of the probe while the probe performs a search—the claimed probe system may be operational prior to, or after, actually performing a search, for example, after it receives the feedback as limitation 1.e requires and then while simply waiting for input from one or more users designating a URL to access with its web browser. *See* Reply 16–17; Ex. 1004, Fig. 3 (step 100 ("DATA STREAM OPENED?")). That is, as Petitioner contends, Duvall's "filtering system *detects when the client opens the data stream for a particular port and IP address* (step 100), and searches the filter database for matching filters." Pet. 30 (quoting Ex. 1004, 4:37–42 (emphasis added); citing Ex. 1003 ¶ 128). In other words, Duval's filtering system is operational at step 100 of Figure 3, when it runs to detect "DATA STREAM OPENED?" prior to "search[ing] the filter database for matching filters" on a current search and also after a previous search. *See* Ex. 1004, 3:49–63, 4:37–42, Fig. 3 (step 100). Neither

Patent Owner nor Dr. Lee contends that there is a cache coherency problem for dynamic updates while the system merely monitors a port. *See* PO Resp. 37 (citing Ex. 2016 ¶ 134–141 (discussing cache coherency issues)); Inst. Dec. 38–41 (discussing monitoring the open port).

Specifically, to meet limitation 1.e, Duvall's client processor 20 and editing manager (under Petitioner's showing) need only be "reasonably capable" of accessing filter database 24 at server 30 or (RAM at the client (which downloads the filter database)) to modify same, while the processor's implementing software monitors a port as it does at step 100 of Figure 3. That is, in Duvall's system, "[t]he client *monitors . . . ports* and maintains internal tables that indicate the state of each active TCP data stream, *whether that stream is open or closed*, for both incoming and outgoing transmissions." *Id.* at 3:59–63 (emphasis added); *see also* Pet. 30 (quoting Ex. 1004, 4:37–42, Fig. 3 (step 100 ("DATA STREAM OPENED?"). So when a data stream is closed and the system is monitoring the ports to see if "DATA STREAM OPENED?," Duvall's probe is operational. *See* Ex. 1004, code (57), 2:1–11, Figs. 1–3.

Therefore, as Petitioner shows, Duvall's editing manager is at least reasonably capable of allowing dynamic modifications of an analysis capability as limitation 1.e requires, even if Duvall does not explicitly disclose such a capability. Alternatively, as Petitioner also shows, Duvall implicitly discloses or renders obvious limitation 1.e even under a "configured to" claim interpretation.

Based on the record and foregoing discussion, we determine that the combination of Duvall and Chu teaches limitation 1.e.

g. Objective Indicia of Nonobviousness

i) Legal Principles

Objective evidence of non-obviousness "may often be the most probative and cogent evidence in the record" and "may often establish that an invention appearing to have been obvious in light of the prior art was not." *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA, Inc.*, 699 F.3d 1340, 1349 (Fed. Cir. 2012) (quoting *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983)). Objective evidence may include long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, and praise. *See Graham*, 383 U.S. at 17–18; *Leapfrog Enters., Inc. v. Fisher–Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007).

"For objective evidence of secondary considerations to be accorded substantial weight, its proponent must establish a nexus between the evidence and the merits of the *claimed invention*." *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010)). "A nexus may not exist where, for example, the merits of the claimed invention were 'readily available in the prior art.'" *ClassCo, Inc. v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016) (quoting *Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1580 (Fed. Cir. 1983)). "Additionally, there is no nexus unless the evidence presented is 'reasonably commensurate with the scope of the claims.'" *Id.* (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)). "There is no hard-and-fast rule for this calculus, as '[q]uestions of nexus are highly fact-dependent and, as such are not resolvable by appellate-created categorical rules and hierarchies as to the relative weight or significance of proffered evidence.'" *Id.* at 1221–1222 (quoting *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331 (Fed. Cir. 2016) and reasoning that "because claims 2 and 14 are

considerably broader than the particular features praised in the articles, it would be reasonable for the Board to assign this evidence little weight").

"[A] patentee is entitled to a rebuttable presumption of nexus between the asserted evidence of secondary considerations and a patent claim if the patentee shows that the asserted evidence is tied to a specific product and that the product '*is* the invention disclosed and claimed.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). Presuming nexus is not appropriate "[w]hen the thing that is commercially successful is not coextensive with the patented invention." *Id.* at 1373 (quoting *Demaco*, 851 F.2d at 1392). Presuming nexus may be appropriate if "the unclaimed features amount to nothing more than additional insignificant features." *Id.* at 1374.

"A finding that a presumption of nexus is inappropriate does not end the inquiry into secondary considerations"; rather, "the patent owner is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the 'direct result of the unique characteristics of the claimed invention.'" *Fox Factory*, 994 F.3d at 1374–75 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). In other words, "[w]ithout the presumption, a patentee may establish nexus by showing the secondary considerations evidence is the 'direct result of the unique characteristics of the claimed invention,'" *Magseis FF LLC v. Seabed Geosolutions (US) Inc.*, 860 F. App'x 746, 751 (Fed. Cir. 2021) (not for publication) (quoting *Huang*, 100 F.3d at 140), "rather than a feature that was 'known in the prior art,'" *id.* (quoting *Ormco Corp. v. Align Tech., Inc*., 463 F.3d 1299, 1312 (Fed.Cir.2006).

Recently, in *Zaxcom*, the Federal Circuit indicated that *Fox Factory*'s "coextensiveness" requirement is pertinent to the "commensurate in scope" standard regarding the "presumption of nexus." *See Zaxcom, Inc. v. Lectrosonics, Inc.*, 2022 WL 499843, at *2 (Fed. Cir. 2022). Specifically, *Zaxcom* held that "the Board determined that Zaxcom's evidence of industry praise and long-felt need was entitled to *a presumption of nexus*, noting that these indicia were *commensurate in scope* with the claims as now narrowed, . . . a *determination that comports with the legal standards for a presumption*." *Id.* (emphasis added) (citing *Fox Factory*, 944 F.3d at 1373; *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). Stated another way, "there is no nexus unless the evidence presented is 'reasonably commensurate with the scope of the claims.'" *ClassCo, Inc.*, 838 F.3d at 1220 (quoting *Rambus*, 731 F.3d at 1257). "There is no hard-and-fast rule for this calculus, as '[q]uestions of nexus are highly fact-dependent and, as such are not resolvable by appellate-created categorical rules and hierarchies as to the relative weight or significance of proffered evidence.'" *Id.* at 1221–1222 (quoting *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331 (Fed. Cir. 2016)) (reasoning that "because claims 2 and 14 are considerably broader than the particular features praised in the articles, it would be reasonable for the Board to assign this evidence little weight").

Several cases prior to *Fox Factory* and *ClassCo* address the commensurate in scope requirement, without specifically addressing the presumption of nexus. Together, the cases suggest that coextensiveness, or the reasonably commensurate in scope requirement, is not met when the claims are significantly broader that the proffered evidence of nonobviousness (which may indicate significant unclaimed features

contribute to any success or praise or solve an unmet, long-felt need, etc.) For example, in *MeadWestVaco Corp. v. Rexam Beauty and Closures, Inc.*, 731 F.3d 1258, 1264 (Fed. Cir. 2013), the court held that the district court erred by considering "secondary considerations of non-obvious [that] involved only fragrance-specific uses, but the claims now at issue [i.e., claims 15 and 19] are not fragrance-specific." The district court erred because it "credited evidence advanced to show long-felt need and commercial success specific to the perfume industry" but some claims at issue "are not limited to fragrance-specific claims." *See id.* at 1264–65 (reasoning that "objective evidence of non-obviousness must be commensurate in scope with the claims which the evidence is offered to support") (quoting *Ayst Techs., Inc. v. Emtrak, Inc.*, 544 F.3d 1310, 1316 (Fed. Cir. 2008); *see also In re Law*, 303 F.2d 951, 954 (CCPA 1961) ("Thus, assuming the affidavits are a proper showing of commercial success, they do not show commercial success of dockboards covered by the appealed claims which are not limited to the bead of claim 13."); *In re Tiffin*, 448 F.2d 791, 792 (CCPA 1971) (finding commercial success and long-felt need with respect to "'cups' used in vending machines," but "agree[ing]" with "[t]he solicitor's position . . . that the objective evidence of non-obviousness *is not commensurate with the scope of claims 1–3 and 10–16, reciting 'containers' generally*, but establishes non-obviousness only with respect to 'cups' and processes of making them" (emphasis added)).

ii) Analysis

Patent Owner argues that "Counterpane MSM is an embodiment of the Schneier Patent and is captured by the claims." PO Resp. 60. Therefore, according to Patent Owner, "[t]he Board should consider evidence of a long-felt but unresolved need in the network security market, industry praise, and

commercial success of Counterpane MSM as objective evidence of non-obviousness." *Id.*

According to Patent Owner "Counterpane MSM is "essentially the claimed invention." PO Resp. 61. According further to Patent Owner, "Counterpane MSM utilizes a probe (i.e., Sentry) and an analyst system (i.e., Socrates)." *Id.* (citing Ex. 2009, 6, 12; Ex. 2011, 2). According to Patent Owner, after Counterpane MSM collects data, filters potential security threats, further analyzes post-filtering residue, and sends identified events to analyst systems, "trained security analysts "'filter[] out the chaff' and refine the potential security threat information that is presented to customers." *Id.* at 61 (citing Ex. 2012).

Patent Owner indicates that the arguments and evidence apply to claims 1 and 18. *See* PO Resp. 61 (listing "cl.1; *see also* cl. 18"). However, as explained below, Patent Owner's arguments and evidence fail to show a presumption of nexus or nexus because the challenged claims are not reasonably commensurate in scope with the proffered evidence. In addition, as also explained further below, claims 1 and 18 are distinct claims citing different combinations that at most represent different broad subcomponents of the relied-upon Counterpane MSM commercial system and services.

Patent Owner further explains that with regard to how Counterpane MSM works,

> although Dr. Lee stated [during his deposition] he had not personally reviewed "internal documents" about how exactly certain functions were implemented ([Ex. 1046], 45:22–46:2), he reiterated his opinion was formed based on the "cited . . . industry report[s] or references," and he "kn[e]w this technology" because "Bruce Schneier was giving a talk at a conference [he] attended" (*id.*, 29[:]4–21).

Sur-reply 26 (arguing that "Dr. Lee specifically relied on Exhibits 2009–2015 and 2017, which match his recollection" (citing Ex. 2016, 213), and that "[n]othing else is needed to establish the nexus"). This testimony, based on Dr. Lee's personal knowledge and his "recollection" is "entitled to little or no weight," because it "does not disclose the underlying facts . . . on which the opinion is based." 37 C.F.R. § 42.65. Supporting this finding, Dr. Lee contends he "did not have to specifically go into limitation by limitation" to show a nexus to the "Counterpane MSM" system. Ex. 1046, 31:14–15.

Petitioner shows that it asked Dr. Lee the following about limitation 1.b (Reply 26):

> Have you shown that: the Counterpane MSM includes a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering?

Ex. 1046, 35:7–14. But Patent Owner objected because "[Dr. Lee] did not offer the opinion what you're questioning about" so the question "i[s] outside the scope." *See id.* at 36:4–7; Reply 26. As Petitioner argues, "[t]he totality of PO's analysis consists of one paragraph, and neither PO nor its expert makes any attempt to map the limitations of any claim to Counterpane." *Id.* (citing PO Resp. 61–62; Ex. 2016 ¶ 214).

In any event, asserting a presumption of nexus, as outlined above, Patent Owner relies on "trained security analysts" who "filter out the chaff" and "refine the potential security threat information that is presented to customers," as integral to the success of its Counterpane MSM system. *See* PO Resp. 61–62 (citing Ex. 2009, 6, 12; Ex. 2012, 2; Ex. 2016 ¶ 214). But

claim 1 does not *require* "trained security analysts" who do anything, let alone present information to customers or filter out chaff. Neither does claim 18. The '641 patent describes "security analysts" as "personnel specializing in the analysis of network attacks," but claim 1 and 18 do not recite or require "security analysts." *See* Ex. 1001, 2:43–45.

Therefore, at least for these reasons, and others noted below, claims 1 and 18 are not reasonably commensurate in scope with the relied-upon evidence. Patent Owner relies on these unclaimed features, and others noted below, to support its argument that Counterpane MSM solved a long-felt need and garnered industry praise and success. *See* PO Resp. 61–63.

In its Sur-reply, Patent Owner contends that Dr. Lee

> mapped the claim limitations to the product (*see* EX2016, [¶] 214), identified which claims the product embodies *(see id.*, [¶] 215, stating "Counterpane MSM embodies the challenged claims"), and discussed the analysis of post-filtering residue (*see id.*, stating "[t]he Sentry also utilizes an analysis engine to further analyze post-filtering residue which is then sent to the SOC and Socrates) and dynamic modifications (*see id.*, [¶¶] 221–222).

