

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE INC.,
Patent Owner.

IPR2023-00821
Patent 10,699,008 B2

Before KEVIN F. TURNER, JOHN D. HAMANN, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

BELISLE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

IriusRisk, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–20 (“Challenged Claims”) of U.S. Patent No. 10,699,008 B2 (Ex. 1001, “the ’008 patent”). ThreatModeler Software, Inc. (“Patent Owner”) filed a Preliminary Response to the Petition. Paper 6 (“Prelim. Resp.”). We instituted an *inter partes* review of claims 1–20 of the ’008 patent on all grounds of unpatentability alleged in the Petition. Paper 7 (“Institution Decision” or “Dec.”).

After institution, Patent Owner filed a Response. Paper 18 (“PO Resp.”). Petitioner filed a Reply. Paper 21 (“Pet. Reply”). Patent Owner filed a Sur-reply. Paper 22 (“PO Sur-reply”). We held an oral hearing in this case on August 14, 2024, and a transcript of the hearing is included in the record. Paper 28 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6 (2018). Under the applicable evidentiary standard, Petitioner has the burden to prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d) (2022). “Preponderance of the evidence means the greater weight of evidence, evidence which is more convincing than the evidence which is offered in opposition to it.” *United States v. C.H. Robinson Co.*, 760 F.3d 1376, 1383 (Fed. Cir. 2014) (internal quotations omitted). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed below, we determine Petitioner has established by a preponderance of the evidence that claims 1–20 of the ’008 patent are unpatentable.

II. BACKGROUND

A. Related Matters

At the time of the Petition’s filing, the parties indicated that the ’008 patent was involved in one U.S. district court action, namely, *ThreatModeler Software Inc v. IriusRisk, Inc.*, Case No. 1:22-cv-912-MN (D. Del.) (“District Court Case”). Pet. 1; Paper 3, 2.

Petitioner also indicated that Patent Owner asserts related U.S. Patent No. 10,713,366 B2 (“the ’366 patent”) against Petitioner in the District Court Case. Pet. 1. The ’366 patent is the challenged patent in IPR2023-00656, in which we determined Petitioner had not established by a preponderance of the evidence that any of claims 1–20 of the ’366 patent was unpatentable. *See IriusRisk Inc. v. ThreatModeler Software, Inc.*, IPR2023-00656, Paper 33 (PTAB Oct. 2, 2024).

B. The ’008 Patent

The ’008 patent is titled “Threat Model Chaining and Attack Simulation Systems and Related Methods,” and issued June 30, 2020, from U.S. Patent Application No. 16/228,738, filed December 20, 2018, and claims priority through a series of continuation-in-part applications to four U.S. Provisional Patent Applications filed in 2017 (priority is not at issue in this proceeding). Ex. 1001, codes (10), (21), (22), (45), (54), (63).

The ’008 patent generally relates to “threat modeling processes and systems,” where “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized,” and “[t]hreat modeling allows a user to analyze potential attack vectors and prioritize vulnerabilities.” Ex. 1001, 1:43–54.

Threat model chaining methods include providing one or more databases including . . . threat model components, threats, each threat associated with at least one of the threat model components, and compensating controls, each compensating control associate[d] with one of the threats, providing a diagram interface configured to display a relational diagram defining a first threat model, and configuring the diagram interface to add a component group to the first threat model [and] include in it a second threat model. Attack simulation methods include providing the one or more databases and diagram interface and configuring the diagram interface to visually display attack paths of threats associated with diagrammed threat model components which compromise a selected threat model component. Attack simulation systems include one or more computing devices coupled with one or more databases configured to store and interrelate threats, threat model components, and compensating controls, and allow diagramming and defining of threat models.

Id. at code (57). According to the '008 patent, its system(s) and method(s) can generate threat models “for any application, process, or system under consideration,” including “modeling the possible threats to commuting to work safely, modeling the possible threats to preventing the spread of an infectious disease, or modeling the possible attacks on a computer network (cybersecurity).” *Id.* at 8:38–49.

The '008 patent describes process 200 storing a plurality of threats 202 and threat model components 204 in a data store 206, where threats 202 and components 204 are used to create threat model 208 and ultimately, threat report 214, as shown, for example, in Figure 2, reproduced below. Ex. 1001, 8:50–9:6, Fig. 2.

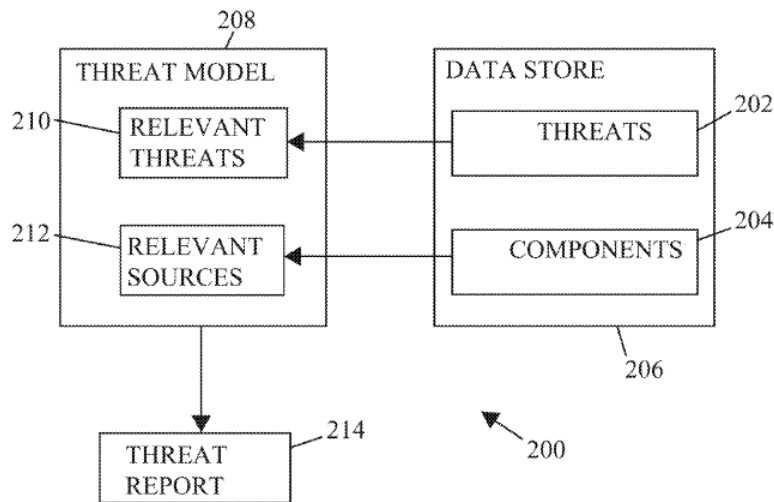


Figure 2 depicts a representative example of a threat modeling process.

Id. at 8:38–39, Fig. 2. Each threat model component “is a potential relevant source for one or more threats.” *Id.* at 9:28–30. For example, “one threat may be ‘Bluejacking’ and one component, which would be correlated to this threat through the database, could be [a] ‘BLUETOOTH port.’” *Id.* at 9:30–32; *see id.* at 9:32–61. The ’008 patent also describes “compensating controls” stored in a modified data store, which includes data store 206 (discussed above), where such compensating controls “may mitigate different threats emanating from different components.” *Id.* at 9:62–10:16, 25:57–59, Fig. 3.

Figure 19, reproduced below, shows a modeled attack vector diagram including six compensating controls (each labeled “CC”).

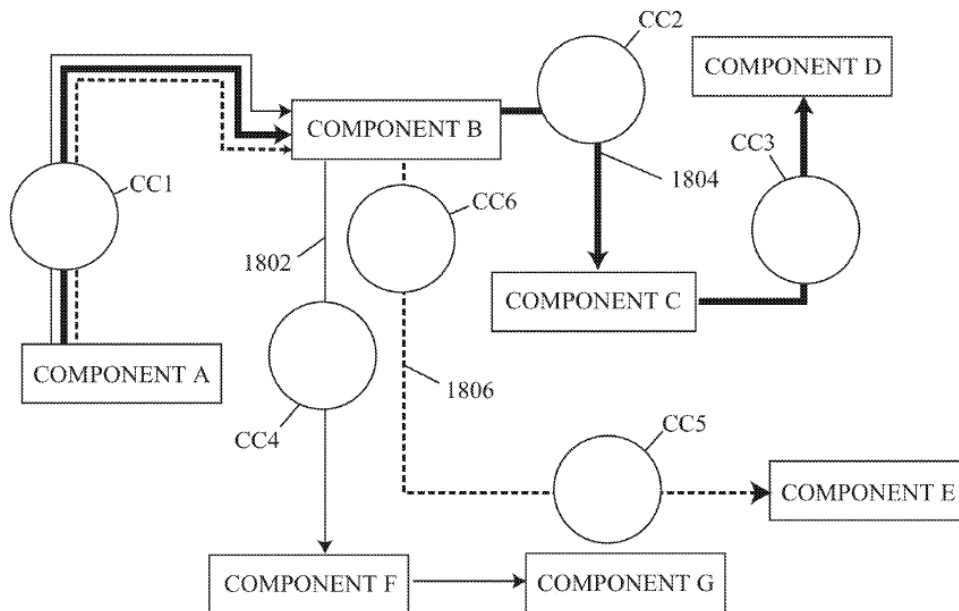


FIG. 19

Figure 19 depicts a block diagram illustrating attack paths of multiple threats of a threat model with compensating controls added thereto.

Id. at 25:55–26:6, Fig. 19. In this illustration, “a threat emanating from component G threatens to compromise component A (or the asset within or associated with component A), [as shown by] the attack vector 1802 passing through component F and component B to reach component A.” *Id.* at 25:43–48. “A threat emanating from component E also threatens to compromise component A, [as shown by] the attack vector 1806 passing through component B to reach component A.” *Id.* at 25:48–50. “A threat emanating from component D also threatens to compromise the asset, [as shown by] the attack vector 1804 passing through component C and component B to reach component A.” *Id.* at 25:50–53.

The '008 patent states that “[t]he term ‘compensating control’ in implementations herein may be an alternative mechanism to a security

requirement or standard,” Ex. 1001, 6:14–20, or “‘compensating control’ may have a more general definition” as any alternative to a security requirement, *id.* at 6:49–67. For example, the ’008 patent states that “a ‘security requirement’ may be defined as a hardware solution and a ‘compensating control’ may be defined as a software solution, such as a change in the code or software added to a system.” *Id.* at 6:58–67.

The ’008 patent provides an interface including a diagram interface, configured to display a relational diagram to visualize the aforementioned threats associated with threat model components and compensating controls using visual representations, such as shapes. *See* Ex. 1001, 16:3–13; 23:36–45.

According to the ’008 patent, in an exemplary threat modeling system, “threat model chaining” may simplify the process of creating threat models:

Each grouping of components, however, could be diagrammed separately as an independent threat model and then saved as a component so that it may be imported into another threat model/diagram. When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or nested within) the threat model of the existing diagram/threat model. In this way the user can modify a threat model by incorporating previously defined threat models. This ability is generally termed “threat model chaining” herein and is a useful mechanism for allowing a user to diagram complex systems/processes without having to repeatedly build common elements among the systems/processes.

Ex. 1001, 20:23–36.

C. Illustrative Claim

The ’008 patent includes twenty claims, all of which are challenged. Claims 1, 4, and 12 are the independent claims. Claims 1 and 4 are

illustrative and are reproduced below with labels, such as “[a],” added to limitations in the same manner as used by the parties.

1. [p] A threat model chaining method, comprising:
 - [a] providing one or more databases, the one or more databases comprising:
 - [b] a plurality of threat model components stored therein;
a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and
 - [c] a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases;
 - [d] providing one or more interfaces, including a diagram interface, configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases;
 - [e] configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and;
 - [f] configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

Ex. 1001, 35:36–63.

4. [p] An attack simulation method, comprising:
- [a] providing one or more databases, the one or more databases comprising:
 - [b] a plurality of threat model components stored therein;
 - a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and
 - [c] a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases;
 - [d] providing one or more interfaces, including a diagram interface, configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases;
 - [-]¹ configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model; and
 - [e] configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model through the one or more interfaces, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

Ex. 1001, 36:16–42.

¹ In mapping its unpatentability contentions against independent claim 4, Petitioner omitted this “configuring” limitation, although this limitation is identical to limitation 1[e] in independent claim 1, which Petitioner does address. *Compare* Pet. 32–35, *and* Ex. 1003 ¶¶ 79–80, *with* Pet. 43–44, *and* Ex. 1003 ¶¶ 89–94.

D. Evidence of Record

Petitioner relies on the following patent evidence.

Name	Patent Document	Exhibit
Jones	US 9,602,529 B2, issued Mar. 21, 2017	1004
Zheng	US 10,503,907 B2, issued Dec. 10, 2019	1005
Keenan	US 11,200,228 B2, issued Dec. 14, 2021	1006
Yu	US 9,948,652 B2, issued Apr. 17, 2018	1007
Reith	US 10,216,938 B2, issued Feb. 26, 2019	1008

Pet. 10–11.

Petitioner also relies upon the Declaration of Robert Hurlbut (Ex. 1003).

Patent Owner relies upon the Declaration of Seth James Nielson, Ph.D. (Ex. 2003).

E. Asserted Challenges to Patentability

We instituted *inter partes* review of claims 1–20 of the '008 patent on the following grounds asserted by Petitioner. Dec. 2–3, 41; Pet. 11.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3	102 ²	Jones
1–20	103	Jones, Zheng, Keenan
1–20	103	Jones, Zheng, Keenan, Yu
1–20	103	Jones, Zheng, Keenan, Yu, Reith

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the earliest possible effective filing date of the '008 patent is after March 16, 2013, the effective date of the relevant amendment, the AIA versions of §§ 102 and 103 apply.