Sur-reply 25–26. But Dr. Lee's testimony simply mimics the arguments outlined above without specifying any particular claim limitations and generally pointing to claims 1 and 18. *See* Ex. 2016 ¶ 214 ("Counterpane MSM, is a "system for operating a probe as part of a security monitoring system for a computer network." EX1001, cl. 1; *see also id.*, cl. 18 (Counterpane MSM carries out the claimed method)."). This testimony, like Patent Owner's arguments outlined above, further shows that Patent Owner fails to show a nexus or presumption of nexus to the claimed invention for the reasons noted above and below. In addition, claims 1 and 18 do not require the whole Sentry system or Socrates system, including "an analysis engine *to further analyze post-filtering residue which is then sent to the SOC*

and Socrates," which Patent Owner also relies upon as showing a presumption of nexus. *See* Sur-reply 25–26 (emphasis added). Although claim 1 recites an "analysis system," it does not require performing the relied upon functions of Counterpane MSM. Therefore, for this additional reason, claims 1 and 18 are not reasonably commensurate in scope with the proffered evidence.

In particular as to the Sentry system, Dr. Lee testifies that "Sentries" provide a nexus to the claimed "probe," but testifies that Sentries "utilize over 20,000 filters to filter potential security threats." Ex. 2016 ¶ 214. However, none of the challenged claims requires more than a handful of filters, further showing that the challenged claims are not reasonably commensurate in scope with the alleged evidence of nonobviousness and thus lack a presumption of nexus or a nexus thereto. *See, e.g.*, *Tiffin*, 448 F.2d at 792 (finding commercial success and long-felt need with respect to "'cups' used in vending machines" but "agree[ing]" with [t]he solicitor's position . . . that the objective evidence of non-obviousness *is not commensurate with the scope of claims 1–3 and 10–16, reciting 'containers' generally*" (emphasis added)); *Law*, 303 F.2d at 954 ("Thus, assuming the affidavits are a proper showing of commercial success, they do not show commercial success of *dockboards covered by the appealed claims which are not limited to the bead of claim 13*." (emphasis added)).

That is, for example, the challenged claims *cover* 20,000 filters, but claims 1 and 18 are not limited to this large number of unclaimed filters in Sentries that Dr. Lee relies upon (and other unclaimed significant features as indicated above and below). And as noted above, the claims also do not require an "analysis engine." Accordingly, like the broadly recited generic container in *Tiffin*, the non-fragrance specific uses in *MeadWestVaco,* 731

F.3d at 1264, and the dockboards in *Law*, the claims here simply are materially broader than (i.e., not reasonably "*commensurate in scope with*") the evidence that Patent Owner offers for its objective indicia of nonobviousness, including commercial success, praise, and long-felt need. *Cf. Zaxcom, Inc. v. Lectrosonics, Inc.*, 2022 WL 499843, at *2 ("[T]he Board determined that Zaxcom's evidence of industry praise and long-felt need was entitled to *a presumption of nexus*, noting that these indicia were *commensurate in scope* with the claims as now narrowed, . . . a *determination that comports with the legal standards for a presumption*." (emphasis added)).

In addition, the prior art filtering sub-system and analysis thereof in Duvall reveals that Patent Owner relies on features known in the art to allege nexus or a presumption thereof. *See Ormco Corp.*, 463 F.3d at 1312 (no nexus for features "known in the prior art"); *Yita LLC v. MacNeil IP LLC*, 69 F.4th 1356, 1364 (Fed. Cir. 2023) ("[O]bjective evidence of nonobviousness lacks a nexus if it exclusively relates to a feature that was known in the prior art—not necessarily well-known."). Although *Yita* precludes a finding of nexus to features that "*exclusively* relate," to a "feature . . . known in the prior art," *Yita*, 69 F.4th at 1364 (emphasis added), Patent Owner's showing fails to point to claimed features of *merit* in claim 1 that are not in Duvall. That is, claim 1 largely reads on Duvall, with Chu merely supplementing Duvall's teachings as to an analyst system and the capability for security analysis systems, both at least suggested by Duvall as outlined above (and also readily available in the prior art). In other words, "[a] nexus may not exist where, for example, the *merits* of the claimed invention were 'readily available in the prior art.'" *ClassCo*, 838 F.3d at

1220 (quoting *Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1580 (Fed. Cir. 1983)) (emphasis added).

As indicated above, Patent Owner also contends that Counterpane MSM solves a long-felt need. PO Resp. 62–63. According to Patent Owner, "[t]he challenged claims provide a novel approach to discovering more threats than were possible with previous techniques and provided an architecture enabling reactive and proactive responses to potential threats." *Id.* at 62. According to Patent Owner, prior art systems were static, and the inventors noted that "[r]eal security is dynamic." *Id.* (quoting Ex. 2009, 9). Patent Owner also contends that prior art systems "did not perform discrete filtering functions" and "did not have the level of detection, monitoring, and response that were provided by Counterpane MSM." *Id.* Patent Owner also argues that "Counterpane MSM . . . took at the lead in the OS/400 server market and was the 'only managed security provider' to do so." *Id.* at 63 (quoting Ex. 2012, 3).

But none of the challenged claims require managing systems "in the OS/server market," resolving a minimum number of threats, or any set level of detection, monitoring, and response as provided by Counterpane MSM (e.g., with 20,000 filters in Sentry and with the "proprietary software" of Socrates). *See* Ex. 2009, 12 (stating "Socrates is our proprietary software system"). Therefore, as Petitioner argues, Patent Owner does not establish that "Counterpane solved any long-felt need." *See* Reply 27–28.

Dr. Lee's testimony is similar to Patent Owner's arguments in that it attempts to tie resolving an unresolved long-felt need to unclaimed features. For example, alleging a long-felt need, Dr. Lee testifies that "competitors were mainly . . . monitoring companies that performed discrete filtering functions and did not have the level of detection, monitoring, and response

that were provided by Counterpane." Ex. 2016 ¶ 219. However, like Patent Owner, Dr. Lee does not quantify any "level" of detection, monitoring, or response. Dr. Lee also fails to show that others attempted to solve any specific security problem covered by the claims over any period prior to the invention and then failed to do so. *See id.* ¶¶ 215–219. Dr. Lee also does not specify what a "response" is. To the extent it refers to providing feedback to a customer, claims 1 and 18 do not require it, let alone whatever level of it that Counterpane MSM sells to its customers.

Therefore, the challenged claims recite significant unclaimed features outlined above and further below, and they cover systems and methods that do and do not solve the alleged problem. For example, without the 20,000 filters of Sentry, the Socrates software, the level of detection, monitoring, and response that Counterpane MSM provided, the trained security analysts, and servicing the OS/400 server market, and other features Patent Owner relies upon to solve an alleged unmet long-felt problem, Patent Owner's evidence suggest the broad claims challenged here will not solve the alleged problem of discovering more threats than were possible at the level that Counterpane MSM provided for diverse systems including the OS/400 server market. Accordingly, Patent Owner's showing of an unresolved long-felt need fails. *See Therasense, Inc. V. Becton, Dickinson & Co*., 593 F.3d 1325, 1336 (Fed. Cir. 2010) ("Because *the claims were broad enough to cover devices that either do or do not solve the . . . problem*, Abbott's objective evidence of non-obviousness fails because it is not commensurate in scope with the claims which the evidence is offered to support" (emphasis

added) (quoting *In re Grasselli*, 713 F.2d 731, 743 (Fed. Cir. 1983), *vacated on other grounds*, 374 F. App'x 35 (Fed. Cir. 2010)).[14]

In addition to the above, Patent Owner's evidence points to other significant unclaimed features. For example, as Petitioner argues, and as indicated above, the alleged dynamic feature of Counterpane MSM involves the use of "trained security experts." Reply 27 (quoting Ex. 2009, 9). But the challenged claims do not require "trained security experts." Also, Petitioner shows that "the use of 'trained security experts' was already known in the market." *Id.* (citing Ex. 1037, 277 ("IBM's Emergence Response Center offers a fee-based service with NetRanger" with a "network operations center" staffing "security experts"); Ex 1050, 1 (discussing "Pilot Network Services" in 1999: "security experts monitor the sophisticated technology 24×7 and continually develop upgrades to detect and repel attacks aimed at Pilot customers.").

Moreover, Patent Owner and Dr. Lee rely on Exhibit 2009, titled "Counterpane and Managed Security Monitoring," by named inventor Bruce Schneier, in an attempt to show an unmet long-felt need. The Schneier document is largely cumulative of the other documents Patent Owner relies upon in that it describes the MSM Counterpane system. *See* PO Resp. 62–63 (citing Ex. 2009; Ex. 2010; 2012); Ex. 2016 ¶¶ 215–222 (citing same). Exhibit 2009 is essentially a product brochure by Mr. Schneier about the commercial Counterpane MSM system, advertising "The Business Case for

[14] *Fox Factory* notes that "[a]lthough the panel opinion in *Therasense* was vacated by an order granting appellants' petition for rehearing en banc on the issue of inequitable conduct, 374 F. App'x 35, the portions of *Therasense* addressing obviousness—which are the portions we rely on in this case—were reinstated. 649 F.3d 1276, 12[9]6 (Fed. Cir. 2011) (en banc)." *Fox Factory*, 944 F.3d at 1373 n.2.

Security Monitoring." *See* Ex. 2009. It is not any more persuasive than Patent Owner's similar evidence discussed above.

For purposes of completeness, we review Exhibit 2009 in more detail. It states that "[t]he way to build resilient security is with vigilant, adaptive, relentless defense by experts (people not products)." Ex. 2009, 1. It states that "Counterpane's business is Managed Security Monitoring (MSM). In plain English, that means we watch over your network. And the watching is done by real people: expert analysts who monitor your network 24 hours a day." *Id.* at 6. It states that "Counterpane's expert Security Analysts are able to detect security incidents—both external intrusions and insider attacks—in real time, *and tailer immediate, effective responses for its customers*." *Id.* at 1 (emphasis added). It states that "Counterpane's value is our *unique combination of people and technology*." *Id.* at 9 (emphasis added). "If the attack is not a false alarm, *our analysts contact you immediately with detailed information about the threat and expert recommendations for corrective action*." *Id.* at 6 (emphasis added). "The Sentry collects data, . . . then sorts, analyzes, and correlates it using over 20,000 security filters and our own Analysis Engine, and sends the resulting alerts to one of our Secure Operations Centers." *Id.* *"[W]hat matters most is the caliber of people defending you*." *Id.* (emphasis added). The system uses "*Socrates, an expert software system developed by Counterpane*." *Id.* (emphasis added)

Dr. Lee relies on Exhibits 2009, 2010, and 2012, which describe Counterpane MSM. *See* Ex. 2016 ¶ 216 (citing Exs. 2009; 2010, 2012). For example, Exhibit 2010 describes Socrates as "a program" that "assigns categories and priorities to the network activities it detects, seeking signs of hostile computer attacks. Certain events that might be normal at one time—

backup files being made over a network at 3 a.m., for example—might suggest a hostile intruder or an attack at another." Ex. 2010, 2.

Although, as indicated above, claim 1 recites an analyst system, it does not require any specific caliber of people, which Mr. Schneier describes as what "matters most" in the Counterpane MSM system. Ex. 2009, 6. And claim 1 does not require the analyst system to actually do anything, let alone "*tailer immediate, effective responses for its customers*" by "expert analysts" or otherwise. And as determined above, it does not require any set level of detection, monitoring, or response as provided by Counterpane MSM. It does not require the proprietary Socrates software that assigns categories and priorities.

In similar fashion, claim 18 recites "providing the problem ticket to a security analyst console for analysis." But similar to claim 1, "for analysis" in claim 18 does not actually require any specific analysis by an expert, high caliber or otherwise, and at the least, it does not require an immediate effective response, or the Socrates proprietary software, or the level of monitoring and response provided by Counterpane MSM. The generic term "for analysis" is a statement of intended use of the console. *See Therasense*, 593 F.3d at 1336 (finding no unresolved long-felt need because the claims were "broad enough to cover devices that either do or do not solve the . . . problem").

In a section titled "How Does Counterpane Work," Exhibit 2009 states that "[a]t Counterpane, we believe that while all security products provide some level of protection, no set of products is infallible. Real security is achieved only when all network products, security and otherwise, work together." Ex. 2009, 12. The section also describes that Counterpane MSM systems require several hardware and software features, including

Sentry, Socrates, and a Secure Operations Center (SOC). Ex. 2009, 12. As noted above, Socrates is "proprietary software." *Id.* As also noted above, the challenged claims do not require this "proprietary software," which is part of the unclaimed system that "work[s] together" with experts of high caliber to provide the asserted security solution. *See id.* In addition, Socrates turns messages into tickets. *See id.* Claim 1 does not require tickets. *See Therasense*, 593 F.3d at 1336 (finding no unresolved long-felt need because the claims were "broad enough to cover devices that either do or do not solve the . . . problem").

Claim 1 also does not require any SOCs, and none of the challenged claims require the SOCs as described by Mr. Schneier:

> SOCs are the physical locations where Counterpane's analysts work, continually monitoring your networks. . . . SOCs are physically hardened facilities, protected by access tokens, biometric access devices, and constant audio and video surveillance. To protect the integrity of your network, *the SOCs are redundant: each constantly monitors the other and each can sever the other's connectivity and assume the other's workload in the event of a physical attack or System failure*.

Ex. 2009, 12 (emphasis added). None of the challenged claims require "physically hardened facilities, protected by access tokens, biometric access devices, and constant audio and video surveillance," or *redundant monitoring of one SOC by another or the functionality to sever the other's connectivity or take on its workload*, all of which are part of the asserted long term solution that "work[s] together" according to the evidence Patent Owner offers.[15] *See id.*; *Therasense*, 593 F.3d at 1336 (finding no

[15] Claim 6 requires, and the preamble of claim 18 recites, a "secure operations center." However, the '641 patent does not describe the SOC as requiring the hardened facilities or the redundancy between two or more

unresolved long-felt need because the claims were "broad enough to cover devices that either do or do not solve the . . . problem").

Patent Owner also provides additional, similar evidence about the Counterpane MSM system and service and contends it shows there is industry praise and commercial success. *See* PO Resp. 63–65 (citing Ex. 2013, 2 (listing Counterpane Internet Security as a "visionary"); Ex. 2014, 7 (describing Counterpane MSM as a "leading vendor" in "managed security monitoring"); Ex. 2011, 1, 3 (describing "Counterpane's industry leading Security Monitoring Service" and quoting a security analyst who also recognized "Counterpane has been an industry leading security services provider since the market's inception"); Ex. 2015; Ex. 2016. For reasons similar to those noted above, the praise or success that Patent Owner relies upon amounts to reliance on many individual significant features that operate together as one large system as a whole (i.e., the whole Counterpane MSM system and services), none of which the challenged claims require. The challenged claims, which recite at most different sub-components or features of a total security system, do not even *cover* the whole Counterpane MSM system, as explained further below.

For example, that the whole company, Counterpane, sold for more than 20 million dollars according to Patent Owner shows that the Counterpane company, instead of the features of claim 1 or claim 18, is the subject of the praise or commercial success. *See* PO Resp. 64 (citing

---

SOCs as described in Exhibit 2009. *See* Ex. 1001, 2:65–3:9 (listing optional features). For claims 6 and 18, as indicated below, Petitioner relies on prior art operations centers or customer service management systems that provide secure network communications as secure operations centers. *See* Pet. 45–46, 67–68. Patent Owner does not dispute that this satisfies the plain meaning. *See generally* PO Resp.

Ex. 2017). Patent Owner does not provide sufficient, if any, evidence to show that Counterpane's sale (or any of its sales of services) relates to the value of any commercial product or system that a single claim of the '641 patent even covers. Nor does Patent Owner assert that there is a license for the '641 patent. *Cf. EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985) (Successful licensing is not an "infallible guide to patentability.").

Claim 1's preamble recites "[a] system for operating a probe *as part of a security monitoring system*." Claim 18's preamble recites a "method of operating a secure operations center *as part of a security monitoring system for a customer computer network*." Any praise, any commercial success, and any unresolved long-felt solution, advanced by Patent Owner, simply does not arise from "*part of* a security monitoring system." Rather, as Mr. Schneier, Dr. Lee, and Patent Owner indicate, the proffered evidence relates to significant unclaimed features of the whole Counterpane MSM commercial system or the company itself. Hence, even if the preambles of claims 1 and 18 are limiting, claims 1 and 18 at most represent sub-components of the larger Counterpane MSM system, while Patent Owner relies on features of the whole Counterpane MSM system as evidence of nonobviousness.

Stated differently, claims 1 and 18 relate to two different sub-combinations of features, which in turn at most relate to different sub-components of Counterpane MSM. Yet, as outlined above, Patent Owner argues that the same evidence shows a nexus to both independent claims. This reliance is fatal to Patent Owner's showing under *Fox Factory*. "The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features." *Fox Factory,* 944

F.3d at 1378 ("Because the Board erroneously presumed nexus between the evidence of secondary considerations and the independent claims, we vacate the Board's obviousness determination and remand for further proceedings."). Patent Owner "retains the burden of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention," but Patent Owner fails to meet that burden. *See id.* (On remand, "[Patent Owner] SRAM will bear the burden of proving that the evidence of secondary considerations is attributable to the claimed *combination* of wide and narrow teeth with inboard or outboard offset teeth, as opposed to, for example, prior art features in isolation or unclaimed features.").

Accordingly, for the reasons outlined above, Patent Owner does not show a presumption of nexus and does not show a nexus (i.e., "the evidence of secondary considerations is attributable to the claimed *combination*") to any of the challenged claims. *See Fox Factory,* 944 F.3d at 1378. That is, Patent Owner relies on unclaimed features that are not reasonably commensurate in scope with the challenged claims and also relies on prior art features including the filtering clause of limitation 1.b disclosed in Duvall and the same clause in claim 18. Moreover, Patent Owner relies on the same evidence for two different sub-combinations as recited in claims 1 and 18, which does not show a presumption of nexus under *Fox Factory*. At most, Patent Owner shows a weak nexus entitled to little weight as compared to the Petitioner's showing of obviousness.[16]

[16] That is, to the extent the "commensurate in scope" (or "reasonably commensurate in scope") cases are not directly on point to show there is no presumption of nexus or nexus (notwithstanding the indication in *Zaxcom* and *ClassCo* that they are), Patent Owner at most shows a weak nexus so

h. Summary of Claim 1

As found above, the record shows that no presumption of nexus exists and no nexus exists between Patent Owner's proffered evidence and the claimed invention. Even if some weak nexus exists, Petitioner's showing of obviousness outweighs any evidence of nonobviousness. On the full record, after weighing the arguments and evidence as set forth in the parties' briefing, including evidence of secondary considerations of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claim 1 would have been obvious.

4. Analysis of Claims 2–7 and 15–17

a) Claims 3–5, 7, and 15–17

Having reviewed Petitioner's arguments and supporting evidence on this full record, including the arguments and evidence related to secondary considerations as summarized above for claim 1, we determine that Petitioner shows by a preponderance of evidence that the combination of Duvall and Chu would have rendered claims 3–5, 7, 16, and 17 obvious. *See* Pet. 42–49. Patent Owner does not address Petitioner's showing separately with respect to claims 3–5, 16, and 17. *See generally* PO Resp.

b) Claims 2 and 6

Claim 6 depends from claim 2, which recites "[t]he system of claim 1, wherein the identifying step includes performing a multi-stage analysis of the status data." There is no "step" in claim 1, because it is not a method

---

that even if there is some nexus, we assign "little weight" to it. *See ClassCo,* 838 F.3d at 1221–22 (reasoning "[t]here is no hard-and-fast rule [for determining] 'the relative weight or significance of proffered evidence'" (quoting *WBIP*, 829 F.3d at 1331), and that "because claims 2 and 14 are considerably broader than the particular features praised in the articles, it would be reasonable for the Board to assign this evidence little weight").

claim. In any event, claim 2 apparently refers to limitation 1.b, which recites "a filtering subsystem coupled to analyze status data to *identify* potentially security-related events represented in the status data."

Relying on it showing limitation 1.b, Petitioner contends that Duvall performs claim 2's "multi-stage analysis of the status data." Pet. 42 (citing Pet. § VI.A.2.c; Ex. 1003 ¶ 156). Petitioner submits the following as a summary of its limitation 1.b showing:

> For example, Duvall searches filters in multiple stages: "The filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last[.]" EX1004, 4:27–30. Duvall evaluates status data in multiple stages, first "determin[ing] if any require immediate action," and then "determin[ing] whether a deferred action must be taken with respect to any of the retrieved filter[s]." *Id.*, 4:38–50, 4:65–5:1, 5:8-29 (discussing additional analysis performed for deferred actions); EX1003, ¶156. *Duvall's Figure 4 shows an iterative analysis of residue transmission data, providing "a multi-stage analysis of the status data*." EX1003, ¶157. *Moreover, Duvall in view of Chu teaches an additional analysis stage involving a user (e.g., trained professional) to further evaluate residue data transmissions*. *Id.*

Pet. 42–43 (citing Pet. § VI.A.2(c); Ex. 1005, 44).

As set forth above and for reasons similar to those with respect to claim 1, including the analysis of secondary considerations, as Petitioner demonstrates, claim 2 would have been obvious. That is, Duvall's Figure 4 discloses an iterative multi-stage process analysis of residue status data, and the combination of Duvall and Chu teaches an additional analysis of same involving a trained professional. For example, as to the former, in the analysis of residue status data, Figure 4's steps 130–134 require an iterative comparison of keywords and directional indicators (receiving, transmitting) to the residue status data. *See* Ex. 1004, Fig. 4. Even if there is a match at

step 134, step 136 ("COMPARE FILTER PATTERN ACCORDING TO COMPARE DIRECTIVE") requires a subsequent comparison, which results, if no ("N") at step 138, in another iterative process back to step 130. *Id.* As to the latter, Duvall teaches that an editing manager provides further analysis of filters to see if "the filtering system is filtering too much or too little" (*id.* at 8:1–10), with Chu also providing user input for a similar problem as discussed above in connection with claim 1.

Accordingly, Petitioner's showing for claim 2 demonstrates a multi-stage analysis of the status data at the probe based on Duvall's Figure 4 and also a multi-stage analysis at an analyst system of the probe based on the combination of Duvall and Chu. *See supra* §§ III.3.A.c–d. Patent Owner does not address Petitioner's showing for claim 2 separately from claim 1. *See generally* PO Resp.

Claim 6 recites "[t]he system of claim 2, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe."

Based partly on its showing for claim 2, Petitioner relies on the knowledge of an artisan of ordinary skill, and contends that "a POSA would have understood the analyst system [referenced in claim 2] could be on-site or at a secure remote site, i.e., 'a secure operations center configured to receive data from the probe.'" Pet. 45 (citing Ex. 1003 ¶¶ 169–170; Ex. 1037, 277 ("Instead of staffing your own team of security experts, you can use IBM's strength in this area. A network operations center is staffed 7 x 24, and a specific expert is assigned to your account. When an event is detected, IBM's security experts notify you and help you respond to the event. Up-front planning and response policy design also are available.")).

To further support its position, Petitioner contends as follows:

> Duvall discloses that its filtering system can "be incorporated into a firewall [or] gateway." EX1004, 1:60–64. A POSA would have recognized that accessing a firewall or gateway can be, and most typically is, accessed remotely, e.g., from a separate "network operations center." EX1003, ¶171 (citing EX1037, 277). Further Duvall discloses that the filtering system is accessed through an "editing manager" that is "preferably password protected." EX1004, 8:2–9, 8:21–23. Thus, Duvall recognizes the need for security and a POSA would have recognized that the security analyst system would likewise be secure, including communications between the analyst system and the firewall (e.g., through HTTPS, SSL, TLS, etc.). EX1003, ¶171.

Pet. 45.

As indicated above, Petitioner shows that "it was common in the industry at the time to provide off-site security (e.g. hosted by a third party)," for example, using a known IBM system. *See* Pet. 45 (citing Ex. 1003 ¶ 172; Ex. 1037, 277 (describing the known IBM system)). Petitioner also shows that "Duvall discloses off-site operations where the 'updating mechanism in the filtering system can locate a particular HTTP or FTP update server 32 over the Internet . . . . [T]he updating mechanism causes the filtering system to download from the update server . . . filters.'" *Id.* at 46 (quoting Ex. 1004, 7:21–29). And Petitioner demonstrates that "[c]ustomers of Duvall's system are 'given an opportunity to obtain a subscription . . . to obtain further [filter] updates.'" Pet. 46 (quoting Ex. 1004, 7:35–40).

Based on the above-noted teachings and knowledge of the artisan of ordinary skill related to well-known third party subscriptions for security monitoring, and off-site access as disclosed in Duvall's system, Petitioner submits that "a POSA would have recognized that the trained professionals need not be located at the corporate firewall, but can be located remotely

(possibly as a third party subscription service), in their "*secure operations center"* such as a network operations center ('NOC')." Pet. 46 (citing Ex. 1003 ¶ 172). Accordingly, Petitioner submits that "an analyst system would receive residue data, evaluate that data, update the respective filters, and provide those updates to the corporation per the terms of the subscription." *Id.* (citing Ex. 1003 ¶ 172).

Petitioner further submits that "a POSA would have been motivated to ensure that the trained professionals managing Duvall's filtering system were doing so as part of a 'secure operations center'," because "this would ensure unauthorized users could not edit, add, or remove filters that could allow malicious traffic into the corporate network." Pet. 46 (citing Ex. 1003 ¶ 172).

Patent Owner argues that "[t]he only analysis Petitioner suggests would be performed by Duvall-Chu's analyst system occurs after both the identifying step and after information about those identified events have been sent to the analyst system." PO Resp. 39 (citing Pet., 38–40, 44–46). Patent Owner explains that limitation 1.b ("a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering") must occur before limitation 1.c ("a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system"). According to Patent Owner, claim 6's multi-analysis step refers back to "the analysis" of limitation 1.b via claim 2 ("wherein the identifying step includes performing a multi-stage analysis"), so the multi-stage analysis in claim 6 must occur in limitation 1.b. *Id.* at 29. In short,

Patent Owner contends that "Petitioner thus fails to show how any analysis at a SOC is incorporated *into* the identifying step (as required by Claim 6)." *Id.* (citing Pet. 38–39).