5–8, 13–15	103	Jones, Zheng, Keenan, Yu, Reith ³
------------	-----	--

III. ANALYSIS

A. Applicable Law

Petitioner challenges the patentability of claims 1–20 of the ’008 patent on grounds that the claims are anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 in light of various references, namely Jones, Zheng, Keenan, Yu, and Reith. “In an [*inter partes* review], the petitioner has the burden from the onset to show *with particularity* why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)) (emphasis added). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

1. Anticipation

To serve as an anticipatory reference under 35 U.S.C. § 102, “the reference must disclose each and every element of the claimed

³ Petitioner’s obviousness challenge to the listed claims is based on the listed references (Jones, Zheng, Keenan, Yu, and Reith) “and the knowledge of a POSITA,” where “POSITA” means a person of ordinary skill in the art. Pet. 11. We consider, however, such knowledge as part of any obviousness analysis. *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013). Thus, this asserted ground is not different from the asserted ground challenging claims 1–20 over these same references. We address these grounds separately, however, to track how Petitioner presents its arguments for better clarity.

invention, whether it does so explicitly or inherently.” *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009). “The identical invention must be shown in as complete detail *as is contained in the . . . claim.*” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989) (emphasis added). The elements must be arranged as required by the claim, “but this is not an ‘*ipsissimis verbis*’ test,” i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 832–33 (Fed. Cir. 1990) (citing *Akzo N.V. v. United States Int’l Trade Comm’n*, 808 F.2d 1471, 1479 & n.11 (Fed. Cir. 1986)).

2. Obviousness

A claim is unpatentable under 35 U.S.C. § 103 “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when of record, objective evidence of obviousness or non-obviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Secondary considerations may include the following: “commercial success, long felt but unsolved needs, failure of others, etc.”⁴ *Id.* The totality of the evidence submitted may show that the challenged claims would not have been obvious to one of ordinary skill in the art. *In re*

⁴ Patent Owner does not present objective evidence of non-obviousness.

Piasecki, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The Supreme Court has made clear that we apply “an expansive and flexible approach” to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming a combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. To reach this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.* “To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

B. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art, at the time of the earliest effective filing date of the '008 patent:

would have had a Bachelor's degree in computer engineering, computer science, mathematics, or a similar discipline, with at least three years of relevant industry or research experience, including experience in software development and designing or implementing threat models. Additional work or research experience can substitute for less or different education, and vice-versa.

Pet. 11 (citing Ex. 1003 ¶ 33).

Patent Owner does not present an alternative definition in this proceeding. *See* PO Resp. 3.

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). The level of ordinary skill in the art also is reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Neither party argues that the outcome of this case would differ based on our adoption of any particular definition of the level of ordinary skill in the art. Considering the subject matter of the '008 patent, the background technical field, the prior art, and Petitioner's proposed and unopposed definition of the skilled artisan, we apply the level of skill set forth above, which is consistent with the testimony of Mr. Hurlbut (Ex. 1003 ¶ 33).

C. Claim Construction

We construe claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips*, 415 F.3d at 1312–13; *see CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (There is “a ‘heavy presumption’ that a claim term carries its ordinary and customary meaning.”). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317.

Only those claim terms that are in controversy need to be construed, 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) (stating that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’”

(quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

In our Institution Decision, we stated that briefing during the trial on the proper interpretation of certain claim terms may assist us in resolving issues presented in this case, and invited the parties to address the proper construction of the limitation “*redefine* the first threat model by *including in it* a second threat model associated with the component group,” as recited, for example, in independent claim 1. Dec. 15–16. The parties dispute the meaning of this claim limitation. PO Resp. 16–23; Pet. Reply 1–5; PO Sur-reply 1–2. The parties otherwise do not contend that claim construction is necessary to resolve the controversy in this case. *See* PO Resp. 16–23; Pet. Reply 1–5; PO Sur-reply 1–2. To the extent necessary to resolve the controversy before us, we address claim interpretation in our patentability analysis below.

D. Anticipation of Claims 1 and 3 by Jones

Petitioner contends claims 1 and 3 are unpatentable under 35 U.S.C. § 102 as anticipated by Jones (Ex. 1004). Pet. 13–16, 20–41; Pet. Reply 1–13. Patent Owner opposes Petitioner’s contentions. PO Resp. 16–33; PO Sur-reply 1–8. For the reasons expressed below, and based on the complete record before us, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1 and 3 are unpatentable as anticipated by Jones. We turn first to an overview of Jones.

1. *Overview of Jones (Ex. 1004)*

Jones generally is directed to “modeling and analysis of cybersecurity threats in complex-system (e.g., aviation) platforms.” Ex. 1004, 1:5–7.

Jones summarizes its disclosure as follows:

A system is provided for modeling and analysis of cybersecurity threats may include a data flow diagram (DFD) creator, threat indicator and threat analyzer. The DFD creator may identify elements of an information system, and compose a DFD including nodes and edges representing components and data flows of the information system. The threat indicator may identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system. In metadata associated with the nodes, edges and secondary node, the DFD creator and threat indicator may provide structured information including attributes of the components, data flows and cybersecurity threat. And the threat analyzer may perform an analysis of the cybersecurity threat based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof.

Id. at code (57).

Jones’ Figure 9, reproduced below, illustrates an exemplary graphical user interface (“GUI”) including a level n threat-model DFD 902 produced from the level n DFD 902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.⁵ Ex. 1004, 19:10–14, Fig. 9; *see id.* at 19:14–28.

⁵ “The DFD represent the information system at some level n of the hierarchy, and may at times be referred to as a level n DFD (e.g., level 2 DFD). The DFD creator 106 [*see infra* Figure 1] may also provide structured information including attributes of the components and data

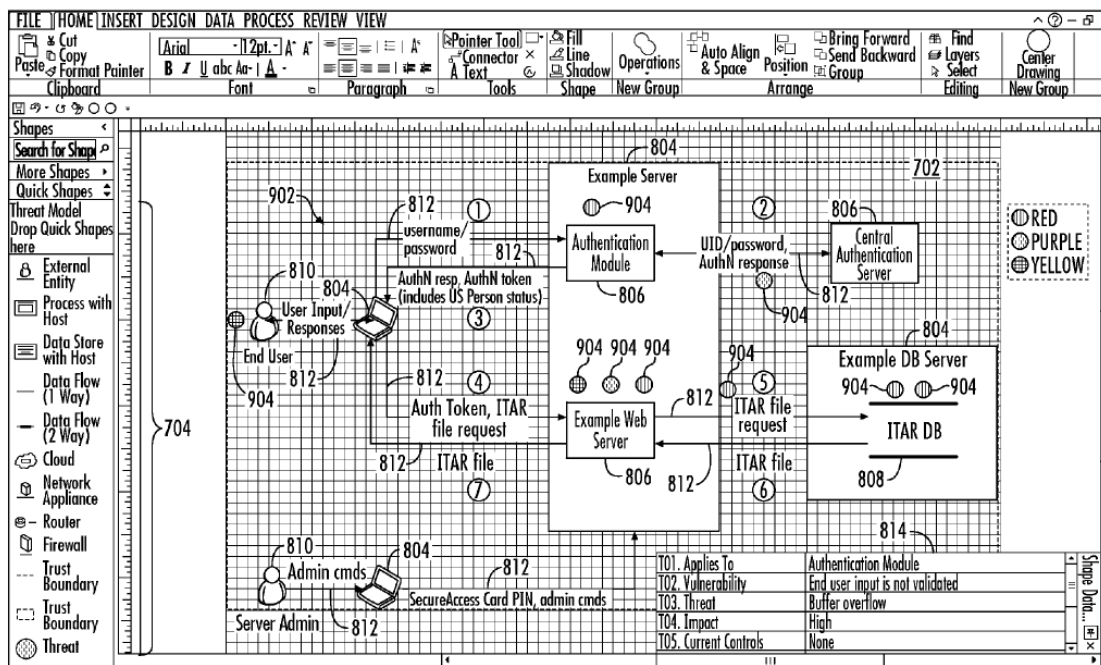


FIG. 9

Figure 9 depicts an exemplary GUI in which a DFD, threat-model DFD and their metadata may be composed or produced.

Id. at 3:25–28, Fig. 9.

According to Jones, “it may be desirable to look deeper into one or more components of the information system, such as to provide a more thorough analysis of those components or their cybersecurity threats.” Ex. 1004, 6:12–15. In this case, Jones discloses a “decomposer 110” “configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows therebetween,” as shown, for example, in Figure 1, reproduced below. *Id.* at 6:15–18, Fig. 1.

flows, and may do so in metadata according to some metadata schema and associated with the nodes and edges of the DFD.” Ex. 1004, 5:51–58.

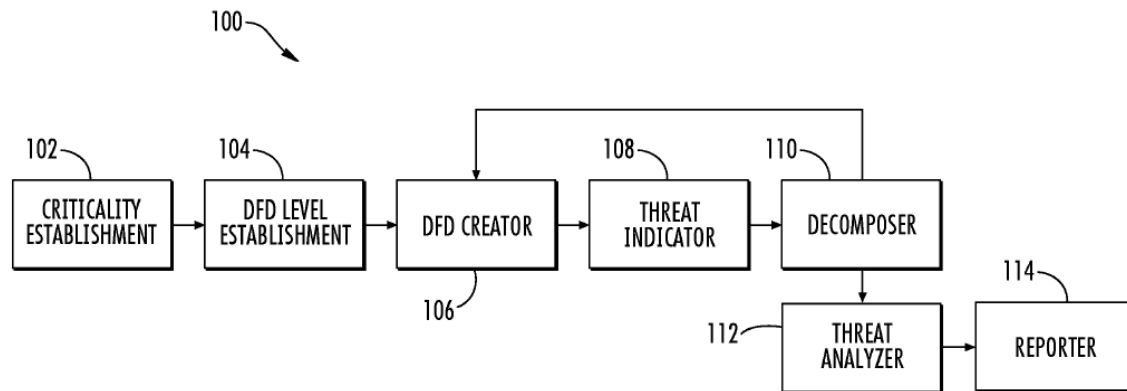


FIG. 1

Figure 1 depicts a system for modeling and analysis of cybersecurity threats in a complex-system platform.

Id. at 3:13–16, Fig. 1.

Referring to Figure 1, above, Jones further explains:

The decomposer may then provide *feedback* of its decomposition to the DFD creator 106, *which may modify the threat-model DFD* for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby *producing a level $n+1$ threat-model DFD*. And again, the threat indicator 108 may be applied to identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and *add appropriate secondary nodes (and appropriate metadata) representing those threats*. Or *instead of modifying* the existing threat-model DFD, in some examples, the DFD creator and threat indicator *may begin again to compose a new DFD and threat-model DFD for this level of the hierarchy*. This decomposition and follow-on modeling of the information system's components and threats may continue until a desired level of the information system is achieved.

Ex. 1004, 6:18–34 (emphases added), Fig. 1; *see id.* at Figs. 2–5.

We further discuss below the disclosure of Jones in connection with the parties' arguments.

2. *Analysis*

a) *Independent Claim 1*

The parties dispute whether Jones discloses to the skilled artisan two limitations, namely 1[e] “configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model”; and 1[f] “configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.”

Pet. 32–40; PO Resp. 23–31; Pet. Reply 5–11; PO Sur-reply 2–6; Ex. 1001, 35:50–63.

(1) *Limitation 1[e]—“configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model”*

Petitioner argues Jones discloses limitation 1[e] by describing, *inter alia*, that its data flow diagram (“DFD”) “includes *shapes* for elements including various *hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812,*” where “[t]he *shapes* may include a graphic and, in some examples, accompanying text that may be taken from

the shape data (e.g., the name of the *information system component* or type of data flowing in the data flow).” Pet. 32–33 (quoting Ex. 1004, 18:58–62, 19:5–9; citing Ex. 1003 ¶¶ 79–80). Petitioner argues Jones also describes “an interface that displays a relational diagram (DFDs), the relational diagram defining a threat model,” and that “[t]he interface uses visual representations of its various components using shapes, as shown in Figs. 7–9, and 10B.” Pet. 33–35 (citing, *inter alia*, Ex. 1004, 3:25–28 (“FIGS. 7-9 depict an example graphical user interface in which a DFD, threat-model DFD and their metadata may be composed or produced.”), 18:44–19:28, Figs. 7–9, 10B); *see* Ex. 1003 ¶ 80.

Patent Owner responds that Jones does not disclose “a relational diagram using ‘visual representations of one or more of the compensating controls,’” and argues that although “Jones Figure 9 does show visual representations of threat model components and threats,” “visual representations *of compensating controls* are not depicted at all.” PO Resp. 29 (citing Ex. 2003 ¶ 106, Ex. 1004, Fig. 9); *see id.* at 30 (“[N]one of [Figures 7–9 and 10B] disclose visual representations of compensating controls on a relational diagram.”); Ex. 2003 ¶¶ 107–108.

Petitioner replies that “[Patent Owner] misses that Jones depicts compensating controls in a rectangular box in the bottom right corner [of Figure 9] under the label ‘Current Controls,’” and submits that “[Patent Owner] does not dispute that Jones discloses compensating controls” and that “there is no dispute that the ‘current controls’ in Jones are compensating controls.” Pet. Reply 10 (citing Pet. 34; Ex. 1016, 64:7–18, 34:6–22; Ex. 1004, 14:1–18). Petitioner argues the noted rectangular box in Figure 9 “is on the relational diagram,” and thus, “[Figure] 9 shows a relational

diagram using ‘visual representations of one or more of the compensating controls.’” *Id.* Petitioner argues Patent Owner’s challenge here is based on an undisclosed, unsupported, narrow construction of “visual representations”:

[Patent Owner’s] argument is based on a not proffered construction of “visual representations,” where the rectangular box is somehow not a “visual representation.” Element 1[e] does not require that the “visual representation” be a particular shape or in a particular place on the relational diagram. Thus, the claims do not exclude a rectangular box on the relational diagram from being a “visual representation.” Jones further discloses that each attribute listed in the rectangular box may be represented on the relational diagram as a secondary node. EX-1004, 19:10-28 (“attributes and even further attributes of the cybersecurity threats may be entered for their shapes. ... ***the window 814 may be recalled for each of the shapes***, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node)).” As such, Jones’ attributes, including the security controls, may be represented as shapes on a diagram. Thus, Jones discloses using “visual representations of one or more of the compensating controls” as required by Element 1[e].

Id. at 10–11. We find Petitioner’s arguments persuasive.

Patent Owner responds that “the claims require that the visual representations of the compensating controls be part of a ‘relational diagram’ in which the relational diagram defines a threat model,” and “Jones’ pop-up window 814 is not part of a relational diagram.” PO Sur-reply 5 (citing Ex. 1001, 35:50–55). Patent Owner argues that, although “workspace 702 in Jones includes aspects of a relational diagram, pop-up window 814 is not part of that diagram,” and regardless, “pop-up window 814 contains textual information about a shape – not a visual representation

of a compensating control.” *Id.* at 5–6 (citing Ex. 1004, 19:18–23). Patent Owner argues “window 814 cannot be considered part of a relational diagram because window 814 does not depict any information about relationships between or among any of the shapes in workspace 702.” *Id.* at 6. We find Patent Owner’s arguments unavailing and not commensurate with the broad scope of claim 1.

We first return to the relevant language of claim 1: “display[ing] a relational diagram of [a system] . . . *using* visual representations of . . . threat model components and visual representations of . . . compensating controls.” Ex. 1001, 35:50–55 (emphasis added). Patent Owner does not dispute that Jones discloses displaying a relational diagram of a system using visual representations of threat model components. *See* PO Resp. 29; PO Sur-reply 5–6. As for whether Jones discloses displaying the relational diagram of a system *using* visual representations of compensating controls, we agree with Petitioner that Jones does so. Jones plainly discloses, for example, that its relational diagram includes “a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD [i.e., data flow diagram]” (Ex. 1004, 19:10–14, Fig. 9; Ex. 1001, code (57)), and that such “shapes” in the diagram in turn use window 814 (e.g., a “pop-up” window as observed by Patent Owner (PO Sur-reply 5)) to visually present and represent compensating controls, such as “Current Controls,” relating to threats represented by such shapes in the relational diagram (Ex. 1004, Fig. 9, 19:10–28). Patent Owner does not dispute that Jones’s “Current Controls” are within the scope of the claimed “compensating controls” (*see* Ex. 1016, 64:7–18, 34:6–22; Ex. 1004, 14:1–18; *see generally* PO Resp.; PO Sur-reply), and to be clear, we find

that the textual display or description of such controls in pop-up window 814 in Jones's Figure 9 is both visual and representative of the control itself. As argued by Petitioner (Pet. Reply 10–11), claim 1 as a whole, and limitation 1[e] in particular, does not require that the “visual representations” of compensating controls be particular shapes, be in particular places on the relational diagram, or be revealed or represented all at once in the relational diagram, and Patent Owner does not direct us to any such requirement in claim 1.

Based on the foregoing and the complete record before us, we find Petitioner sufficiently establishes that Jones discloses limitation 1[e].

- (2) *Limitation 1[f]*—“*configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components*”
 - (a) *Claim Construction*: “*redefine the first threat model by including in it a second threat model associated with the component group*”

Claim 1 recites, in relevant part, “*add[ing] a component group [i.e., a predefined interrelated group of two or more of the threat model components] to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group.*” Ex. 1001, 35:56–63 (emphases added).

Patent Owner proffers that the subject limitation should be construed to mean “change the first threat model by adding a predefined interrelated

component group and its associated second threat model to the first threat model where the added component group was not a part of the first threat model before being added.” PO Resp. 16–17; *see id.* at 17–19. Patent Owner argues, in various forms, that the skilled artisan “would understand the word ‘redefine’ to require the threat model to change, not simply to be expanded with more detail.” *Id.* at 17. Patent Owner similarly argues that “[t]he claim language also requires that the ‘component group’ is ‘add[ed]’ to the first threat model,” and thus (allegedly) “the component group could not have been part of the first threat model prior to being added,” and “the component group must have had its own ‘second’ threat model before it was added to the first threat model.” *Id.* Patent Owner also argues that its position here is supported by the Specification, which discusses, as an example, creating a “Windows 7” component group with an associated independent (second) threat model that may be saved in a “toolbox” as a “component,” which in turn may be imported into another threat model/diagram such that a user may diagram complex systems or processes without having to repeatedly build common elements among the systems or processes. *Id.* at 18–19; Ex. 1001, 19:50–20:58, Fig. 10.

Petitioner proffers that the subject limitation should be construed to mean “modify or change the first threat model by adding to it a second threat model associated with the component group,” where “[t]he plain and ordinary meaning of ‘redefine’ is to ‘modify’ or ‘change’ and the plain and ordinary meaning of ‘including’ is ‘adding.’” Pet. Reply 1–2, 4. Petitioner argues that “the portion of [Patent Owner’s] construction reciting ‘where the added component group was not a part of the first threat model before being added’ adds extraneous words that improperly change the meaning of the

claim terms beyond their plain and ordinary meaning,” and that “[t]he claims do not exclude a situation where the component group added to the first threat model already exists in that first threat model.” *Id.* at 3.

Patent Owner responds “Petitioner’s criticisms ignore the language of the claims themselves.” PO Sur-reply 1. Patent Owner argues that its proposed construction “is exactly consistent with the claims,” and “[a]dding a duplicative component group to the first threat model ‘thereby redefine[s]’ the first threat model because the duplicative component group itself was not previously part of the threat model.” *Id.* at 2.

We turn first to the claim language itself. We are mindful of Judge Rich’s guidance from over thirty years ago: in all aspects of claim construction, “the name of the game is the claim.” *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) (quoting Giles Sutherland Rich, *Extent of Protection and Interpretation of Claims—American Perspectives*, 21 Int’l Rev. Indus. Prop. & Copyright L. 497, 499 (1990)).

Claim 1 recites, in relevant part, “add[ing] a component group to the first threat *model* and thereby *redefine* the first threat *model* by including in it a second threat *model associated with the component group*, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.” Ex. 1001, 35:56–63 (emphases added). We agree with the parties that the claim language itself supports “redefine” as meaning to “change.” See PO Resp. 16–17; Pet. Reply 1–2, 4. That is, claim 1 explicitly recites that the first threat model is redefined, or in other words, “changed,” by “adding” to it other threat model components and their associated “second” threat model. But contrary to Patent Owner’s arguments (PO Resp. 16–19), we find no support in claim 1 to further

narrow the interpretation of the subject limitation to exclude all scenarios except “where the added component group was not a part of the first threat model before being added.” *See* Ex. 1001, 35:36–63 (claim 1). We similarly find no support in the Specification or limited prosecution history (*see* Pet. 9), and Patent Owner does not direct us to any, showing that the inventor acted as its own lexicographer or disavowed any claim scope to allot this narrowed interpretation to the subject limitation.

Accordingly, based on the complete record before us, we determine that “redefine the first threat model by including in it a second threat model associated with the component group” means “change the first threat model by adding to it a second threat model associated with the component group.”

We note that Patent Owner’s claim construction arguments highlight a conflict between, on the one hand, what claim 1 actually recites, and on the other hand, what Patent Owner proffers claim 1 to recite in view of prior art asserted in this case. More specifically, claim 1 defines the invention as configuring a diagram interface to *display* a threat *model* of an underlying system (for example) and, through user inputs, change or redefine the *displayed* threat *model* by adding to *that model* certain threat model components and their associated threat model. Notably missing from claim 1 is any limitation directed to changing (e.g., adding) elements or components to *the underlying system* for which a threat model is being displayed. Thus, contrary to Patent Owner’s claim construction arguments (above) and its validity arguments (below), claim 1 encompasses displaying a changed (or redefined) threat model even where the underlying system being modeled itself does not change in composition.

(b) *Parties' Arguments*

(i) *The Petition*

Petitioner argues Jones discloses limitation 1 [f] by describing, *inter alia*, that its system may “modify the threat-model DFD [data flow diagram] for the decomposed components to include their nested components . . . thereby producing a level n+1 threat model DFD.” Pet. 35–36 (quoting Ex. 1004, 6:12–34; citing Ex. 1003 ¶¶ 81–84).

In particular, Petitioner argues (and Mr. Hurlbut testifies) Jones discloses limitation 1 [f], including “a second threat model,” by describing, *inter alia*:

[I]t may be desirable to look deeper into one or more components of the information system, such as *to provide a more thorough analysis of those components or their cybersecurity threats*. In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested *components* [plural] and data flows there between. The decomposer may then provide *feedback* of its decomposition to the DFD creator 106, which may *modify the threat-model DFD for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD*. [Ex. 1004, 6:12–34.]

Pet. 35–36 (emphases added) (citing Ex. 1004, 6:12–34; Ex. 1003 ¶¶ 81–84).

As we understand Petitioner’s argument (and its expert’s testimony), Petitioner argues Jones “modifies,” i.e., “redefines,” a “first threat model” (level n) by “including” in it cybersecurity threats (e.g., via metadata) associated with nested components (i.e., “a second threat model”), to produce the “modified” (“redefined”) “first threat model” (level n+1). *See id.*; *In re Bond*, 910 F.2d at 832–33 (anticipation “is not an ‘*ipsissimis verbis*’ test”). In other words, Petitioner argues that, although Jones may not

use the identical terminology as the '008 patent, Jones nevertheless explicitly discloses limitation 1[f] *to the skilled artisan*, by describing modifying a first “threat” model from a level “n” model to a level “n+1” model by including therein threats associated with a particular layer of components (nested components), i.e., a second “threat” model.

Petitioner argues “Jones allows for user input through a graphical user interface GUI, as shown in Figure 9 [reproduced above].” Pet. 39.

Petitioner argues Figure 9 “illustrates the GUI including a level n threat-model DFD 902 produced from the level n DFD 902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.” Pet. 36 (quoting Ex. 1004, 19:10–28). According to Petitioner’s expert, Mr. Hurlbut, the skilled artisan “would understand that the interrelated group of two or more threat model components in Jones may be predefined because Jones discloses identifying elements of the information system, which would be dependent on a predefined system when Jones’ system is applied.” Ex. 1003 ¶ 82 (cited at Pet. 36); *see* Pet. 36–39 (citing, *inter alia*, Figs. 1–3, 5, 9). Petitioner argues, “[i]n Jones, the ‘cybersecurity threats (or rather their shapes) are placed in the workspace 702’ within the GUI.” Pet. 39–40 (citing Ex. 1004, 18:44–57 (“[T]he GUI 700 may include a workspace 702 for composition of a level n DFD from shapes representing its nodes and edges.”), 18:30–43, Figs. 7–9).

Based on the foregoing, according to Petitioner’s expert, Mr. Hurlbut, the skilled artisan “would understand that Jones’ nesting disclosure meets this limitation [1[f]].” Ex. 1003 ¶ 84 (cited at Pet. 40).

(ii) *Patent Owner's Response*

Patent Owner responds, in sum, that Jones does not disclose *adding* a component group to a first threat model, as recited in limitation 1[f]. PO Resp. 23; *see id.* at 23–29.

[T]he “component group” that is added to the first threat model must comprise “a predefined interrelated group of two or more of the threat model components.” Thus, the “component group” must be defined before it is added to the first threat model. The claim language also requires that the “component group” is “add[ed]” to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model “thereby redefine[s]” the first threat model “by including in it a second threat model associated with the component group.” Thus, the component group must have had its own “second” threat model before it was added to the first threat model. The addition of the component group also requires that the threat model of the component group is added to the first threat model. PO Resp. 24 (citing Ex. 2003 ¶¶ 96–97). Patent Owner argues, in Jones, “[t]he ‘nested’ subcomponents were already present *in the information system and the threat model* created by Jones’ system for analyzing the information system.” *Id.* at 25 (emphases added). We note that the deposition testimony of Petitioner’s expert cited by Patent Owner as support for this statement only supports that the nested subcomponents were already present in the underlying information system, not that threat model components for such subcomponents were already present in all levels of threat models for such system. *See* Ex. 2002, 71:9–72:3 (cited at PO Resp. 25–26) (“Q. And all of that is part of that *information system* that’s being analyzed? A. Yes. Correct.” (emphasis added)). Patent Owner similarly argues, but only in the context of the underlying information

system this time, that “[a]dding’ the ‘component group’ does not occur in Jones because all components and subcomponents *of the information system* being examined *are already present in the information system*.” *Id.* at 26 (citing, *inter alia*, Ex. 2002, 71:9–72:3) (emphases added).