At the outset, system claims, such as claims 1, 2, and 6, do not normally require any order in the limitations recited. Here, however, limitation 1.b's "*identify[ing*] potentially security-related *events* represented in the status data" inferentially must occur prior to limitation 1.c's "transmit *information* about the *identified events* to an analyst system." That is, identifying events in limitation 1.b occurs prior to transmitting information about the events in limitation 1.c.

In any event, Petitioner's combination shows that a multi-stage analysis occurs at the probe (via its showing of claim 2) and at the SOC, as claim 6 requires, and this results in information flowing both ways—from the probe to the SOC, and from the SOC to the probe. For example, Petitioner submits that "[a]s discussed for claim 2, Duvall's 'multi-stage analysis includes analysis at the probe and at a secure operations center,' including evaluating status data in multiple stages." Pet. 44 (citing Pet. § VI.A.5; Ex. 1004, 4:27–30, 4:39–49, 4:65–5:1, 5:8–29; Ex. 1003 ¶ 169). As indicated above, Patent Owner does not dispute this showing. Turning back to claim 6, Petitioner also submits that in its combination, "an analyst system [at the SOC] would receive residue data [at the probe], evaluate that data, update the respective filters [thereby identifying events in limitation 1.b], and provide those updates to the corporation [which includes the analyst system at the probe] per the terms of the subscription [i.e., thereby transmitting information at limitation 1.c]." *See* Pet. 46 (citing Ex. 1003 ¶ 172). According to the prior art IBM system that Petitioner relies upon in its showing for claim 6, "[a] network operations center [NOC] is staffed 7 x

24, and a specific expert is assigned to your account. When an event is detected [at the SOC/NOC]*, IBM's security experts notify you [at the corporation analyst system] and help you respond to the event.*"

Accordingly, we determine that claim 6 would have been obvious even if claims 1, 2, and 6 include the temporal requirement advanced by Patent Owner.[17]

Based on the full record, including the arguments and evidence as set forth in the parties' briefs including as related to secondary considerations of nonobviousness as summarized above for claim 1, we determine that Petitioner shows by a preponderance of evidence that the combination of Duvall and Chu would have rendered obvious claims 2 and 6.

[17] Petitioner's Reply submits that the '641 patent only describes an analyst system at the SOC, and Patent Owner's Sur-reply does not dispute this. *Compare* Reply 18–19, *with* Sur-reply 26. If Petitioner is correct, then claim 6, via its dependency on limitations 1.b and 1.c, and the corresponding written description thereof, would require the anomalous outcome of analyzing information at the SOC's analyst system and then sending that analyzed information from the SOC's analyst system to itself. *See* Reply 18–19. However, based on the showing in the Petition and Patent Owner's arguments in the Response, we need not resolve any ambiguity in claim interpretation because neither limitation 1.c nor claim 6 specifies the location or number of the "analyst system[s]," where Petitioner's showing essentially involves two locations for analyst systems. *Cf. Samsung Electronics America v. Prisua Eng'g Corp.*, 948 F.3d 1342, 1353 (Fed. Cir. 2020) ("[T]he proper course for the Board to follow, if it cannot ascertain the scope of a claim with reasonable certainty for purposes of assessing patentability, is to decline to institute the IPR or, if the indefiniteness issue affects only certain claims, to conclude that it could not reach a decision on the merits with respect to whether petitioner had established the unpatentability of those claims under sections 102 or 103.").

c) Claim 15

Claim 15 recites "[t]he system of claim 1, further comprising instantaneous self-tuning the probe based on previously collected status data." Petitioner relies partly on its showing for limitation 1.e and contends that "Duvall's filtering system always searches the latest and current set of filters when performing its filtering analysis." Pet. 47 (citing Pet. § VI.A.2(f)); Ex. 1004, 4:22–43, 8:3–16; Ex. 1003 ¶ 177). Petitioner explains that therefore, "when filters are updated in Duvall's system, the analysis is 'instantaneously self-tun[ed]' because Duvall is programmed to use the updated filters in subsequent analysis." *Id.* at 47–48 (citing Ex. 1003 ¶ 177). Petitioner also explains that "as discussed for [limitations 1.b–1.d], the 'self-tuning' in the Duvall-Chu combined system is '*based on previously collected status data*' because filter edits are based on the user's analysis of previously collected information associated with potentially security-related events." *Id.* at 48 (citing § VI.A.2(c)–(e) (i.e., analysis of ; Ex. 1003 ¶ 177), *see also id.* at 47 (citing Ex. 1004, 4:22–43, 8:3–16).

Patent Owner argues that "Petitioner's Duvall-Chu combination requires the dynamic modification step Claim 1(e) to be performed to read on Claim 15." PO Resp. 41; *accord* Sur-reply 23–24 (similar arguments). Patent Owner's arguments are unavailing. Claim 15's "self-tuning" limitation is distinct from limitation 1.e's "dynamic modification" recitation. Claim 15 does not refer to limitation 1.e. For example, claim 15's self-tuning need not occur while the claimed system is actually operating or monitoring the computer network, in contrast to how we implicitly construed limitation 1.e based on pre-institution arguments by Patent Owner. *See supra* § III.3.A.f; Ex. 1003 ¶¶ 151–153; Inst. Dec. 36–37 (noting that Patent Owner relies on a district court construction and argues in its Preliminary

Response that Duvall's system is not "modified dynamically" because it does not "modify[] its analysis capability 'during actual operation, rather than offline.'" (quoting Prelim. Resp. 48; Ex. 1013, 2)). Patent Owner cites Dr. Jeffay's deposition testimony to support its position, but Dr. Jeffay's quoted testimony supports Petitioner: "I think dynamic modification is certainly a way in which instantaneous self-tuning can occur. *But are there other ways in which it can occur*? I haven't considered that question."). Petitioner shows "other ways" by relying on Duvall's editor-filter updates as described at column 8:1–15.

Therefore, even if claim 15 requires that the claimed system is configured to instantaneously self-tune the probe as Patent Owner argues (*see* PO Resp. 40–41), we determine that Petitioner shows by a preponderance of evidence that Duvall renders claim 15 obvious as Petitioner demonstrates. Alternatively, we find and determine that Petitioner shows by a preponderance of evidence that Duvall's system teaches claim 15, or at least renders it obvious, even if Patent Owner is correct that the obviousness of claim 15 depends on the obviousness of limitation 1.e under a "configured to" interpretation of that limitation. *See supra* § III.3.A.f.[18]

d) Summary

As indicated above, the record shows that no presumption of nexus exists and no nexus exists between Patent Owner's evidence of objective

[18] Patent Owner's attempt to bind this trial's findings to findings in a previous denial of institution in a related case for a similar limitation in a related patent does not account for differences in the full trial record here, which includes Petitioner's focus on known database techniques, as compared to the pre-institution record in the related case, which does not include that focus. *See* PO Resp. 40 (citing IPR2023-00888, Paper 9, 35) & n.2.

indicia of nonobviousness and the claimed invention. Even if a weak nexus exists, Petitioner's showing of obviousness outweighs the evidence of nonobviousness. On the full record, after weighing the arguments and evidence as set forth in the parties' briefs, including that related to secondary considerations of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claims 2–6 and 15–17 would have been obvious.

B. Alleged Obviousness of Claims 7–13 and 16 in view of Duvall, Chu, and Trcka

Petitioner contends that the combination of Duvall, Chu, and Trcka would have rendered these claims obvious. *See* Pet. 50–57. Patent Owner disputes Petitioner's showing, contending, *inter alia*, that Trcka's "motivation is flawed" (PO Resp. 41), Petitioner did not show how to combine Trkca (*id.* at 43), and Petitioner did not consider security or bandwidth concerns (*id.* at 47–50).

1. Trcka (Ex. 1014)

Trcka is a U.S. Patent Application Publication titled "Network Security and Surveillance System." Ex. 1014, codes (10), (54). Trcka relates to "[a] network security and surveillance system [that] passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic." *Id.* at code (57). According to Trcka, "[a] set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events." *Id.*

Trcka discloses "analysis applications [that] can . . . be used to view, analyze and process . . . traffic data," including "functionality for performing such actions as displaying user-specified types of network events, conducting pattern searches of selected packet data, reconstructing transaction sequences, and identifying pre-defined network problems." Ex. 1014 ¶ 16. Trcka also discloses "analysis tools . . . for allowing authorized users to perform interactive, off-line analyses of recorded traffic data." *Id.* ¶ 53. Trcka discloses a "graphical user interface (GUI)" through which "the user can launch and control the various analysis applications . . . through a common set of menus and controls." *Id.* ¶ 79.

2. Analysis of Dependent Claims 7–13 and 16

Claims 7–13 and 16 ultimately depend from claim 1 generally recite limitations directed to analyzing traffic by further limiting claim 1's limitation 1.b (claims 7–9, 12, 13), and/or "after" limitation 1.c (claims 10–13), reciting limitations performed at the probe and/or at an SOC, and using techniques such as cross-correlation, aggregation, synthesizing of data, tracking frequency of events, and analysis of previously collected status data. Patent Owner generally does not contest that Trcka teaches these techniques, but contests, *inter alia*, Petitioner's rationale and factual underpinnings for combining Trcka with Duvall-Chu. *See* PO Resp. 41–50; Sur-reply 26; Reply 20 (Patent Owner "does not dispute that the subject matter of claims 7–13 and 16 is taught by the prior art." (citing PO Resp. 41–50)).

a) Reasons to Combine the Teachings of Trcka with Duvall-Chu

Petitioner begins by noting, as discussed in connection with claim 1, that Duvall's "editing Manager" "allows the user to make custom changes if

the user believes that the filtering system is filtering too much or too little." Pet. 50 (citing Ex. 1004, 8:2–7). Therefore, Petitioner asserts that "Duvall suggests that a user (e.g., trained professional) reviews network activity to ensure the filters accurately allow and block data transmissions." *Id.* (citing Ex. 1003 ¶ 184; Ex. 1004, 8:2–7). Petitioner contends that "[a]lthough a POSA familiar with network security and filtering mechanisms would have understood numerous ways for performing this review," "Trcka provides details" and "additional guidance." *Id.* (citing Ex. 1003 ¶ 184).

To address the added limitations of dependent claims 7–13 and 16, Petitioner generally relies on Trcka's "network . . . surveillance system [that] passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic." Pet. 50 (alteration in original) (quoting Ex. 1014, code (57). Petitioner also relies on Trcka's "set of analysis applications and other software routines allow[ing] authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events." *Id.* (quoting Ex. 1014, code 57). Petitioner also relies on Trcka's "analysis applications . . . to view, analyze and process traffic data" (*id.* at 50–51 (quoting Ex. 1014 ¶ 16), wherein Trcka's "graphical user interface (GUI)" allows "the user" to "launch and control the various analysis applications," *id.* at 50–51 (alteration in original) (quoting Ex. 1014 ¶ 16)).

Petitioner contends that Trcka's techniques would have aided Duvall-Chu's analysts in determining if or when Duvall's system "filter[s] too much or too little," because "Trcka's analysis applications would enable the user to interact with such information as part of the user's analysis." Pet. 51 (first

quote quoting Ex. 1004, 8:5–7; citing Ex. 1003 ¶ 186). Petitioner explains that "Duvall already suggests that the user, such as trained professionals, should have access to past network activity to accurately update filters." *Id.* (citing Ex. 1004, 8:2–7). In other words, Petitioner argues that using Trcka's data analysis applications and techniques for interacting and monitoring network activity applies to Duvall-Chu's similar system to provide accurate updates for filters. *See id.* (arguing both Trcka's and Duvall's systems operate on packet data including packet headers (citing Ex. 1004, 3:64–4:55; Ex. 1014 ¶¶ 38–39).

Based on the noted teachings, Petitioner contends that "[a] POSA would have had a reasonable expectation of success implementing Trcka's analysis techniques, which would amount to nothing more than combining prior-art elements (i.e., Duvall-Chu's filtering system and editing manager with Trcka's data-analysis applications) according to known methods to yield predictable results." *Id.* (citing Ex. 1003 ¶ 187; *KSR*, 550 U.S. at 417).

b) Analysis

Claim 7 recites "the system of claim 1, wherein the identifying step includes aggregating and synthesizing the status data at the probe."