Patent Owner faults Petitioner’s reliance on Jones to show modeling of a “predefined system,” and more particularly, a “component group compris[ing] a *predefined* interrelated group of two or more of the threat model components.” PO Resp. 27–29; Ex. 1001, 35:60–63 (emphasis added). Patent Owner argues that “[j]ust because the information system in Jones is ‘predefined’ says nothing about whether there is a ‘component group’ including a ‘predefined interrelated group’ of threat model components,” and “[t]here is no teaching in Jones that a ‘component group’ of threat model components is ‘predefined.’” PO Resp. 27; *see id.* at 28 (“Jones discloses decomposing components based on their existing hierarchy; however, how it chooses to decompose (which elements get included in the $n+1$ decomposition) is up to the decomposer, indicating that there is no ‘predefined’ component group.”). But again, as we understand Petitioner’s argument (and its expert’s testimony), Petitioner argues that, to the skilled artisan, Jones’ Figure 9 and associated description shows a DFD for an information system including multiple interconnected (interrelated) components, and based on the existence (or creation) of that system, such components and components nested therein depend on a predefined system at least when Jones’ system is applied. *See* Pet. 36 (citing Ex. 1003 ¶ 82 (The skilled artisan “would understand that the interrelated group of two or more threat model components in Jones may be predefined because Jones discloses identifying elements of the information system, which would be

dependent on a predefined system when Jones' system is applied.”)); *id.* at 37–40.

Patent Owner argues that “the component group must have its own ‘second threat model’ before it is added to the first threat model because the claim requires that the addition of the component group is what causes the first threat model to be ‘redefined.’” PO Resp. 28–29.

(iii) *Petitioner's Reply*

In reply, Petitioner reiterates:

Jones “modifies” (*i.e.*, “redefines”) a “first threat model” (level *n*) by adding to it (*i.e.*, “including” in it) cybersecurity threats (*e.g.*, via metadata) associated with nested components (*i.e.*, “a second threat model”), to produce the “modified” (*i.e.*, “redefined”) “first threat model” (level *n*+1).

Pet. Reply 5.

Petitioner notes that “[Patent Owner] essentially argues that, since components are predefined in the information system, the components cannot be ‘added,’” and argues that Patent Owner’s argument here “conflates Jones’ *information system* and *threat model DFD*—*the components are predefined in the information system* and then ‘added’ to the threat model DFD.” Pet. Reply 6 (citing Ex. 1004, 5:45–6:34) (emphases added).

In other words, the nested components associated with the decomposed component are *predefined in the information system, but not yet modeled in the threat model DFD*. [Patent Owner’s] expert agrees. EX-1016, 53:7-11 (Jones discloses “the creation of a new DFD”), 59:2-9 (“Q So the group of decomposed components exist in the information system but they’re not yet modeled in the threat modeled DFD? A Correct.”). Thus, the nested components are predefined in the information system and “added” to the first threat model DFD,

thereby redefining the first threat model by including in it a second threat model, and [Patent Owner's] argument fails.

Pet. Reply 6–7 (emphasis added); *see id.* at 7–8 (“[A]s with the components of the threat model DFD, Jones’ threat indicator may ‘identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and add appropriate secondary nodes (and appropriate metadata) representing those threats.’” (quoting Ex. 1004, 6:23–28)). Petitioner also submits that Patent Owner’s expert, Dr. Nielson, testified that “the nested components for a decomposed component ‘already exist’ in the information system,” and argues that this contradicts Patent Owner’s argument that such pre-existing, nested components are not “predefined.” *See id.* at 8 n.1.

(iv) *Patent Owner’s Sur-Reply*

Patent Owner responds, “[e]ssentially, Petitioner is now trying to separate the threat model components from Jones’ threat model.” PO Sur-reply 3. Patent Owner argues that “[t]he $n+1$ level subcomponents are already part of the n -level components identified by the DFD creator 106,” and so “when the decomposer 110 decomposes the components into their nested subcomponents, the decomposer is not adding any component group to the threat model,” because “[t]he subcomponents are already present, although not shown visibly.” *Id.* at 4 (citing Ex. 1004, 5:10–19); *see id.* at 2–5. We find Patent Owner’s arguments unavailing, as discussed below.

(v) *Analysis*

We have considered Petitioner’s arguments and cited evidence concerning whether Jones discloses limitation 1[f] to the skilled artisan, and find them persuasive on the complete record before us.

Claim 1 defines the invention, in part, as configuring a diagram interface to *display* a threat *model* of an underlying system (for example) and, through user inputs, change or redefine the displayed threat *model* by adding *to that model* certain threat model components and their associated threat model. *See* Ex. 1001, 35:56–63; *supra* § III.D.2.a.2.a. Notably missing from claim 1 is any limitation that requires changing (e.g., adding) elements or components to *the underlying system* for which a threat model is being displayed. Claim 1 encompasses displaying a changed (or redefined) threat model even where the underlying system being modeled itself does not change in composition. *See supra* § III.D.2.a.2.a.

That said, we agree with Patent Owner that Jones does not explicitly disclose adding elements or components *to the underlying information system* for which a threat model is being displayed to thereby “redefine” that threat model, but this feature is not required by claim 1. *See, e.g.*, PO Resp. 25 (Patent Owner arguing that “[t]he ‘nested’ subcomponents were already present in the information system.”). However, we disagree with Patent Owner that Jones does not disclose adding *threat model components* and a threat model associated therewith *to a first threat model* to thereby “redefine” that threat model, as recited in claim 1. *See* PO Resp. 23–29; PO Sur-reply 2–5; Pet. Reply 6 (Petitioner arguing that Patent Owner “conflates Jones’ information system and threat model DFD—the components are predefined in the information system and then ‘added’ to the threat model DFD.”) (citing Ex. 1004, 5:45–6:34).

We find Jones discloses creating a data flow diagram (DFD) of an underlying information system’s elements at some level of specificity, such

as a level “n” DFD.⁶ Jones discloses using threat indicator 108 to identify threats to such elements of the underlying information system, and adding such threat data to the level n DFD to create a level n threat-model DFD. *See, e.g.,* Ex. 1004, 5:64–6:11. Jones discloses that “it may be desirable to look deeper into one or more components of the information system, such as to provide *a more thorough analysis of those components or their cybersecurity threats.*” *Id.* at 6:12–15 (emphasis added). Jones discloses decomposing components (elements) of the information system as modeled in the level n threat-model DFD into their “nested components and data flows therebetween” and using threat indicator 108 to identify threats to such nested components.⁷ *Id.* at 6:15–18, 6:23–28; *see* Pet. Reply 5. Jones discloses changing or redefining the level n threat-model DFD (first threat model) by including in it the additional threat data associated with the nested

⁶ *See, e.g.,* Ex. 1004, 5:45–53 (“The DFD creator 106 may be configured to identify elements of the information system, and compose a DFD for the information system from those elements and *in accordance with the threat-model level identified by the DFD level establishment system 104.* . . . The DFD represent the information system *at some level n* of the hierarchy, and may at times be referred to as a level n DFD (e.g., level 2 DFD).” (emphases added)), 5:20–24 (“The DFD level establishment system 104 may be configured to assess various criteria of the information system to identify an appropriate level of threat model—threat-model data flow diagram (DFD)—to produce for the information system.”); Pet. Reply 6–7 (citing, *inter alia*, Ex. 1004, 5:45–6:34).

⁷ Contrary to Patent Owner’s argument (PO Resp. 28–29), we agree with Petitioner that Jones discloses that the nested components added to a level n threat-model DFD may have threats associated with them as well as “appropriate metadata” representing those threats (i.e., Jones discloses adding a second threat model associated with the nested components to a first threat model). *See* Ex. 1004, 6:18–28.

components (second threat model) to produce a level n+1 threat-model DFD (redefined first threat model).⁸

We find Jones itself effectively confirms that it discloses such a redefined threat model as recited in claim 1 by explaining that “*instead of modifying the existing [level n] threat-model DFD, . . . the DFD creator and threat indicator may begin again to compose a new DFD and [level n+1] threat-model DFD for this level [n+1] of the hierarchy.*” Ex. 1004, 6:28–31 (emphases added). Contrary to Patent Owner’s arguments (*see* PO Resp. 23–29; PO Sur-reply 2–5), if Jones’s original level n threat model DFD already included all elements of the underlying system and all of the threats associated with all of those elements, then there would have been no need for Jones’s system to “begin again” and “compose a new DFD and threat-model DFD” to capture the nested components such as revealed in the level n+1 threat-model DFD.

We find Jones discloses that a “component group” (e.g., Jones’s nested components) added to the first threat model (level n threat-model DFD) comprises a *predefined interrelated group* of two or more threat model components, for the reasons proffered by Petitioner. *See, e.g.,* Pet. Reply 6–7 (Petitioner arguing that “the nested components associated with the decomposed component are predefined in the information system, but not yet modeled in the threat model DFD,” and citing agreement by Patent

⁸ *See, e.g.,* Ex. 1004, 6:18–23 (“The decomposer may then provide feedback of its decomposition to the DFD creator 106, which may *modify the threat-model DFD* for the decomposed components *to include* their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD.”), 6:23–28; Pet. Reply 5; Pet. 35–36; Ex. 1003 ¶¶ 81–84.

Owner’s expert. (citing Ex. 1016, 59:2–9 (“Q So the group of decomposed components exist in the information system but they’re not yet modeled in the threat modeled DFD? A Correct.”)); Ex. 1003 ¶ 82 (cited at Pet. 36); Pet. 36–39 (citing, *inter alia*, Figs. 1–3, 5, 9). As discussed above, we agree with Patent Owner that Jones does not explicitly disclose adding elements or components to the underlying information system (*see* PO Resp. 25 (“The ‘nested’ subcomponents were already present in the information system.”)), and thus Jones’s information system as a whole is “predefined.” For the same reasons, so too are the nested components of a given element of the predefined information system (i.e., those nested components for a given element do not change). We find the fact that a given element of Jones’s information system breaks down into a set of nested components discloses to the skilled artisan that such “nested components” are both “predefined” and “interrelated.” *See* Ex. 1003 ¶¶ 81–84.⁹

⁹ In arguing that Jones does not disclose a “predefined interrelated group” of threat model components, Patent Owner, in a footnote, alleges that the testimony of Petitioner’s expert, Mr. Hurlbut, is “tainted by bias” arising from his “personal and professional connections” to Petitioner. PO Resp. 27 n.4; *see* PO Sur-reply 21–22. Patent Owner cites no authority to show that such connections necessarily render expert testimony biased, and identifies no actual testimony of Mr. Hurlbut that it alleges to be driven only by bias. On the other hand, Petitioner submits that Mr. Hurlbut also has personal and professional connections to *Patent Owner*—it’s a small world. *See* Pet. Reply 24 (“Mr. Hurlbut personally knows Mr. Agarwal, [Patent Owner’s] CEO and inventor of the ’008 patent.”). In this case, we assess the credibility of both parties’ experts based on the plausibility of and support for their testimony, and weigh such testimony accordingly. *See* Consolidated Trial Practice Guide (“CTPG”) at 32 (“[T]he credibility of experts often turns less on demeanor and more on the plausibility of their theories.”), 35 (“The Board has broad discretion to assign weight to be accorded expert testimony.”); *see also* 84 Fed. Reg. 64,280 (Nov. 21, 2019).

Based on the foregoing and the complete record before us, we find Petitioner sufficiently establishes that Jones discloses limitation 1[f].

(3) *Undisputed Limitations*

Petitioner contends the remaining limitations of independent claim 1, namely, limitations 1[p], 1[a], 1[b], 1[c], and 1[d], also are disclosed by Jones. Pet. 20–32. The Petition provides a detailed assessment of these remaining limitations, with references to disclosures in Jones and the declaration testimony of Mr. Hurlbut. *See id.* (citing, *inter alia*, Ex. 1003 ¶¶ 64–78). Patent Owner does not contend that the remaining limitations in claim 1 are absent in Jones, except as implicated by the disputed limitations, and therefore, has waived such arguments.¹⁰ For the reasons set forth in the Petition (Pet. 20–32), and based on the evidence cited therein (*see, e.g.*, Ex. 1003 ¶¶ 64–78), we find Petitioner sufficiently establishes that Jones discloses limitations 1[p], 1[a], 1[b], 1[c], and 1[d].

(4) *Conclusion for Independent Claim 1*

For the foregoing reasons, and based on the complete record before us, we determine that Petitioner has demonstrated by a preponderance of the evidence that independent claim 1 is unpatentable as anticipated by Jones.

¹⁰ *See* 37 C.F.R. § 42.23(a) (“Any material fact not specifically denied may be considered admitted.”); *In re Nuvasive, Inc.*, 842 F.3d 1376, 1379–82 (Fed. Cir. 2016) (holding that patent owner waived arguments on an issue that were not raised in its response after institution); *see also Papst Licensing GmbH & Co. KG v. Samsung Elecs. Am., Inc.*, 924 F.3d 1243, 1250 (Fed. Cir. 2019) (holding patent owner forfeited argument for patentability not presented to the Board); *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1048 (Fed. Cir. 2019) (explaining that arguments not presented to the Board are waived).

b) Dependent Claim 3

Claim 3 depends from independent claim 1 and recites in full:

The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more *additional* threat model components in the one or more databases, store one or more *additional* threats in the one or more databases, associate each *additional* threat with at least one of the *additional* threat model components through the one or more databases, store one or more *additional* compensating controls in the one or more databases, and associate each *additional* compensating control with at least one of the *additional* threats through the one or more databases.

Ex. 1001, 36:4–15 (emphases added).

Petitioner contends Jones discloses these features of claim 3 by describing, *inter alia*, the steps in the threat model chaining method of limitations 1[p]–1[f], and that each of these steps could be performed an additional time. Pet. 40 (citing, *inter alia*, Ex. 1003 ¶ 85). Petitioner argues that “Jones refers consistently to ‘one or more’ of each of its functions and creating one or more DFDs including the claimed elements.” Pet. 40–41 (citing, *inter alia*, Ex. 1004, 4:13–21 (“[T]he system may be configured to perform one or more of its functions or operations under direct operator control.”), Figs. 7–9 (showing multiple threats, threat model components, and compensating controls), Figs. 10A–10B; Ex. 1003 ¶ 85).

Patent Owner responds that “[n]one of the portions of Jones cited by Mr. Hurlbut or the Petition disclose the storing of a second set of threats, threat model components, and compensating controls and making associations among those threats, threat model components, and

compensating controls, as required by claim 3. PO Resp. 32; *see id.* at 31–33.

Petitioner replies that “[e]ach of these steps is performed in claim 1, and claim 3 merely requires these steps be performed an ‘additional’ time.” Pet. Reply 11–12 (referring to Petitioner’s analysis of limitations 1[b] and 1[c] (Pet. 23–30)); *see id.* at 11–13. Petitioner argues “it is simply not credible to suggest that Jones cannot perform the steps of claim 1 an ‘additional’ time,” and that “Jones system is not limited to a specific number of threats, threat model components, or compensating controls, or associations between them.” *Id.* at 12. Petitioner argues that “[Patent Owner’s] argument appears to be that Jones is somehow limited to only those ‘multiple threats and components’ [revealed in Figures 9 and 10A–10B, for example,] without the ability to [add] more, which is simply not credible.” *Id.* We find Petitioner’s arguments persuasive.

Patent Owner responds by repeating its conclusory argument that Jones does not disclose storing “additional” threats, threat model components, compensating controls, and their respective associations in databases. *See* PO Sur-reply 6 (Patent Owner arguing, “Petitioner is wrong.”), 7 (“Jones does not teach or suggest adding ‘additional’ threat model components, ‘additional’ threats, or ‘additional’ compensating controls to the one or more databases recited in claim 1.”). Patent Owner argues that “[c]laim 1 already required the storage of multiple threat model components, multiple threats, and multiple compensating controls,” and, allegedly, “Petitioner’s flawed reading of claim 3 renders the additional method steps of claim 3 nullities.” *Id.* at 7–8. Notably missing from Patent Owner’s arguments here is any hint of what Patent Owner believes claim 3

substantively adds to claim 1, other than, perhaps, adding more of the same type of data to the database(s).

Claim 1 is an open-ended (“comprising”) claim that requires, in relevant part:

[1[a]] providing one or more databases, the one or more databases comprising:

[1[b]] a *plurality* of threat model components *stored* therein;
a *plurality* of threats *stored* therein, each threat *associated* with at least one of the threat model components through the one or more databases; and

[1[c]] a *plurality* of compensating controls *stored* therein, each compensating control *associated* with at least one of the threats through the one or more databases.

Ex. 1001, 35:37–45 (emphases added). As discussed above in Section III.D.2.a.3, Patent Owner does not dispute that Jones discloses these limitations, which require storing (or “stored”) threats, threat model components, compensating controls, and their respective associations in databases. Jones discloses implementing its system for threat modeling and analysis across a multitude of threats and complex-system platforms, and operating the system more than once. *See, e.g.*, Ex. 1004, 1:59–62, 6:28–31 (“[I]nstead of modifying the existing threat-model DFD, in some examples, the DFD creator and threat indicator may *begin again* to compose a new DFD and threat-model DFD for this level of the hierarchy.” (emphasis added)). Taking stored “threats” as an example, we find the threat-model DFD in Jones’s Figure 9 shows multiple threats 904, where two such threats implicate limitation 1[b]’s stored “plurality of threats” and the other threats implicate claim 3’s stored “additional threats.” *See* Pet. 41; Pet. Reply 12; Ex. 1004, 19:10–28, Fig. 9. As argued by Petitioner, we find the skilled

artisan would have understood that Jones performs the undisputedly disclosed limitations 1[a], 1[b], and 1[c], does so multiple times, and in doing so adds or stores “additional” threats, threat model components, compensating controls, and their respective associations in databases. *See, e.g.*, Ex. 1004, 7:57–8:22, 12:7–13:7 (cited in part at Pet. 24) (both discussing collecting and storing metadata information). We find Patent Owner’s allegations to the contrary simply not credible.

Based on the foregoing and the complete record before us, we find Petitioner sufficiently establishes that Jones discloses the limitations of dependent claim 3.

3. *Summary*

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 1 and 3 are unpatentable as anticipated by Jones.

E. Obviousness of Claims 1–20 over the Combination of Jones, Zheng, and Keenan

Petitioner contends claims 1–20 would have been unpatentable under 35 U.S.C. § 103 as obvious over the combination of Jones (Ex. 1004), Zheng (Ex. 1005), and Keenan (Ex. 1006). Pet. 13–17, 41–57; Pet. Reply 13–19. Although on its face Petitioner includes claims 1 and 3 in this challenge, Petitioner then states, “Claims 1 and 3 are anticipated by Jones” (Pet. 41), and does not explicitly otherwise address these claims under this challenge. *See Cohesive Techs., Inc. v. Waters Corp.*, 543 F.3d 1351, 1364 (Fed. Cir. 2008) (“[I]t is commonly understood that prior art references that anticipate a claim will usually render that claim obvious.”). Patent Owner opposes Petitioner’s contentions. PO Resp. 33–50; PO Sur-reply 8–16. For the

reasons expressed below, and based on the complete record before us, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–20 would have been unpatentable as obvious over the combination of Jones, Zheng, and Keenan. We turn first to an overview of Zheng and Keenan (Jones is discussed above in Section III.D.1).

1. Overview of Zheng (Ex. 1005)

Zheng generally is directed to systems, methods and apparatuses “for dynamically visualizing and analyzing security risks in one or more suites of applications.” Ex. 1005, 1:14–17.

Zheng discloses a system comprising “a visualization module for rendering, on a computer display, a map with components representative of the suite of software applications and relationships among the software applications,” where “[t]he components are displayed in a base layer of the map.” Ex. 1005, 1:48–53. Zheng explains that, “by utilizing a visualization approach like cartography, application architecture can be represented in a compressible view that enhances security and risk analysis,” and that “mapping techniques and concepts can be used in the context of data visualization to create a graphical representation of application connectivity and security.” *Id.* at 3:28–34.

Zheng’s Figure 8, reproduced below, shows an exemplary visualization flow of a multi-layered structure of a system architecture. Ex. 1005, 11:56–57, Fig. 8.

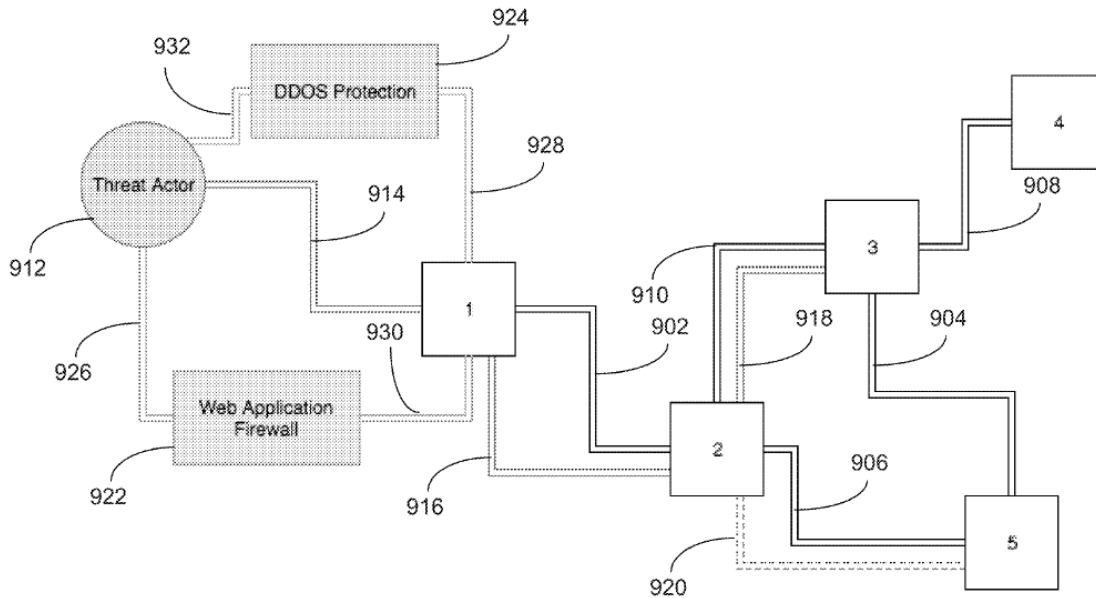


FIG. 8

Figure 8 depicts an exemplary visualization flow.

Id. at 3:19–20, Fig. 8; *see* Figs. 1, 2.

This visualization flow can be implemented by the visualization module 116 of the system 100 of FIG. 1. The numbered boxes 1–5 along with their connections 902, 904, 906, 908, 910 represent various components of the base layer 202 of the multi-layered structure 200 of an application ecosystem. For example, the numbered boxes represent applications within the ecosystem and the connections 902, 904, 906, 908, 910 represent relationships/data flows among the applications. The threat actor component 912 and the connections 914, 916, 918 and 920 can be a part of the threat modeling layer 204 of the multi-layered structure 200, *where the connections 914, 916, 918 and 920 illustrate the impact of the threat actor 912 on various components of the base layer 202.* The DOS Protection component 922 and the firewall component 924, along with the connections 926, 928, 930, 932 can be a part of the security controls layer 206 of the multi-layered structure 200. In some embodiments, *if a user activates a toggle switch such that both the threat modeling layer 204 and the security controls layer 206*

are visualized, the threat segment 920 between components 2 and 5 of the base layer 202 can be displayed as dotted (or flashing or any other warning fashion) to illustrate that this segment of the threat actor route is mitigated or eliminated by the security controls in the security controls layer 206.

Ex. 1005, 11:57–12:14 (emphases added).

Zheng also discloses that the threat modeling layer “visualizes *each security threat* as a threat actor, a threat target and a displayable vector connecting the threat actor to the threat target.” Ex. 1005, 2:36–39 (emphasis added). According to Zheng, the displayable vector can “visualize an attack methodology by the threat actor on the threat target.” *Id.* at 2:39–42.

We further discuss below the disclosure of Zheng in connection with the parties’ arguments.

2. Overview of Keenan (Ex. 1006)

Keenan generally is directed to “an Integrated Object Environment (IOE) running in a graph database environment.” Ex. 1006, 1:22–24. “Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in [a] query-driven, graph database.” *Id.* at code (57). The IOE system “stores, reveals and links characteristics (Structural Metadata) of each object in the topology either within the IOE or in a linked repository, such that accountability, benefits and *consequences of using those assets* can easily and repeatedly be measured in the cost and profitability of the outcomes those assets enable.” *Id.* at 1:47–52 (emphasis added). A user may interact with the IOE through a Graphical User Interface (GUI), including “a View mode, where the user can view any section of the topology and Characteristics by Object” and

“a Modify mode, where the user can add, change and delete Objects or Characteristics.” *Id.* at 11:42–51. According to Keenan, “[t]he intelligence embedded in the stored topology can be viewed in a variety of ways through the GUI, both in terms of the object-to-object relationships and the associated characteristics of objects.” *Id.* at 12:64–67. This includes processing and viewing objects by “technical threat vectors,” where “color fills the object shapes based on the value of the technical risk ranking characteristic of that object.” *Id.* at 16:21–23.

The major components of the IOE appear in Figure 1, reproduced below.