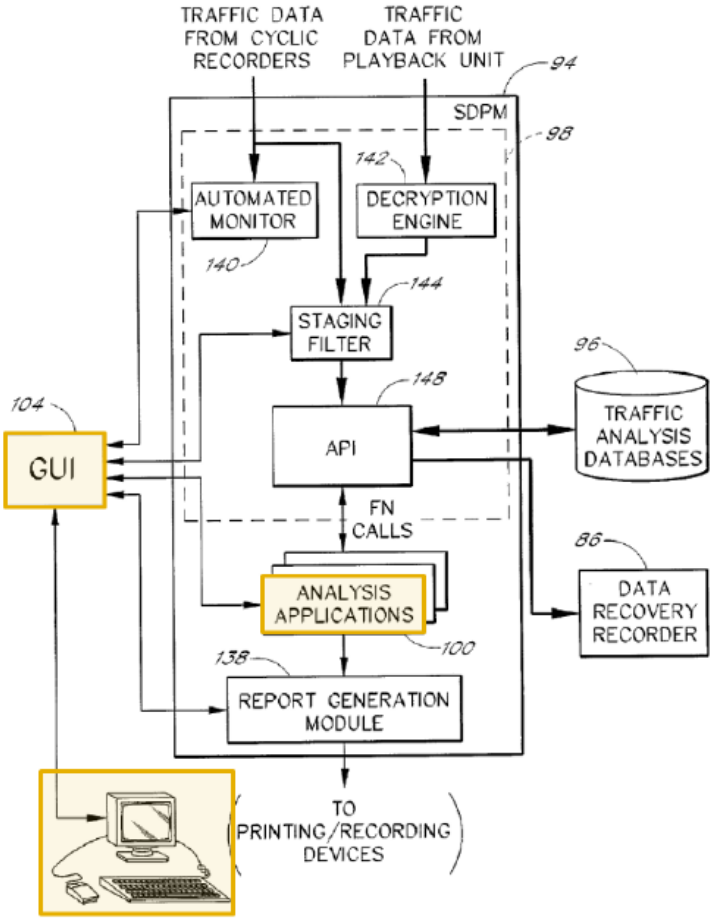
Claims 8 and 12 recite "[t]he system of claim [7/10], wherein the identifying step includes cross-correlating data across the monitored components," respectively.

For these claims, Petitioner relies on "Trcka's 'Audit' and 'Problem Determination' applications, which correlate 'the status data' and other data from different devices to 'particular types of network problems' occurring within a specific timeframe." Pet. 52 (citing Ex. 1014 ¶¶ 112, 116; Ex. 1003, ¶ 190). Petitioner also relies on Trcka's "Network Operating Characteristics Application," which "cross-correlat[es]" activity from

different devices for indications of "congestion," "traffic throughput," and "network outages." *Id.* at 53 (quoting Ex. 1014 ¶¶ 124–125; reproducing Ex. 1014, Fig. 19; citing Ex 1003 ¶ 191). Petitioner explains that Trcka's Figure 19 reveals how "the collected 'status data' is displayed in aggregate, and in a meaningful, synthesized format." Petitioner relies on other applications in Trcka to explain how Trcka's system aggregates, synthesizes, and cross-correlates status data at the probe and otherwise. *See id.* at 52–54.

Claim 10 recites "the system of claim 1, further comprising after the step (c) [of claim 1], a secure operations center coupled to perform further computer-based analysis and to receive data from the probe." Referring to its showing for claim 6, Petitioner contends that Duvall's corporate network suggests a secure operations center "within which users can operate," based on the understanding of a person of ordinary skill in the art. Pet. 54 (citing Pet. § VIA.7; Ex. 1003 ¶ 197). Petitioner contends that it would have been obvious to employ Trcka's computer-based analysis techniques in Duvall-Chu's system to allow analysts to analyze whether "the filtering system is filtering too much or too little." *Id.* at 55–56 (citing Ex. 1004, 8:5–7; Ex. 1014 ¶¶ 15, 16, 53, 79). Petitioner explains that Trcka's analysis techniques include "viewing past network activity using analysis applications, which execute on a computer." *Id.* (citing Ex. 1014 ¶¶ 15, 16, 53, 79, Fig. 7; Ex. 1003 ¶ 198).

To support its showing as to the analysis applications, Petitioner reproduces an annotated (colored) version of Trcka's Figure 7, which is a block diagram, as follows:



EX1014, FIG. 7 (annotated).

Figure 7 shows Trcka's GUI 104 connected to an analyst's computer to employ analysis applications 100 for analyzing traffic data from cyclic recorders (top), a playback unit (top), and from traffic analysis databases 95. *See* Ex. 1014 ¶¶ 95–96 (disclosing that the system monitors raw data traffic tin near real time via the cyclic recorders 82, 84 acting as buffers to store the data). Analysis applications 100 "provide various functionality for allowing users to interactively perform non-real-time or 'off-line' analysis of pre-recorded raw traffic data read-in from the Data Playback Unit 68 and the cyclic recorders 82, 84." *Id.* ¶ 98.

Claim 11 recites ""[t]he system of claim 10, wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis." Petitioner contends that one of Trcka's analyst applications as discussed above in connection with claim 10 includes a "Report Generator Module" that

> "manipulates the data to match a format preselected by the user" and "can then be delivered to a printer or display, or can be saved to a file." [Ex. 1014] ¶104. Reports in Trcka's system can include information such as "transaction activity," "unauthorized accesses to restricted files and databases," "statistics on congestion, peak loads, traffic throughput, network outages, and utilization," and "frequent transfers of files to outside entities." *Id.*, ¶¶112, 123, 125. This report data is "aggregate[ed]" and "synthesiz[ed]" because it is data generated from raw network activity and synthesized into a meaningful format. EX1003, ¶200.

Pet. 56. Petitioner also explains that "such techniques would allow trained network professionals to view aggregated information regarding blocked or unknown data transmissions in a synthesized data format, alerting the trained professionals to all such activity at the same time (i.e., '*on an ensemble basis'*)." *Id.* at 57 (citing Ex. 1014 ¶ 104; Ex. 1003 ¶ 201).

Claims 9 and 13 add the same limitations but depend from different claims, claims 7 and 10, respectfully, addressed above. Relative to the other dependent claims, Petitioner relies on a different application in Trcka for these similar claims. *See id.* at 54 (Claims 9 and 13 recite "[t]he system of claim [7/10], wherein the identifying step includes analyzing the frequency of occurrence of each of the events," respectively, and Petitioner relies on Trcka's "Audit" and "Problem Determination" applications). Petitioner shows that the analysis for claims 9 and 13 occurs during the identifying

limitation 1.b via its showing for claims 1, 7, and 10, from which they depend. *See id.*

Clam 16 recites "[t]he system of claim 1, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts." Claim 16 applies to limitation 1.e (the "dynamic modifying" limitation), and Petitioner specifically refers to its showing for limitation 1.e and modifies it by applying Trcka's techniques for generating audit trails from archived data. Pet. 57 (citing Ex. 1014 ¶ 112). Petitioner reasons that employing Trcka's techniques include analyzing past network activity by researching past data to help identify security related events and thereby further enable trained professionals to determine when Duvall's "filtering system is filtering too much or too little," and to update filters accordingly. *Id.* at 57–58 (citing Ex. 1004, 8:5–7; Ex. 1003 ¶ 205).

Generally addressing Petitioner's showing for claims 7–16, Patent Owner argues that "Trcka's analysis techniques only analyze the data recorded in its archive," and "Trcka's archive will not reflect Duvall's decisions to either block or allow data because Trcka only records what ends up being sent over the network." PO Resp. 41.[19] Patent Owner also argues that Trcka's analysis applications only operate on the archived traffic data "in an 'off-line' mode." *Id.* at 44 (citing Ex. 1014 ¶ 15). Patent Owner also argues that "Trcka's *offline* analysis of data in an archive is facially incompatible with analyzing transmissions intercepted by Duvall's system."

[19] Petitioner addresses claims 14 and 15 in another ground, which also involves Duvall, Chu, and Trcka, but also adds Ziese. *See infra* § III.C. To the extent Patent Owner's arguments also apply to claims 14 and 15, our analysis here applies.

Id. at 44 (citing Ex. 2016 ¶ 167). Patent Owner also argues that Trcka's analysis applications are "interactive analysis applications," so they "require[] human and not automatic operation." *Id.* at 46 (citing Ex. 1014 ¶ 15). Patent Owner submits that "[i]n contrast, the operating system of Duvall's client devices performs the 'identifying step' automatically by applying filters." *Id.* (citing Ex 1004, 6:10–29; 9:14–11:19). This argument applies to claims 7–9, 12 and 13, which refer to claim 1's "identifying step," as summarized above. Patent Owner also argues that "Duvall's 'identifying step' operates – and needs to operate - on live data, as it is intercepted by the operating system so that certain commands or transmissions can be blocked or altered." PO Resp. 45 (citing Ex 1004, 6:10–29).

With respect to claim 10 and 11, Patent Owner argues that they "require further computer-based analysis at a SOC, rather than as part of the 'identifying step.'" *Id.* at 47. According to Patent Owner, Trcka only analyzes archived data, and "Petitioner's expert never considers *how* such an archive could be made available to a remote SOC such that Trcka's analysis could be used to analyze whether Duvall's system was 'filtering too much or too little.'" *Id.* at 47 (citing Ex 1003 ¶ 186, ¶¶ 196–202).

Based on these arguments, Patent Owner contends that "[t]here is thus no disclosure of how a POSA could incorporate Trcka's techniques . . . to enable the user to analyze whether 'the filtering system is filtering too much or too little,'" and "a POSA would have lacked a reasonable expectation of success in combining Trcka with Duvall-Chu for this specifically-alleged purpose." PO Resp. 47 (citing Ex. 2016 ¶ 159); *accord* Sur-reply 27 (similar argument).

These arguments do not undermine Petitioner's showing, because Patent Owner does not address the thrust of Petitioner's showing. Patent

Owner's arguments also take isolated teachings from Trcka and Duvall and isolated rationales from Petitioner's showing. In addition, Patent Owner mis-characterizes Trcka's applications as only operating on archived data. Petitioner shows that Trcka's system, such as Figure 7 represents, includes different analysis applications, including for accessing archived data or near real-time data. *See* Ex. 1014, Fig. 7. Petitioner also points to Trcka's teaching that it "passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic." Pet. 50 (citing Ex. 1014, code (57); Ex. 1003, ¶¶ 84–88).

With respect to the thrust of Petitioner's showing and its reliance on Trcka's archived data, Petitioner shows via its analysis of claim 1 (as summarized above) that Duvall's system processes status data by comparing incoming data to existing filters in a "filter database." *See, e.g.*, Pet. 29–30 (analyzing limitation 1.b (citing Ex. 1004, 8:18–26, Fig. 2). Then, as the Petition explains relative to limitation 1.c (and limitations 1.d and 1.e), Duvall's editing manager allows users to manually modify filters based on existing data provided by feedback (e.g., archived data about previous websites used in the past to modify filters). *See id.* at 38–40. This "allows the user to make custom changes [to the filters] if the user believes that the filtering system is filtering too much or too little." *Id.* at 39 (quoting Ex. 1004, 8:3–10). Then, Petitioner explains, in context of limitation 1.d, which may occur both before or after limitation 1.c (because system claim 1 does not require an order for this limitation), that after limitation 1.c, "decisions made by the trained professional (e.g., whether the filters should be modified) would be based on observable information about the data (e.g., transmission path, URL, etc.)," and also based on "feedback" at the probe

via Duvall's editing manager. *Id.* at 40 (citing Ex. 1003 ¶ 147). In a similar fashion, with respect to limitation 1.e, Petitioner explains that "Duvall's filtering system accommodates dynamic updates because it searches 'filter entries stored in the database' when performing its analysis, . . . which would reflect changes to filters as they are edited." Pet. 42 (quoting Ex. 1004, 4:25–26; citing Ex. 1004, 4:22–43, 8:3–16; Ex. 1003 ¶ 152). Petitioner's showing for claim 6 shows that at limitation 1.b, Duvall's system, as combined with Chu and in light of the knowledge of an artisan of ordinary skill, analyzes data at the probe and at the SOC. *See supra* § III.A.4.b.

In essence, some of Duvall's stored filters represent filters created by manual interaction via human operator inputs at the editing manager based on status data that the operator analyzes to see if the system filters too much or too little at and after limitation 1.c (e.g., limitation 1.e). It follows, as explained above in connection with claim 1, that the filter database is ultimately a representation of past data received (i.e., archived data), because Duvall's human/corporate operators create new filters based on current data and based *on stored filters* created to handle *past data*. *See* Ex. 1004, Fig. 4, 8:1–16. Therefore, the filter analysis that Duvall's system performs both automatically via Duvall's Figure 4 and manually via Duvall's editing manager at limitation 1.c at an SOC and/or automatically based on feedback (as suggested by Duvall's corporate and editing manager teaches according to Petitioner's showing for claims 1 and 6), represents past data (at least suggesting archived data) that Duvall's system then applies for subsequent automatic filter analysis performed via step 1.b.

That is, as Petitioner argues, "[t]he Petition explains" that "Duvall already suggests that the user, such as trained professionals, should have

access to *past network activity to accurately update filters*, Ex. 1004, 8:2–7, and Trcka's analysis applications would enable the user to interact with such information as part of the user's analysis." Reply 20 (quoting Pet. 51; citing Ex. 1003 ¶ 186). Therefore, contrary to Patent Owner's arguments, as explained above, and as Petitioner explains in connection with limitations 1.b–1.e and claim 6, Duvall's system provides for manual user-editor updates to provide dynamic modification based on stored data and feedback. *See supra* §§ III.A.3.f; III.A.4.b.