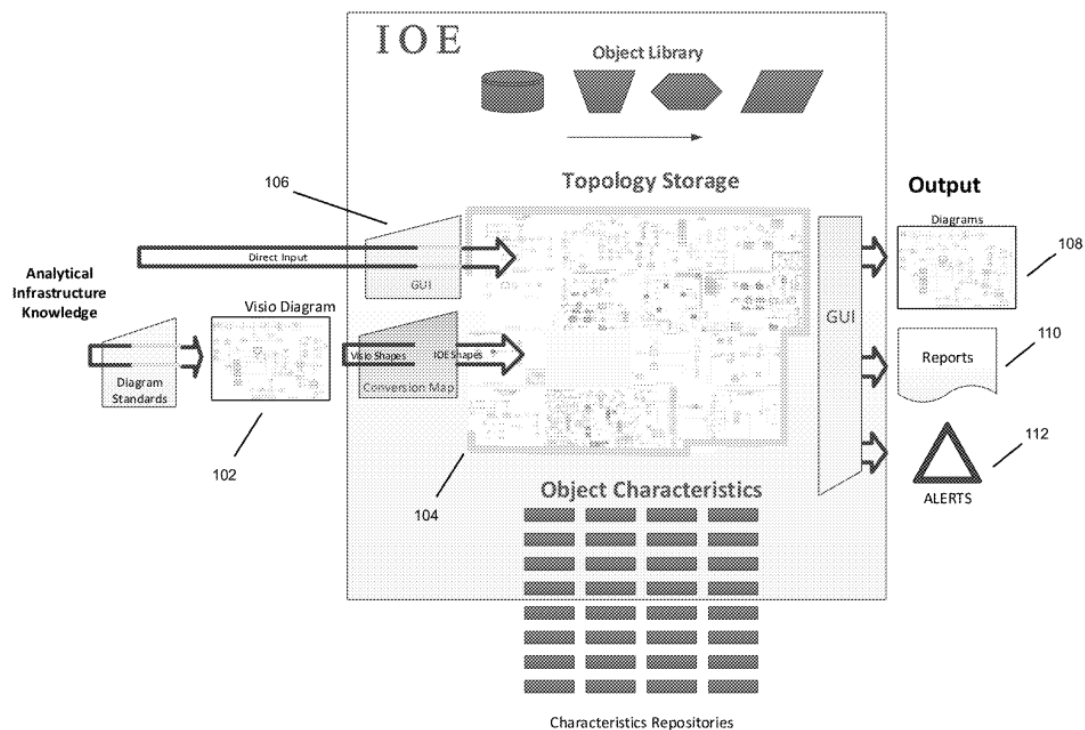


FIGURE 1

Figure 1 depicts an integrated object environment represented in a graph database.

Ex. 1006, 2:44–46, 5:28–33, Fig. 1. Referring to Figure 1, Keenan discloses:

[E]ach real world component in the infrastructure is defined as an object with associated characteristics such as state, and its relationship to other objects. The objects and characteristics are stored in a graphical format 102 such as a Visio file. The system converts the Visio files 102 into a standard, canonical format for storage in a topology graph database 104 of the infrastructure. Alternatively, a GUI 106 is provided for inputting directly into the topology database. Rendering software (GUI) 106 converts the graph database and associated characteristics into Views, which are exportable as diagrams 108, as well as reports 110 and alerts 112.

Id. at 5:33–44, Fig. 1. Keenan discloses one such view or report as a “Technical Risk Measurement view,” which “uses color to represent different types of risk (e.g., cyber, environmental, accidental, etc.).” *Id.* at 16:45–48, Fig. 7 (“Palette View” examples, including “Technical Risk Measurement”).

As shown in Figure 1, for example, Keenan also discloses that “[a] map is preset that maps Visio shapes and formats to IOE shapes and formats.” Ex. 1006, 18:36–37. In this context, a user selects an import function in the IOE GUI, “which first checks to see if [an] object already exists in [the] IOE based on external ID number first, then name match,” and “[i]f the object already exists, a message is posted to the screen, such as, ‘The following objects matched existing objects from the IOE, new relationships will be loaded to existing object.’” *Id.* at 18:37–43. Existing objects are then updated with new relationships based on the imported Visio diagram. *Id.* at 18:43–44.

Keenan discloses that “[t]he GUI of the IOE preferably includes *a variety of interactive functions* for the user.” Ex. 1006, 17:11–12 (emphasis added).

One such interactive function is path highlighting The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected. The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off.

Id. at 17:12–20.

We further discuss below the disclosure of Keenan in connection with the parties’ arguments.

3. *Analysis*

a) Dependent Claim 2

The parties dispute whether the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests to the skilled artisan the limitations of dependent claim 2, namely, “configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.” Pet. 42, 55–57; Pet. Reply 13–15; PO Resp. 33–39; PO Sur-reply 8–10.

We note that independent claim 4 (“attack simulation method”) and independent claim 12 (“attack simulation system”) both include the features of dependent claim 2. Petitioner first addresses these features in discussing dependent claim 2 (Pet. 42, 55–57), and then refers to that analysis in addressing the same features in independent claims 4 and 12 (Pet. 43–44

(4[p], 4[e]), 48–50 (12[p], 12[e]). Patent Owner responds in kind. *See* PO Resp. 33–40, 45–46. Thus, we likewise turn to dependent claim 2 to consider the parties’ arguments concerning the foregoing limitations.

(1) *The Petition*

Petitioner argues Zheng discloses the limitations of dependent claim 2 by describing, *inter alia*, “a ‘threat modeling layer’ that visualizes a threat actor and threat target, and a ‘displayable vector’ associating the threat actor and threat target that can ‘visualize an attack methodology by the threat actor on the threat target.’” Pet. 42 (citing Ex. 1005, 2:36–42 (“[T]he threat modeling layer *visualizes each security threat* as a threat actor, a threat target and a displayable vector connecting the threat actor to the threat target.” (emphasis added)), 5:6–24, 5:35–47, 7:13–48, 9:24–27, 10:10–11:3). According to Petitioner’s expert, Mr. Hurlbut, the skilled artisan “would understand that Zheng’s system may show attack paths of ‘all’ threats because Zheng discloses a system with data related to ‘know[n] or historical attacks’ that can have far-reaching impacts ‘across the entire ecosystem.’” Ex. 1003 ¶ 87 (cited at Pet. 42). Mr. Hurlbut also testifies that “a singular attack path of a threat may comprise ‘all’ threats in a system, and Zheng does not limit itself to identifying less than all threats.” *Id.*

Petitioner submits that the skilled artisan “would have found it obvious to modify Jones’ system to ‘visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component,’” and cites to, *inter alia*, its proffered evidence and arguments regarding reasons to combine the teachings of Jones, Zheng, and Keenan. Pet. 42 (citing Pet. § X.C.19; Ex. 1003 ¶ 88). In particular, as we understand Petitioner’s obviousness

argument, Petitioner *also* contends Zheng and Keenan *both* teach visual features and user selection features that, when combined with Jones, “would improve the overall user experience.” *See* Pet. 56 (citing Ex. 1003 ¶ 120) (cited at Pet. 42); *see id.* at § X.C.19.

For example, Zheng’s disclosure of displaying attack paths would enhance the system of Jones by allowing the user to view attack paths in [the] manner described in Zheng, which would enhance the user’s understanding of the potential threats.^[11] As another example, Keenan’s disclosure of *allowing a user to toggle between displaying or hiding certain features in a visual diagram* would enhance the system of Jones by providing the user with yet another option for displaying a diagram in the manner best suited for the user’s interests at the time.^[12] [The

¹¹ Zheng describes, for example, “*add[ing] interactive controls to the applications in the base layer 202*” “[d]epending on which layer(s) are *selected by a user for visualization*” (Ex. 1005, 8:18–24 (emphases added)); “*a user activat[ing] a toggle switch* such that both the threat modeling layer 204 and the security controls layer 206 are visualized” (*id.* at 11:57–12:14 (emphasis added)); a “user . . . interact[ing] with [a] resulting visualization . . . to achieve the desired display effects” and that “a particular type of threats in the threat modeling layer 204 can be toggled on or off to provide more focused visualization” (*id.* at 11:41–49); and that “the user can provide input to the computer (e.g., interact with a user interface element)” (*id.* at 13:9–23).

¹² Keenan describes, for example:

The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected. The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off.

Ex. 1006, 17:12–20 (emphases added). Patent Owner takes issue with the Board connecting this disclosure in Keenan to Petitioner’s statement *in the Petition* that “Keenan’s disclosure of allowing a user to toggle between

skilled artisan] would be motivated to include this feature in the system of Jones to allow a user to simplify a diagram by hiding a feature and then displaying that feature again *when the user instead wants to view the complete diagram*. EX-1003, ¶120. All human beings sometimes can better understand a visual presentation when it is simplified, and the *ability to toggle a visual feature* enables the presentation of a simpler view. *Id.*

Pet. 56 (emphases added); Ex. 1003 ¶ 120; *see id.* at 56–57 (discussing reasons to combine the asserted references and reasonable expectation of success).

(2) Patent Owner’s Response

Patent Owner responds initially by arguing that Petitioner cannot look beyond Zheng to teach the features of claim 2: “Petitioner and Mr. Hurlbut solely rely on Zheng for the teaching or suggestion of the elements of claim 2,” and “[n]o other reference is alleged to teach or suggest these claim features.” PO Resp. 33–34 (citing, *inter alia*, Ex. 2002, 85:15–24 (Mr. Hurlbut testifying during deposition: “Q. Did you rely on any other reference is [sic] in analyzing claim 2 here in paragraphs 87 and 88 [of your declaration testimony]? A. No. Just Zheng. Yes. Right. This is attack paths.”)).

Patent Owner argues “Zheng does not teach or suggest the selection of any threat model components much less the selection of ‘one’ threat model component” that would in turn causes all attack paths of all threats associated with the selected component to be displayed. PO Resp. 34–35. Similarly, Patent Owner argues, “[i]n Zheng, the display of information in

displaying or hiding certain features in a visual diagram would enhance the system of Jones” PO Resp. 38–39.

various layers is an all or nothing proposition – the entire layer is displayed or the entire layer is not displayed,” and thus, “[b]ecause Zheng either displays an entire layer or not, Zheng teaches that all potential paths from a threat to all potential targets can be displayed.” *Id.* at 35.

As for the combination of Jones, Zheng, and Keenan, Patent Owner argues “[t]he Petition and Mr. Hurlbut fail to provide an adequate explanation of how and why the teachings of Zheng and Jones can be combined.” PO Resp. 36; *see id.* at 36–38. Patent Owner argues “Jones expressly teaches looking at the attributes of threats one at a time,” but “Zheng on the other hand teaches displaying an entire layer or not displaying the layer at all,” so “[t]o the extent Zheng display[s] attack paths, Zheng displays all attack paths for all threats for all diagram components, or Zheng displays none at all.” *Id.* at 36; *see id.* at 37–38 (“Jones teaches displaying attributes of a single threat – not even all threats for a particular diagram component. Zheng is on the other end of the spectrum. Zheng displays all threats for all diagram components.”; “Jones allows a user to delve deeper into a threat model on a threat-by-threat basis. Zheng does not allow that threat-by-threat analysis.”).

(3) *Petitioner’s Reply*

Petitioner replies that “[Patent Owner] acknowledges that all aspects of dependent claim 2 are met, except for the user selection of one component to display the threat and attack paths because the only option in Zheng is to display an entire layer.” Pet. Reply 13. But, according to Petitioner, “[Patent Owner] ignores Zheng’s disclosure . . . that ‘[a] user can interact with the resulting visualization (step 820) to achieve the desired display effects.’” *Id.* at 14 (quoting Ex. 1005, 11:41–42).

Zheng's layers, including the threat modeling layer, "has sub-categories in the layer that can be toggled (e.g., enabled or disabled) by the user." *Id.*, 11:41-46. For example, "a particular type of threats in the threat modeling layer 204 can be toggled on or off to provide more focused visualization." *Id.*, 11:46-49. Thus, contrary to [Patent Owner's] argument that all attack paths in Zheng must be displayed, a user can display any portion of any layer as desired to provide a more focused visualization. A user could, for example, toggle off all threats except those for a specific component and thus display all attack paths for that specific component.

Pet. Reply 14; *see id.* at 14–15.

As for Petitioner's reasons for combining Jones and Zheng (and Keenan), Petitioner argues that Patent Owner "mischaracterizes both Zheng and Jones," because, according to Petitioner, "a user can select or toggle specific aspects of Zheng's layers to display specific attack paths 'to provide a more focused visualization.'" Pet. Reply 14–15. Petitioner also complains that Patent Owner is attacking Jones and Zheng (and Keenan) individually, rather than addressing whether the subject matter of claim 2 would have been obvious *to the skilled artisan* in light of the combined teachings of those references. *See id.* at. 15.

(4) Patent Owner's Sur-Reply

Patent Owner responds, "[f]irst, claim 2 requires the selection of 'one of the diagrammed threat model components,'" but "[t]he cited portion of Zheng toggles an entire type or sub-category of threats – not an individual threat"; and "[s]econd, claim 2 requires the selection of a threat model component," but "[t]he cited portion of Zheng toggles a sub-category of threats – not a threat model component." PO Sur-reply 8–9; *see id.* at 9

(“[C]laim 2 requires the selection of one threat model component – not a threat.”; “Jones only teaches displaying all threats at once.”).

Patent Owner complains that “[t]he Reply (improperly) cites to Zheng’s teachings related to the toggling of ‘sub-categories’ within a layer,” which were “not relied upon in the Petition.” PO Sur-reply 8–9 (referring to Ex. 1005, 11:41–55). We disagree with Patent Owner that Petitioner is changing its invalidity theory in its Reply as to dependent claim 2, and find Petitioner is legitimately responding to arguments in Patent Owner’s Response concerning claim 2 (see, for example, Patent Owner’s argument that “[i]n Zheng, the display of information in various layers is an all or nothing proposition” (PO Resp. 35)). *See Everstar Merch. Co. v. Willis Elec. Co.*, No. 2021-1882, 2022 WL 1089909, at *4 (Fed. Cir. Apr. 12, 2022) (“Any ambiguity as to whether a reply constitutes a new argument is eliminated when the reply is a legitimate reply to arguments introduced in a patent owner’s response or the Board’s institution determination.”). We also find Patent Owner’s substantive arguments unavailing, as discussed below.

(5) *Analysis*

We have considered Petitioner’s arguments and cited evidence concerning whether the combination of Jones, Zheng, and Keenan would have taught or at least fairly suggested the features of dependent claim 2 to the skilled artisan, and find them persuasive on the complete record before us.

In particular, given the following context:

(1) Jones describes a system for modeling and analyzing cybersecurity threats in an information system and displaying such models as threat-model data flow diagrams (DFD), where users may

select a shape (including shapes for threats) in the diagram that in turn recalls pop-up window 814, which includes data concerning the threat affecting a given component (Ex. 1004, 1:5–7, code (57), 19:10–28, Fig. 9; *see supra* § III.D; PO Resp. 36 (Patent Owner arguing that “Jones expressly teaches looking at the attributes of threats one at a time.”));

(2) Zheng describes that its “threat modeling layer *visualizes each security threat* as a threat actor, a threat target and *a displayable vector* connecting the threat actor to the threat target” (Ex. 1005, 2:36–42 (cited at Pet. 42) (emphases added));

(3) Patent Owner concedes that Zheng teaches at least that “*all* potential paths from a threat to *all* potential targets can be displayed” (PO Resp. 35; *see* Pet. Reply 13); and Petitioner’s expert, Mr. Hurlbut, likewise testifies that the skilled artisan “would understand that Zheng’s system may show attack paths of ‘all’ threats” (Ex. 1003 ¶ 87);

(4) Zheng describes toggling displayed threat model diagram features on or off “to achieve the *desired* display effects”:

A user can *interact* with the resulting visualization (step 820) *to achieve the desired display effects*. In some embodiments, at least one of the base layer 202, the threat modeling layer 204, the security controls layer 206, or the threat update layer 208 has *sub-categories in the layer that can be toggled* (e.g., enabled or disabled) by the user. For example, *a particular type of threats* in the threat modeling layer 204 *can be toggled on or off to provide more focused visualization*.

(Ex. 1005, 11:41–49 (cited at Pet. Reply 14) (emphases added));

(5) Zheng does not disparage or otherwise teach away from *displaying* attack paths of “all” threats directed against less than “all” potential targets (i.e., all threats compromising a single selected threat model component); and

(6) Mr. Hurlbut testifies that “[d]isplaying and manipulating diagrams on computers was well known at the time and [the skilled artisan] would [have been] well versed in such programs” (Ex. 1003 ¶ 121);

we find Petitioner’s position persuasive, namely, that Zheng (or more specifically, the combination of Jones, Zheng, and Keenan) would have taught *or at least fairly suggested* to the skilled artisan *in 2017* the features of dependent claim 2 (e.g., providing the *desired display effect* of displaying attack paths of all threats associated with diagrammed threat model components which compromise a selected threat model component). *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981); *In re Burckel*, 592 F.2d 1175, 1179 (CCPA 1979) (“[A] reference must be considered not only for what it expressly teaches, but also for what it fairly suggests.”).

Moreover, given that the skilled artisan would have known of *displaying* “all potential paths from a threat to all potential targets” (Zheng) (*see* PO Resp. 35) and *displaying* (at least) one threat to one potential target (Jones) (*see* Ex. 1004, code (57), 19:10–28, Fig. 9), and given the state of the art in 2017 including as reflected by Keenan, which describes selecting *one* object in a topology on a screen and toggling on or off the *displaying* of upstream and downstream flows into and out of the object selected (Ex. 1006, 17:12–20), we find it not credible that the skilled artisan in 2017 would not have considered it desirable (or feasible) *as a display option* to

visually display all attack paths against a user-selected threat model component. Indeed, the *data* for all such threats exists in the Zheng system (*see* PO Resp. 36 (“Zheng displays all attack paths for all threats for all diagram components.”)), the question becomes merely *which data* would the user desire to display.

We find Petitioner sufficiently establishes that the skilled artisan would have had a rational reason to combine these teachings of Jones and Zheng (and Keenan). Jones, Zheng, and Keenan all relate to systems for generating and displaying models of underlying systems (or processes, etc.), and combining the teachings and suggestions of Zheng (and Keenan) concerning visual features and display options as described above with Jones would, according to the testimony of Mr. Hurlbut, “improve the overall user experience” and “enhance the user’s understanding of the potential threats.” Ex. 1003 ¶ 120 (cited at Pet. 56); *see* Pet. 55–57. Mr. Hurlbut testifies that the skilled artisan would have combined the teachings of Zheng (and Keenan) concerning toggling on or off visual features of a model with Jones “to allow a user to simplify a diagram by hiding a feature and then displaying that feature again when the user instead wants to view the complete diagram.” Ex. 1003 ¶ 120 (cited at Pet. 56); *see id.* (“All human beings sometimes can better understand a visual presentation when it is simplified, and the ability to toggle a visual feature enables the presentation of a simpler view.”).

We find unavailing Patent Owner’s arguments that Petitioner has not sufficiently shown such a rational reason to combine the subject references. Patent Owner argues, in sum, that “Jones teaches displaying attributes of a single threat – not even all threats for a particular diagram component,” and

“Zheng is on the other end of the spectrum,” because “Zheng displays all threats for all diagram components.” PO Resp. 36–38. Patent Owner argues “[t]he Petition and Mr. Hurlbut do not attempt to reconcile these divergent teachings,” and they do not explain why the skilled artisan “would discard Jones’ teaching to display attributes about a single threat in favor of Zheng’s teaching to display all threats for all diagram components in a single layer.” *Id.* at 38; *see supra* § III.E.3.a.2. Patent Owner (and its expert) appears to argue that the ordinarily skilled artisan would not have physically (bodily) incorporated Zheng’s system into Jones’s system (or would not have known how to do so), but that is not the test of obviousness.

To prove obviousness, Petitioner need not show that the skilled artisan somehow would have incorporated Zheng’s system and its display structure or format within Jones’s system and its display structure or format. “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. . . . Rather, the test is what the combined teachings of those references would have suggested to those of ordinary skill in the art.” *Keller*, 642 F.2d at 425; *see In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) (“It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements.”); *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983) (“[I]t is not necessary that the inventions of the references be physically combinable to render obvious the invention under review.”).

We find Patent Owner’s dispute here also ignores substantial teachings of Zheng (and Keenan) concerning users interacting with models to achieve desired display effects and to toggle on or off various sub-

categories of data displayed to users. *See, e.g.*, PO Resp. 36–38; Pet. Reply 14 (quoting Ex. 1005, 11:41–49 (Zheng: “A user can interact with the resulting visualization (step 820) to achieve the desired display effects.”; “[A] particular type of threats in the threat modeling layer 204 can be toggled on or off to provide more focused visualization.”)); Pet. 56 (citing Ex. 1003 ¶ 120; paraphrasing Ex. 1006, 17:12–20 (Keenan: “The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected.”; “Clicking again on the object toggles this feature off.”)). We find these teachings of Zheng (and Keenan) weigh against Patent Owner’s position. *See Fleming v. Cirrus Design Corp.*, 28 F.4th 1214, 1223 (Fed. Cir. 2022) (“When considering obviousness of a claimed invention, the Supreme Court has emphasized that the ‘person of ordinary skill is also a person of ordinary creativity, not an automaton.’”).

We find, as argued by Petitioner, the skilled artisan would have had a reasonable expectation of success in combining the teachings of Jones and Zheng (and Keenan) as discussed above, because “[d]isplaying and manipulating diagrams on computers was well known at the time and [the skilled artisan] would be well versed in such programs” (Ex. 1003 ¶ 121 (cited at Pet. 56–57); *see* Pet. 56–57 (“Computer-based threat modeling involves very predictable technologies, and [the skilled artisan] would not [have] encounter[ed] any insurmountable challenged in implementing this combination.”)). Although Patent Owner disputes whether a rational reason exists to combine the subject references (discussed above), Patent Owner otherwise does not dispute reasonable expectation of success. *See generally* PO Resp. 36–38.

Based on the foregoing and the complete record before us, we are persuaded that Petitioner's cited evidence provides sufficient rational reasons to combine Jones, Zheng, and Keenan with a reasonable expectation of success in doing so, and sufficiently establishes that the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests the limitations of dependent claim 2.

(6) Conclusion for Dependent Claim 2

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 2 would have been obvious over the combination of Jones, Zheng, and Keenan.

b) Independent Claims 4 and 12

Petitioner contends independent claims 4 and 12 are substantially the same as dependent claim 2 (including underlying independent claim 1), except that features of "threat model chaining method" claim 2 (and claim 1) are variously embodied in "attack simulation method" claim 4 and "attack simulation system" claim 12. Pet. 43–44 (citing Ex. 1003 ¶¶ 89–94), 48–50 (citing Ex. 1003 ¶¶ 104–108); Pet. Reply 15–17. Patent Owner argues patentability of independent claims 4 and 12 based on the same reasons provided for independent claim 1 and dependent claim 2. *See* PO Resp. 39–40, 45–46; PO Sur-reply 10. We agree with the parties that independent claims 4 and 12 recite limitations commensurate in scope with independent claim 1 and dependent claim 2. Thus, for the same reasons provided above for independent claim 1 and dependent claim 2, and the reasons set forth in the Petition (Pet. 43–44, 48–50), we conclude that Petitioner has demonstrated by a preponderance of the evidence that

independent claims 4 and 12 would have been obvious over the combination of Jones, Zheng, and Keenan.

c) *Dependent Claims 6 and 7*

Dependent claims 6 and 7 recite:

6. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving a *user toggle* of one of the diagrammed compensating controls (hereinafter “first control”) of the first threat model to an *on state* through the one or more interfaces, *toggle all attack paths mitigatable by the first control to a mitigated display state*.

7. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving a *user toggle* of the first control to an *off state* through the one or more interfaces, *toggle all attack paths mitigatable by the first control to an unmitigated display state*.

Ex. 1001, 36:49–61 (emphases added). Claim 6 is directed to toggling “on” the *display* of all attack paths mitigatable by the first control in a mitigated state, and claim 7 is directed to toggling “off” that mitigated display state. Or in today’s parlance, in claim 6, a user clicks on a compensating control icon to display all attack paths mitigatable by that control, and in claim 7, the user clicks on the icon again to stop such a display.

Petitioner contends the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests the features of dependent claims 6 and 7.

Pet. 45–46 (citing Ex. 1003 ¶¶ 97–98); Pet. Reply 16. In particular, Petitioner argues:

Keenan discloses toggling various features on and off. EX-1006 at 12:29-35; 17:19-21[] (“The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. **Clicking again on the object toggles this feature off.** Paths upstream and downstream from up to six objects can be toggled on at the same

time. A different highlighting color may be used for each.”). Thus, Keenan discloses a “user toggle” that allows a user to turn a feature on and off.

Pet. 45. Petitioner argues “Jones discloses the diagrammed compensating controls and the diagram interface,” and “Zheng discloses diagrammed attack paths.” Pet. 46. Petitioner’s expert, Mr. Hurlbut, persuasively testifies:

[The skilled artisan] would have found it obvious to combine these features of Jones and Zheng with the toggling feature of Keenan to “toggle all attack paths mitigatable by the first control to a mitigated display state,” as claimed because, among other reasons, [the skilled artisan] would have recognized the utility of using a toggle feature to highlight certain features of the diagrammed threat model as shown in Keenan.

Ex. 1003 ¶ 98 (cited at Pet. 46); *see* Pet. 46 (citing, *inter alia*, Pet. § X.C.19).

Petitioner argues that just as the attack paths may be toggled on the diagram interface to a mitigated display state, they also may then be toggled to an unmitigated display state. Pet. 46. We find Petitioner’s arguments persuasive.

Patent Owner disputes Petitioner’s contentions. PO Resp. 40–42; PO Sur-reply 10–11. Patent Owner argues “Jones does not teach or suggest the display of ‘compensating controls’ on the relational diagram recited in claim 4.” PO Resp. 41; PO Sur-reply 10. We disagree, as discussed above in Section III.D.2.a.1 (limitation 1[e]).