Therefore, as Petitioner shows, it follows that Trcka's system for analyzing archived data naturally fits into Duvall-Chu's scheme ultimately in determining whether the system is filtering too much or too little, including when the combined system analyzes archived data at identifying limitation 1.b stage or after transmitting information to an analyst system at limitation 1.c. *See* Pet. 51 ("A POSA would have been motivated to incorporate Trcka's techniques for recording and viewing past network activity in Duvall-Chu's system to enable the user to analyze whether "the filtering system is 'filtering too much or too little.'" (quoting Ex. 1004, 8:5–7; Ex 1003 ¶ 186)).

That is, the record does not support Patent Owner's argument that Petitioner's showing is faulty because it does not consider how Trcka's system fits into different stages of the analysis, namely at 1) limitation 1.b (the identifying limitation at the probe to which claims 7–9, 12 and 13 relate), and 2) an analysis at the SOC that occurs "*after* the 'identifying step,'" to which claims 10 and 11 relate). *See* PO Resp. 43; *see also id.* at 46–48 (similar argument). In other words, as set forth above, Trcka's system naturally fits into Duvall's system at various stages including those that pertain to limitations 1.b and "after" limitation 1.c. Petitioner further

supports this finding by noting that "Duvall and Trcka . . . operate upon similar traffic data, ensuring that Trcka's analysis techniques would apply equally well to the data in Duvall-Chu's system." Pet. 51 (citing Ex 1003 ¶¶ 186; Ex. 1004, 3:64-4:55; Ex. 1014 ¶¶ 38–39).

Additionally, contrary to Patent Owner's arguments, as summarized above, Petitioner shows how Trcka's scheme naturally fits into the claimed stages for each claim. *See* Reply 21 ("The Petition and Dr. Jeffay explain, for each specific claim, where Trcka's techniques would be incorporated into the Duvall-Chu system.").

As one example, Petitioner points to its showing for claim 10, which relies on Duvall's corporate network as an SOC to apply Trcka's "analysis applications," as summarized above. *See* Reply 21 (citing Pet. 54–56; Ex. 1003 ¶¶ 197–198).

As another example for applying Trcka's analysis techniques to the "identifying step," which claims 7, 8, and 12 recite, Petitioner specifically states that a "POSA would have understood that Trcka's aggregation and synthesis occurs '*at the probe*' where the data would be stored." Pet. 53 –54 (citing Pet. § VI.B.1; Ex. 1003 ¶ 191).

As another example, for claim 16, Petitioner demonstrates how Trcka's system further enables Duvall-Chu's system at a specific analysis point in Duvall's system (its modification control system/editing manager at the probe) relative to limitation 1.e to provide the ultimate determination of whether or when to modify filters accordingly in order to identify potential security threats. *See supra* § III.A.3.f (limitation 1.e).

Therefore, a review of the Petition shows that it accounts for different aspects of the Duvall-Chu combination for each of claims 7–14 and 16 by pointing out that the analysis occurs either at the probe (for dependent

claims 7–9, 12, and 13, which recite "the identifying step," limitation 1.b), or at the SOC (for dependent claims 10–11 and 14, which recite "after the step (c)"), or at the "dynamic modifying step," limitation 1.e (for dependent claim 16). Pet. 52–58.[20]

Patent Owner also argues that "for Trcka's analysis to work in a SOC, not only does the SOC need access to the raw traffic, but every single packet sent or received on the network must also be accessible from the SOC." *Id.* at 48. Patent Owner also argues that privacy and security concerns (e.g., providing a third-party at the SOC access to a corporations raw data), and bandwidth concerns (e.g., sending archived packets), all dictate against modifying Duvall-Chu to include Trcka's teachings because "an attacker would have full visibility into the corporate network" and in transmitting raw packets from Trcka's archive to the SOC. *See id.* at 48–50.

These arguments are unavailing. As Petitioner shows, "Duvall's 'corporate network' . . . provides a 'secure operations center' within which analysis can be performed, and any form of remote access would employ secure communications, alleviating purported security and privacy concerns." *See* Reply 21 (citing Pet. 45, 54–55; Ex. 1003 ¶¶ 171, 179). As noted above, Trcka's title is "Network Security and Surveillance System." Ex. 1014, code (54). Trcka's states that it its "network security and surveillance system passively monitors and records the traffic present on a local area network, wide area network, *or other type of computer network*," and "[r]aw data packets present on the network are continuously routed (with optional packet encryption)." *Id.* at code (57) (emphasis added).

[20] As indicated above, the Petitioner analyzes claims 14 and 15 in another ground. Claim 15 does not refer to a previous "step" in claim 1.

With respect to alleged bandwidth concerns because of raw packet transmission, as noted, Trcka indicates there are no bandwidth concerns because "[r]aw data packets present on the network are continuously routed (with optional packet encryption) to a high-capacity data recorder." Ex. 1014, code (57). Nonetheless, Patent Owner contends that "at the time of invention the cost of bandwidth was many times what it is today." PO Resp. 50 (citing Ex. 2016 ¶ 183). Patent Owner also argues that "POSA would thus not have found it obvious to double its network bandwidth at the time just to incorporate Trcka's analysis in a SOC." *Id.* (citing Ex. 2016 ¶ 183). As such, Patent Owner essentially argues that the cost of implementing Trcka's system, based on bandwidth, is twice the cost without it.

As Petitioner argues, however, these concerns, like Patent Owner's allegation of privacy concerns, "are unrelated to any 'technological incompatibility' that would prevent the Duvall-Chu-Trcka combination." Reply 22 (citing *Grit Energy Sols., LLC v. Oren Techs., LLC*, 957 F.3d 1309, 1323 (Fed. Cir. 2020) (noting that only "technological incompatibility" is relevant to the obviousness inquiry; whether "businessmen" would combine two references "for economic reasons" is irrelevant). To the extent bandwidth, cost, and privacy are relevant in obviousness inquiries, such concerns are either simply trade-off concerns that an artisan of ordinary skill readily would have considered, or are beyond the scope of the challenged claims, which do not recite any bandwidth, cost, or privacy limitations.

Patent Owner also argues that "if Duvall was incorporated into a firewall, Trcka's techniques would also be unable to distinguish between the firewall and Duvall's filtering system." PO Resp. 42 (citing Ex. 2016

¶ 159). Patent Owner similarly argues that there is no reasonable expectation of success in the combination. *See id.* ("There is thus no disclosure of how a POSA could 'incorporate Trcka's techniques . . . to enable the user to analyze whether 'the filtering system is filtering too much or too little.' EX1003, ¶186. Because of these issues, a POSA would have lacked a reasonable expectation of success in combining Trcka with Duvall-Chu for this specifically-alleged purpose. EX2016, ¶159.").

Patent Owner's arguments rest on its unavailing and faulty analysis of how Petitioner combines Trcka with Duvall-Chu. Petitioner does not rely on Trcka to distinguish between a firewall and Duvall's filtering system. Also, with respect to claim 6, Petitioner explains that Duvall discloses that "its filtering system can 'be incorporated into a firewall [or] gateway.'" Pet. 45 (citing Ex. 1004, 1:60–64). Petitioner explains that Duvall further recognizes security issues by "preferably" providing "password protect[ion]" to access its editing manager and filters. *Id.* (quoting Ex. 1004, 8:2–9; citing Ex. 1004, 8:21–23). Petitioner further explains that "[a] POSA would have recognized that accessing a firewall or gateway can be, and most typically is, accessed remotely, e.g., from a separate "network operations center." *Id.* (citing Ex. 1003 ¶ 171; Ex. 1037, 277). Therefore, Petitioner submits that "a POSA would have recognized that the security analyst system would likewise be secure, including communications between the analyst system and the firewall (e.g., through HTTPS, SSL, TLS, etc.)," and the corporate analyst system (e.g. editing manager) behind the firewall. *See id.* (citing Ex. 1003 ¶ 171).

Therefore, based on the evidence outlined above and relied upon by Petitioner, we find that incorporating portions of Duvall's system (its stored filtering system and/or editing manager) behind a firewall to maintain

security and render its corporate analyst system accessible via a third-party secure operations center while using Trcka's analysis techniques to improve the filtering analysis would have amounted to "nothing more than combining prior-art elements (i.e., Duvall-Chu's filtering system and editing manager with Trcka's data-analysis applications) according to known methods to yield predictable results." *See* Pet. 51–52 (citing Ex. 1003 ¶ 187; *KSR*, 550 U.S. at 417); Ex. 1003 ¶ 187 ("Implementing Trcka's analysis techniques in the Duvall-Chu system amounts to nothing more than combining prior-art elements (i.e., Duvall-Chu's filtering system and editing manager and Trcka's data-analysis applications) according to known methods to yield predictable results.").

c) Summary of Claims 7–13 and 16

As found above, the record shows that no presumption of nexus exists and no nexus exists between Patent Owner's evidence of objective indicia of nonobviousness and the claimed invention. Even if a weak nexus exists, Petitioner's showing of obviousness outweighs the evidence of nonobviousness. On the full record, after weighing the arguments and evidence as set forth in the parties' briefs, including that related to secondary considerations of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claims 7–13 and 16 would have been obvious.

C. Alleged Obviousness of Claims 14 and 15 in view of Duvall, Chu, Trcka, and Ziese

Petitioner contends that claims 14 and 15 would have been obvious over the combination of Duvall, Chu, Trcka, and Ziese. *See* Pet. 58–63. Patent Owner disagrees, arguing that it would not have been obvious to

employ Ziese's servers in Duvall-Chu-Trcka's system. PO Resp. 50–54; Sur-reply 27.

1. Ziese

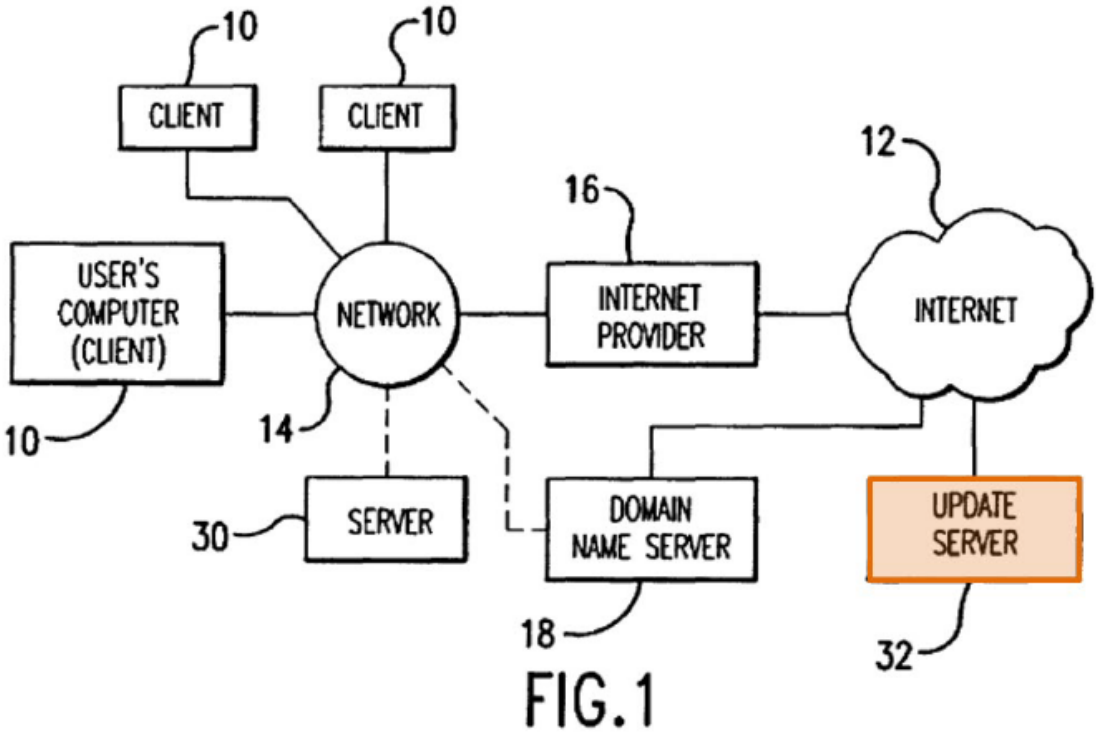
Ziese is a U.S. Patent titled "Method and System for Dynamically Distributing Updates in a Network." Ex. 1015, codes (10), (54). Ziese discloses "dynamically distributing intrusion detection and other types of updates in a network that substantially eliminate or reduce disadvantages and problems associated with prior methods and systems." *Id.* at 2:2–6. According to Ziese, "programs are automatically updated by downloading and distributing an update in response to an automated event," and "[a]s a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction." *Id.* at 2:39–44.

2. Analysis of Claims 14 and 15

Claim 14 recites "[t]he system of claim 10, wherein the computer-based analysis includes cross-probe correlation." Claim 15 recites "[t]he system of claim 1, further comprising instantaneous self-tuning the probe based on previously collected status data."

Petitioner contends that it would have been obvious to implement Duvall's server 30, which serves multiple clients in a client-server architecture (10, 30), within a corporate network at a single network site, in a distributed setting, based on Ziese's teachings, so that each of Duvall's client-server architectures are present at each disparate network site.

Duvall's Figure 1, a block diagram of Duvall's client-server system, as annotated by Petitioner, follows:



EX1004, FIG. 1 (annotated).

Duvall's Figure 1, as annotated by Petitioner, illustrates Duvall's client-server architecture (10, 30) on the left attached to update server 32 on the right (annotated in brown) connected via Internet 12. Petitioner explains that "Duvall already suggests the use of centralized update [from update server 32], further disclosing (similar to Ziese) an 'updating mechanism' for distributing filter updates to its filtering system "over the Internet." Pet. 61 (citing Ex. 1004, 7:15–67; Fig. 1).

The Petition explains that Ziese discloses "[p]rivate networks, such as company intranets," may be distributed over "wide area networks (WANs)" that include "disparate network sites." Pet. 58 (citing Ex. 1015, 1:26–31, 2:29–26). Duvall, on the other hand, applies to a "corporate network" at a single network site, disclosing a "server 30 that is on the client's own

network," as shown in Duvall's Figure 1. *Id.* at 58–60 (citing Ex. 1004, 8:18–24).

In other words, "Petitioner's combination . . . addresses the case of a distributed corporate network, as taught by Ziese." Reply 23. According to Petitioner, this would "ensure that [Duvall-Chu-Trcka's] filtering system applies filters to data transmissions before the transmission is allowed to enter a public network, such as the Internet." Pet. 58–60 (citing Ex. 1003 ¶¶ 207–210). Petitioner indicates that the combination would have improved Duvall-Chu's system because, for example, "[a]s a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction." *See id.* at 59 (quoting Ex. 1015, 2:39–44). The Petition similarly explains that instead of updating Duvall's editing manager on each local server, "i.e., updates that would apply to all clients within a corporation," "Ziese's techniques resolve this problem, allowing updates to be made centrally and automatically distributed to 'disparate network sites.'" *Id.* at 60 (citing Ex. 1015, 2:25–46).

Patent Owner argues that Petitioner's combination requires modifying Duvall to include additional servers and Duvall teaches away from additional servers. PO Resp. 51. Contrary to this line of argument, however, as Petitioner argues and as summarized above, "the proposed combination does not require modifying Duvall to include additional servers—it merely addresses the scenario where Duvall's architecture is implemented at multiple network sites." Reply 22 (citing Pet. 58–62).

Patent Owner responds that "Petitioner's 'scenario' is neither disclosed nor inherent," and "[t]hus Petitioner's lack of motivation for this modification is fatal." Sur-reply 27. This argument does not address

Petitioner's stated persuasive rationale that the combination provides for central automatic updates to different servers at distributed locations, which Duvall already suggests via its update server, resulting in providing uniform updates to all clients from one location with minimal operator interaction and ensuring secure connections to the Internet at each location.

Based on the record, we determine that claims 14 and 15 would have been obvious. *See* Pet. 58–63.

3. Summary

As found above, the record shows that no presumption of nexus exists and no nexus exists between Patent Owner's evidence of objective indicia of nonobviousness and the claimed invention. Even if some weak nexus exists, Petitioner's showing of obviousness outweighs the evidence of nonobviousness. On the full record, after weighing the arguments and evidence as set forth in the parties' briefs, including that related to secondary considerations of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claims 14 and 15 would have been obvious.

D. Alleged Obviousness of Claims 18–25 in view of Duvall, Chu, and Cogger

Petitioner contends that claims 18–25 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, and Cogger. Pet. 67–84. Claim 18 is independent. *See supra* § II.D (reproducing claim 18). Claims 19–25 depend from claim 18. Patent Owner disputes Petitioner's contentions, grouping the claims together, and arguing that it would not have been obvious to implement Cogger's CSM and problem ticket teachings with Duvall-Chu's combined system. PO Resp. 54–60.

1. Cogger (Ex. 1033)

Cogger is a U.S. Patent titled "Integrated Interface for Web Based Customer Care and Trouble Management." Ex. 1033, codes (10), (54). Cogger relates to "opening and tracking trouble tickets over the public Internet." *Id.* at 2:50–52. According to Cogger, "customer profile information is used to prepopulate data fields in dialogs used to open a trouble ticket." *Id.* at 2:56–57. "Once a trouble ticket is opened, the customer workstation tracks the existing trouble tickets through a browser based graphical user interface." *Id.* at 2:58–60.

Figure 8(g) of Cogger is an illustration of a graphical interface for implementing tickets and follows:

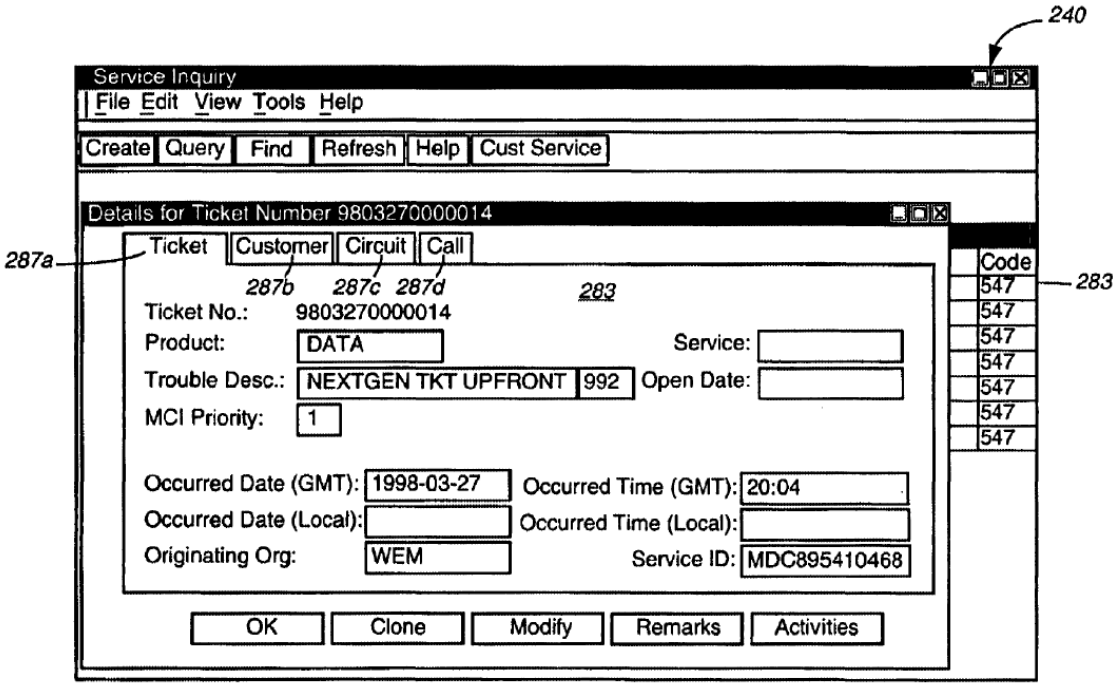


FIG. 8(g)

Figure 8(g) depicts a "graphical user interface[] that may be presented to a customer for opening a new and querying an existing trouble ticket." Ex. 1033, 4:49–51. More specifically, Figure 8(g) depicts a "Details" window 283 that includes selectable tabs comprising information about a

selected ticket. *Id.* at 20:3–6. According to Cogger, "selection of the ticket tab 287a . . . provides ticket information including: ticket number, ticket product, ticket service, date occurred, trouble description, and organization (ORG) code, etc." *Id.* at 20:7–10. Further, "[t]he customer tab 287b, circuit tab 287c, and call tab 287d . . . provide additional detailed information including: ticket priority, ticket status, ticket identifier, etc." *Id.* at 20:10–13. Cogger discloses that "the number of data elements will be different for different types of tickets." *Id.* at 20:13–15.

2. Analysis of Claims 18–25

The preamble and first step of claim 18 follow:

> 18, A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:
>
> creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering . . . .

Petitioner primarily relies on its analysis of claim 1 as outlined above to address the preamble and identifying the potentially security related events as recited in the "creating" step of claim 18 above. *See* Pet. 67–69 (citing Pet. § VI.A..2(a)). With respect to the "secure operations center" (SOC) as recited in the preamble, to the extent it is limiting, Petitioner reads it partly on Cogger's Customer Service Management System (CSM), contending it would have been obvious for Cogger's CSM to which receive trouble tickets from different security analysts at corporate networks in the Duvall-Chu system, in order to better track, evaluate, and resolve security

issues, as described further below. *See id.* at 64–67 (citing Ex. 1033, 2:50–3:3, 3:65–66; Ex. 1003 ¶¶ 224–230).

Petitioner explains that Duvall recognizes that "Internet sites are being added to the Internet at a fast rate," and reasons that "a corporation may not have the resources to keep its filtering up to date." Pet. 64 (first quote quoting Ex. 1004, 7:16–29). Therefore, Petitioner contends that a person of ordinary skill "would have been motivated to adapt Duvall in view of Chu to process residue data by a third party having [the] expertise," such as a third party managing Cogger's CSM, because the third party would "have more expertise in identifying what data transmissions to allow and what data transmissions to block" in processing Duvall-Chu's residue information. *See id.* (citing Ex. 1003 ¶ 220).

With respect to the "event record" as recited in the first step of claim 18, Petitioner also asserts that a person of ordinary skill "would have understood that the transmitted information [in the Duvall-Chu system and as recited in limitations 1.b and 1.c] is 'an event record' because it is information about the network event." Pet. 69 (citing Ex. 1003 ¶ 232).

Patent Owner relies on its unavailing arguments addressed above with respect to claim 1's analysis of post-filtering residue. *See* PO Resp. 26–29. We address Patent Owner's arguments with respect to creating an event record as introduced in the above step of 18 and discuss the remaining steps of claim 18 next.

That is, the remaining steps of claim 18 include "event record" and "trouble ticket" limitations, which involve "correlating," "using," and "consolidating" the event record information with other information/records ultimately into a "problem ticket" and "providing" same to a "security analysis console for analysis":

> correlating the event record with customer information and a symptom record;
>
> using the correlated symptom record to link the event record to problem resolution information;
>
> consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and
>
> providing the problem ticket to a security analyst console for analysis.

To address the above limitations, Petitioner turns to Cogger for its "trouble ticket techniques" and incorporates them into "Duvall-Chu's system to prompt a network administrator, as disclosed in Cogger, to resolve residue data transmissions." *See* Pet. 67 (citing Ex. 1003 ¶ 228; Pet. § II.I.5 (summarizing Cogger's teachings)).

Further addressing reasons to combine Cogger's secure CSM ticket system with Duvall-Chu (and the preamble's "secure operations center"), Petitioner contends that "Cogger discloses '*operating a secure operations center*' in the form of a 'Customer Service Management System' (CSM) that receives trouble tickets transmitted from customers." Pet. 67 (second quote quoting Ex. 1033, 3:65–66; citing Ex. 1003 ¶ 229). Petitioner relies on Cogger's "disclos[ure] that communication between customers and the CSM is 'secure,' providing 'secure web servers and back end services to provide applications that establish user sessions . . . and communicate with adaptor programs to simplify the interchange of data across the network.'" *Id.* (emphases omitted) (quoting Ex. 1033, 5:46–50; citing *id.* at 7:55–60 (describing secure TCP messaging over secure Internet paths); Ex. 1003 ¶ 229).

Petitioner explains that "[i]n the Duvall-Chu-Cogger system, Cogger's CSM would be implemented as part of Duvall-Chu's network-administrator

resolution pathway for receiving and analyzing tickets transmitted from subscriber networks." Pet. 68 (citing Ex. 1003 ¶ 230; Pet. § VI.D.1). According further to Petitioner, "Duvall-Chu-Cogger's [resulting] residue data-review system" is "like Cogger's CSM," as it suggests "*a secure operations center as part of a security monitoring system for a customer computer network*." *Id.* (citing Ex 1003 ¶ 230). Petitioner adds that a person of ordinary skill in the art "would have been motivated to ensure personnel operating Duvall-Chu-Cogger's service were doing so securely because the service would receive network activity from private customer networks (e.g., 'a corporate network')." *Id.* (citing Ex. 1004, 8:21–23; Ex. 1003 ¶ 231).

Petitioner adds that a person of ordinary skill in the art "would have been motivated to incorporate such information into a 'trouble ticket,' as in Cogger, to efficiently and coherently provide the information to a trained professional (e.g., Cogger's network administrators [at the CSM])." Pet. 69 (citing Ex. 1003 ¶ 233). Petitioner also argues that "[t]he information as recorded in the trouble ticket thus also provides 'an event record.'" *Id.* (citing Ex. 1003 ¶ 233).

Petitioner reads the remaining limitations in the "correlating" step, the "using" step," the "consolidating" step, and the "providing" step, onto Cogger's ticket teachings. *See* Pet. 69–75. Petitioner's showing is persuasive regarding the information and records that the problem ticket requires in claim 18. *See* Pet. 65 (noting Cogger's trouble ticket s customizable and "will be different for different types of tickets" (quoting Ex. 1033, 20:13–15; reproducing *id.* at Fig. 8g (trouble ticket)), 69–75 (addressing the information and records of the claim steps based on citations to Cogger).

Regarding Petitioner's problem ticket showing, Patent Owner concedes that Petitioner's expert suggests that Duvall-Chu-Cogger teaches "'consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket,' because Cogger discloses such information in its problem tickets." PO Resp. 58 (quoting Ex. 1003 ¶ 242). And Patent Owner concedes that "Cogger's problem tickets contain such information." *Id.* In other words, Patent Owner concedes that the various types of information and records as recited in the noted steps of claim 18 to form the recited problem ticket. *See id.* Based on a review of the record and as summarized above, Patent Owner's concessions corroborate Petitioner's persuasive trouble ticket showing.

However, Patent Owner contends that Cogger does not describe its CMS in sufficient detail. *See* PO Resp. 57 ("Cogger's CSM is just a black box" (citing Ex. 2016 ¶¶ 198–206)). Based on this contention, Patent Owner further contends that "Cogger does not disclose any systems or processes allowing a customer service representative to access or use the CSM." *Id.* Therefore, Patent Owner contends that "Petitioner's expert's suggestion that 'a POSA would have implemented Cogger's CSM' is . . . unsupported by evidence." *Id.* at 58.

Patent Owner also argues that "Cogger does not disclose any systems or processes used to create, store, or manage the trouble tickets in the CSM." PO Resp. 58. According to Patent Owner, "Petitioner's expert fails to show how Duvall-Chu could be modified to populate such information in the problem tickets." *Id.*; *accord* Sur-reply 24 (similar arguments).

These arguments are unavailing. As Petitioner recognizes, Patent Owner's arguments in part essentially assert a lack of enablement of

Cogger's CSM ticket teachings. *See* Pet. PO Resp. 55–57; Reply 23–25. As Petitioner also recognizes, there is no absolute requirement for an obviousness reference to be self-enabling. *See* Reply 24 (citing *Symbol Techs., Inc. v. Opticon, Inc.*, 935 F.2d 1569 (Fed. Cir. 1991); *KSR*, 550 U.S. at 406); *Symbol Techs.*, 935 F.3d at 1578 ("a non-enabling reference may qualify as prior art for the purpose of determining obviousness under § 103") (citing *Reading & Bates Constr. Co. v. Baker Energy Resources Corp.*, 748 F.2d 645, 652 (Fed. Cir. 1984) (reference that lacks enabling disclosure is not anticipating, but "itself may qualify as a prior art *reference* under § 103, but only for what is disclosed in it"); *Beckman Instruments, Inc. v. LKB Produkter AB*, 892 F.2d 1547, 1551, (Fed. Cir. 1989) ("Even if a reference discloses an inoperative device, it is prior art for all that it teaches")); *Raytheon Techs. Corp. v. General Elec. Co.*, 993 F.3d 1374 (Fed. Cir. 2021) ("We have explained that there is no absolute requirement for a relied-upon reference to be self-enabling in the § 103 context, so long as the overall evidence of what was known at the time of invention establishes that a skilled artisan could have made and used the claimed invention.").

And even if enablement of Cogger's CSM ticket teachings were relevant here, as a prior art reference, Cogger carries a presumption of enablement. *See In re Antor Media*, 689 F.3d 1282, 1287–1288 (Fed. Cir. 2012); *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1355 (Fed. Cir. 2003); *Apple Inc. v. Corephotonics, Ltd.*, No. 2020-1438, 2021 WL 2577597, at *4 (Fed. Cir. 2021) (holding that in the context of AIA trial proceedings, "regardless of the forum, prior art patents and publications enjoy a presumption of enablement, and the patentee/applicant has the burden to prove nonenablement for such prior art" and that "[i]t was error for the Board to suggest otherwise"). Nonetheless, the ultimate burden

remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

In any event, the Petition shows that an artisan of ordinary skill, relying on sufficient detail in Cogger, enables the functionality of a CSM, including relative to its ticketing system. *See* Reply 25 (citing Pet. 64–74; Ex. 1033, 17:50–26:62, Figs. 8(a)–8(k)). And as summarized above, Petitioner provides persuasive reasons to turn to Cogger and implement Cogger's CM ticket teachings with Duvall-Chu's system with a reasonable expectation of success. Pet. 64–67. For example, Petitioner argues that "Cogger's trouble tickets would . . . provide a tracking mechanism to Duvall's network administrators of each corporate network to assure residue data is resolved in a timely manner." *Id.* at 66 (citing Ex. 1033, 2:50–3:3; Ex. 1003 ¶ 224). Petitioner also argues that a person of ordinary skill in the art "would have been motivated to incorporate Cogger's techniques for generating and transmitting trouble tickets in Duvall-Chu's system for use in prompting Cogger's network administrators to resolve residue data." *Id.* at 65 (citing Ex. 1003 ¶ 224). Petitioner also argues that "[t]ransmitting 'trouble tickets' with sufficient information about residue data to . . . network administrators would ensure that the service can appropriately evaluate and resolve such data transmission." *Id*. at 65–66 (citing Ex. 1003 ¶ 224). Petitioner adds that "[t]his would allow . . . network administrators to efficiently update the corporation's filter database as appropriate, adding new filters to address newly-discovered Internet sites." *Id.* at 66 (citing Ex. 1003 ¶ 224).

Contrary to Patent Owner's argument that Cogger only teaches an interface and lacks specifics (PO Resp. 55–56), Patent Owner contradicts itself by arguing that "Cogger relies on a complex pre-existing architecture

and a suite of other pre-existing telecommunications applications." Prelim. Resp. 69 (citing Ex. 1033, 1:32–36; 6:8–14; 13:66–14:17). Even if Cogger lacks certain specifics, the asserted lack of specifics is further evidence on this record that an artisan of ordinary skill already would have known how to implement Cogger's CSM and ticketing system with Duvall-Chu's system with a reasonable expectation of success.

As Patent Owner shows by virtue of annotating Cogger's Figure 2, Cogger's CSM 40 simply connects via interface servers in an MCI Intranet to web servers and a customer's browser over the Internet. *See* PO Resp. 56 (annotating Ex. 1033, Fig. 2). Patent Owner admits that "[a]t best, Cogger . . . discloses *how a customer can access the CSM remotely through its disclosed interface*." *Id.* at 57 (emphasis added). As summarized above, Petitioner shows persuasively that "Duvall-Chu-Cogger's residue data-review system, like Cogger's CSM, provides 'a secure operations center as part of a security monitoring system for a customer computer network.'" Pet. 68. As addressed in connection with claim 6, as Petitioner shows, the combined teachings of Duvall-Chu in light of the knowledge of an artisan of ordinary skill reveal how and why to implement an SOC, which is like Cogger's CSM.

Moreover, Patent Owner notes that Cogger describes its CSM as a "legacy host system." PO Resp. 56 (quoting Ex. 1033, 13:22–24; analyzing Ex. 1033, Fig. 2). Cogger thus implies that an artisan of ordinary skill readily would been able to implement the functionality of a CSM, because as a legacy system, such an artisan would not require any more than Cogger discloses to implement in a similar system such as that of Duvall-Chu. Moreover, "[a]s discussed for [limitation 1.c], Duvall already teaches

providing an 'analyst system' to network administrators to view information about network events." Pet. 75.

Regarding Patent Owner's argument that Petitioner fails to show how to combine Cogger's CSM ticket teachings (PO Resp. 55–60), Petitioner shows that "Cogger's CSM would be implemented as part of Duvall-Chu's network-administrator resolution pathway for receiving and analyzing tickets transmitted from subscriber networks." Pet. 68 (citing Ex. 1003 ¶ 230; Pet. § VI.D.1). Petitioner also shows that the Duvall-Chu combination sends tickets from analysts at corporate network computers to expert analysts at Cogger's CSM for the purpose of optimizing and providing uniform security resolution and tracking across the network. *See* Pet. 64–67; Reply 25 ("[C]ontrary to [Patent Owner]'s assertions, the combination provides an opportunity for 'customer' network administrators [in Duvall-Chu] to assist with creation of trouble tickets before they are transmitted for resolution [to Cogger's CSM]."). As outlined above, the record supports Petitioner's showing.

Moreover, as noted above, Patent Owner admits that "[a]t best, Cogger . . . discloses how a customer can access the CSM remotely through its disclosed interface." PO Resp. 57. Patent Owner also describes Cogger's "customer" analysts as "manually populat[ing] a majority of the information in its problem tickets." *Id.* at 59 (citing Ex. 1033, 21:27–41). And Patent Owner admits that Cogger's "problem tickets contain [claim 18's recited] information" as outlined by Dr. Jeffay. *See* PO Resp. 58 (discussing Ex. 1003 ¶ 242). Patent Owner's arguments and concessions corroborate Petitioner's persuasive showing that person of ordinary skill would have recognized that a customer analyst at corporate network computers readily would and could have prepared (manually or otherwise) and send problem

tickets as recited in claim 18 to expert analysts at Cogger's CSM for the purpose of optimizing and providing uniform security resolution and tracking across the network with a reasonable expectation of success. *See* Pet. 64–67. Accordingly, contrary to Patent Owner's arguments, Petitioner's showing is not "generic" and it "bears" a specific "relation to . . . [a] specific combination of prior art elements." *See* PO Resp. 60 (quoting *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012)).

Finally, claim 18 is a broad claim and does not require the claimed security analyst to resolve any network problems. Rather, claim 18 recites "providing the problem ticket to a security analyst console *for analysis*," which merely amounts to an intended use of the ticket at a console, without specifying any particular analysis of the recited ticket information, let alone a resolution of the ticket's stated problem. As Petitioner shows with respect to claims 1 and 18, Duvall's and Chu's combined system already provides information and feedback about security issues on a network to analysts/users as part of an "analyst system," as outlined above in connection with claim 1. *See, e.g.*, Pet. 40–42 (addressing feedback in Duvall), 67 ("Chu, for example, already discloses alerting a user with expertise to resolve residue data." (citing Ex. 1005, 44)); Ex. 1004, 5:62–65 (providing feedback to a user's screen)).

In any case, even if claim 18 requires some analysis, as indicated above, Petitioner shows that Cogger teaches a "problem ticket" submitted to the CSM and that a person of ordinary skill in the art "would have been motivated to provide a similar 'analyst console' to analysts operating Duval-Chu-Cogger's service to analyze event information received in a trouble ticket and update filters as appropriate." Pet. 74. And "the remarks included

in the trouble ticket would allow a client user or network administrator to add further commentary for use by the Duvall-Chu-Cogger's service in determining how to resolve the received event." *Id.* at 73 (describing the process for allowing residue data with a legitimate URL) (citing Ex. 1003 ¶ 239)).

On the full record, after weighing the arguments and evidence, including evidence of objective indicia of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claim 18 would have been obvious.

Turning to dependent claims 19–25, having weighing the arguments and supporting evidence on this record, including evidence of secondary considerations and the arguments as summarized above for claims 1 and 18, we determine that Petitioner shows by a preponderance of evidence that claim 19–25 would have been obvious. *See* Pet. 75–85. Patent Owner does not separately address Petitioner's showing with respect to these claims. *See* PO Resp. 54–60 (grouping claims 18–25 together).

3. Summary of Claims 18–25

As found above, the record shows that no presumption of nexus exists and no nexus exists between Patent Owner's evidence of objective indicia of nonobviousness and the claimed invention. Even if a weak nexus exists, Petitioner's showing of obviousness outweighs the evidence of nonobviousness. On the full record, after weighing the arguments and evidence as set forth in the parties' briefs, including that related to objective indicia of nonobviousness, we determine that Petitioner shows by a preponderance of evidence that claims 18–25 would have been obvious.

IV. CONCLUSION

For the reasons discussed above, Petitioner has shown by a preponderance of the evidence that claims 1–25 of the '641 patent are unpatentable.[21] The following table summarizes our conclusions:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1–7, 15–17	103(a)	Duvall, Chu	1–7, 15–17	
7–13, 16	103(a)	Duvall, Chu, Trcka	7–13, 16	
14, 15	103(a)	Duvall, Chu, Trcka, Ziese	14, 15	
18–25	103(a)	Duvall, Chu, Cogger	18–25	
Overall Outcome			1–25	

[21] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3),(b)(2).

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that Petitioner establishes by a preponderance of evidence that challenged claims 1–25 are unpatentable; and

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

PETITIONER:

Jonathan Tuminaro
Dan Block
Michael Specht
Steven Pappas
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
jtuminar-ptab@sternekessler.com
dblock-ptab@sternekessler.com
mspecht-ptab@sternekessler.com
spappas-ptab@sternekessler.com

PATENT OWNER:

Nolan M. Goldberg
Baldassare Vinti
PROSKAUER ROSE LLP
NGoldbergPTABMatters@proskauer.com
BVinti@proskauer.com

Jonathan A. Roberts
Raymond Y. Mah
Joseph A. Rhoa
NIXON & VANDERHYE P.C.
jr@nixonvan.com
rym@nixonvan.com
jar@nixonvan.com