Patent Owner argues “none of the cited references teach or suggest ‘security controls’ [(which term is not recited in claims 6 or 7)] or ‘mitigations’ that can be set to an on state and cause the system to ‘toggle all attack paths mitigatable by the first control to a mitigated display state.’” PO Resp. 41; PO Sur-reply 10. But Patent Owner here attacks the references

individually, and ignores what the *combined* disclosures of Jones, Zheng, and Keenan would have taught or at least fairly suggested to the skilled artisan in 2017. The test for obviousness is not whether the claimed invention is expressly suggested in any one or all of the references, as argued by Patent Owner (*see* PO Resp. 41), but whether the claimed subject matter would have been obvious to those of ordinary skill in the art *in light of the combined teachings of those references*. *See In re Keller*, 642 F.2d at 425; *In re Burckel*, 592 F.2d at 1179 (“[A] reference must be considered not only for what it expressly teaches, but also for what it fairly suggests.”).

Patent Owner argues again that the skilled artisan would not have combined the teachings of Jones and Zheng, and thus, would not have arrived at the features of dependent claims 6 and 7. PO Resp. 41–42; PO Sur-reply 10–11. We disagree, as discussed above in Section III.E.3.a.5.

Petitioner replies that “[Patent Owner’s] challenges to dependent claims 6 and 7 appear to primarily relate back to [Patent Owner’s] arguments for claims 1 and 4 and thus fail for the same reasons.” Pet. Reply 16. As discussed above, we agree.

We find Patent Owner’s dispute here again ignores substantial teachings of Zheng and Keenan concerning users interacting with models to achieve desired display effects and to toggle on or off various sub-categories of data displayed to users. *See, e.g.*, Ex. 1005, 11:41–49 (Zheng: “A user can interact with the resulting visualization (step 820) to achieve the desired display effects.”; “[A] particular type of threats in the threat modeling layer 204 can be toggled on or off to provide more focused visualization.”); Ex. 1006, 17:12–20 (Keenan: “The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream

flows into and out of the object selected.”; “Clicking again on the object toggles this feature off.”). We find these teachings of Zheng and Keenan weigh against Patent Owner’s position. *See KSR*, 550 U.S. at 421 (“A person of ordinary skill is also a person of ordinary creativity, not an automaton.”).

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 6 and 7 would have been obvious over the combination of Jones, Zheng, and Keenan.

d) Dependent Claim 8

Dependent claim 8 recites:

8. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving one or more *user inputs* through the one or more interfaces *to remove the first control from the first threat model*, *toggle* all attack paths mitigatable by the first control *to an unmitigated display state*.

Ex. 1001, 36:62–67 (emphases added). As noted above, dependent claim 7, which depends from claim 6, is directed to toggling “off” the mitigated display state to revert to the unmitigated display state. Dependent claim 8, which also depends from claim 6, is directed to “remov[ing]” the compensating control causing the mitigated display state from the model to likewise revert to the unmitigated display state—both claims 7 and 8 cause the mitigatable attack paths being displayed as mitigated to revert to being displayed as unmitigated.

Petitioner contends the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests the features of dependent claim 8. Pet. 46–47 (citing Ex. 1003 ¶ 100); Pet. Reply 16–17. In particular, Petitioner argues that “[c]laims 7 and 8 are substantively identical except for

instead of ‘user toggle’ in claim 7, claim 8 uses the term ‘one or more user inputs through the one or more interfaces to remove the first control from the first threat model.’” Pet. 47; Pet. Reply 16. Similarly, Petitioner’s expert, Mr. Hurlbut, persuasively testifies that the skilled artisan “would understand that there is no substantive difference between a ‘user toggle’ in claims 6-7 and ‘one or more user inputs through one or more interfaces to remove the first control from the first threat model,’” because “[i]n either term, a user inputs into an interface to toggle a control off in the threat model to an unmitigated state.” Ex. 1003 ¶ 100 (cited at Pet. 47); *see* Pet. 47; Pet. Reply 16. “In other words,” according to Petitioner, “the [skilled artisan] would have found it obvious to simply remove a control instead of using a user toggle,” because “[c]ontrary to [Patent Owner’s] argument, removing a control is effectively the same as toggling it off, and a user can easily re-add a removed control.” Pet. Reply 16–17. We find Petitioner’s arguments persuasive.

Patent Owner argues that “[i]nstead of turning off a compensating control as recited in claim 7, claim 8 requires that the compensating control be removed entirely from the relational diagram.” PO Resp. 42. Patent Owner argues “[c]laims having different words are presumed to have different meanings” as a reason to treat claim 8 differently than claim 7. *Id.* at 42–43. Patent Owner argues that “removing is different than toggling off a feature,” because “[r]emoving entails deleting the control from the threat model such that it is no longer part of the threat model,” whereas “[t]oggling a compensating control off leaves the control in place so that it can be easily toggled on without having to be added back to the threat model.” PO Sur-reply 11. We find Patent Owner’s arguments unavailing.

Claims 7 and 8 *both* require “configuring the diagram interface to . . . toggle all attack paths mitigatable by the first control to an unmitigated *display* state.” *See* Ex. 1001, 36:56–61, 36:62–67 (emphasis added). Any difference between claims 7 and 8 relates only to what *user input* triggers the diagram interface to execute such toggling. In claim 7, the *user input* is toggling the first control to an “off” state (e.g., clicking on the control icon to turn it “off”), and in claim 8 the *user input* is an input to “remove” the first control from the threat model (e.g., clicking on the icon or an option to “remove” it). Contrary to Patent Owner’s arguments (PO Resp. 42), however, nothing in claim 8 requires “the compensating control [itself] be removed entirely from the relational diagram.” Indeed, the *user input* to “remove” the first control in the model, like the *user input* to toggle “off” the first control in the model, merely triggers the display to show the unmitigated display state. In this case, we find the scope of a user input to turn “off” the first control to in turn toggle all attack paths mitigatable by the first control to an unmitigated display state overlaps at least in part with a user input to “remove” that first control to effect the same outcome. Thus, we find Petitioner sufficiently establishes that the subject references collectively teach or fairly suggest the features of claim 8 for the same reasons given above for claim 7.

In addition, as discussed above for claims 6 and 7, Patent Owner’s dispute here with claim 8 again ignores substantial teachings of Zheng and Keenan concerning users interacting with models to achieve desired display effects and to toggle on or off various sub-categories of data displayed to users. *See, e.g.*, Ex. 1005, 11:41–49, 17:12–20. Claim 8 recites a desired user input to trigger a desired display effect for a threat model. Patent

Owner ignores these collective teachings of the asserted references. We find these teachings of Zheng and Keenan also weigh against Patent Owner's position. *See KSR*, 550 U.S. at 421 ("A person of ordinary skill is also a person of ordinary creativity, not an automaton.").

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 8 would have been obvious over the combination of Jones, Zheng, and Keenan.

e) Dependent Claim 9

Dependent claim 9 recites:

9. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more *user inputs* through the one or more interfaces, *visually display only attack paths of all threats associated with a subset of the diagrammed threat model components*.

Ex. 1001, 37:1–6 (emphases added).

Petitioner contends the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests the features of dependent claim 9. Pet. 47 (citing Ex. 1003 ¶ 101); Pet. Reply 17. Petitioner's expert, Mr. Hurlbut, persuasively testifies that the skilled artisan "would understand that Keenan's display toggle feature may be incorporated into any element of Jones and Zheng," and "[t]herefore, on an interface, a user may toggle off all features except for the attack paths, thus 'visually display[ing] only attack paths of all threats associated with a subset of the diagrammed threat model components.'" Ex. 1003 ¶ 101 (cited at Pet. 47); *see* Pet. 47.

Patent Owner responds that "[n]either Petitioner nor Mr. Hurlbut make any effort to show that the prior art teaches or suggests displaying attack paths of threats associated with 'a subset' of the diagrammed threat

model components.” PO Resp. 43–44. Petitioner replies that since the combination of asserted references would have taught or suggested to the skilled artisan that “a user may toggle any aspect of the system,” then this likewise would have taught or suggested that “the user may select a ‘subset’ of components” for such toggling. Pet. Reply 17. Patent Owner responds by again arguing, in sum, that Zheng discloses an “all or nothing” display of information layers, which does not teach or suggest displaying attack paths of threats associated with a “subset” of threat model components. We disagree and, and for the reasons previously discussed, find Patent Owner’s arguments unavailing. *See supra* § III.E.3.a.5 (analysis of claim 2).

We note that dependent claim 9 requires “visually display[ing] only attack paths of all threats associated with *a subset of the diagrammed threat model components*,” and dependent claim 2 requires “visually display[ing] attack paths of all threats associated with *the diagrammed threat model components which compromise the selected threat model component*”—the latter *is* a “subset” of the diagrammed threat model components. Claim 9 also requires configuring the diagram interface in response to receiving “user inputs,” and claim 2 requires doing so in response to receiving “a user selection of one of the diagrammed threat model components of the first threat model”—again, the latter *is* a “user input.” Thus, our analysis as to dependent claim 2 also applies to dependent claim 9.

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 9 would have been obvious over the combination of Jones, Zheng, and Keenan.

f) Dependent Claim 10

Dependent claim 10 recites:

10. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more *user inputs* through the one or more interfaces to alter a profile of an attacking component, *alter the visually displayed attack paths*.

Ex. 1001, 37:7–11 (emphases added).

Petitioner contends the combination of Jones, Zheng, and Keenan teaches or at least fairly suggests the features of dependent claim 10. Pet. 48 (citing Ex. 1003 ¶ 102); Pet. Reply 17. Petitioner argues “Zheng discloses displayed attack paths,” and “Keenan discloses modifying a display,” such as “a Modify mode, where the user can add, change and delete.” Pet. 48 (citing Ex. 1006, 11:42–56). Petitioner’s expert, Mr. Hurlbut, persuasively testifies that the skilled artisan “would have found it obvious to combine Keenan’s disclosure of modifying a display with Zheng’s disclosure of displayed attack paths to allow a user through inputs through one or more interfaces to ‘alter a profile of an attacking component, alter the visually displayed attack paths’ as claimed.” Ex. 1003 ¶ 102 (cited at Pet. 48).

Patent Owner responds by again arguing, in sum, that Zheng discloses an “all or nothing” display of information layers, which the skilled artisan would not have combined with Jones and Keenan to achieve the features of dependent claim 10. See PO Resp. 44–45 (“But Jones’ and Keenan’s ability to view or edit individual components is at the opposite end of the spectrum compared to Zheng which only display[s] layers with no ability to modify or even view individual components.”); PO Sur-reply 12–13. We disagree, and for the reasons previously discussed, find Patent Owner’s arguments

unavailing. *See supra* § III.E.3.a.5 (analysis of Zheng, the combination of Jones, Zheng, and Keenan, and claim 2).

In addition, as discussed above for claims 6, 7, and 8, Patent Owner’s dispute here with claim 10 again ignores substantial teachings of Zheng and Keenan concerning users interacting with models to achieve desired display effects and to toggle on or off various sub-categories of data displayed to users. *See, e.g.*, Ex. 1005, 11:41–49, 17:12–20. Claim 10 recites a desired user input to trigger a desired display effect for a threat model. Patent Owner ignores these collective teachings of the asserted references. We find these teachings of Zheng and Keenan also weigh against Patent Owner’s position. *See KSR*, 550 U.S. at 421 (“A person of ordinary skill is also a person of ordinary creativity, not an automaton.”).

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 10 would have been obvious over the combination of Jones, Zheng, and Keenan.

g) Dependent Claim 19

Dependent claim 19 recites:

19. The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more *user inputs*, *diagram* a communication protocol between two of the *diagrammed* threat model components, the *diagrammed* communication protocol including an alphanumeric indicator.

Ex. 1001, 38:33–38 (emphases added).

Petitioner contends the combination of Jones, Zheng, and Keenan, and in particular, Jones, teaches or at least fairly suggests the features of dependent claim 19. Pet. 52–54 (citing Ex. 1003 ¶ 115–116); Pet. Reply 18–20. Petitioner argues that Jones’s Figure 9, reproduced above in

Section III.D.1, discloses “a diagrammed communication protocol including one or more alphanumeric indicators.” Pet. 52–54. Petitioner submits that “the communication protocol between the end user 810 and the computing device 804 is ‘User Input/Responses,’” and “communication protocols between the computing device 804 and the example server(s) 806 include ‘Auth N token’ and ‘ITAR file request’ labels.” Pet. 54.

Patent Owner admits that Zheng, which is one of the asserted references in combination, “discloses a long list of communication protocols,” but argues that “‘User Input/Responses,’ ‘Auth N token’ and ‘ITAR file requests’ are not communication protocols, they are data.” PO Resp. 49; Ex. 1005, 13:38–14:4 (Zheng listing many communication protocols for data transfer between system components). Patent Owner argues that Petitioner’s expert, Mr. Hurlbut, admitted this distinction at his deposition. *See id.* at 49 (Patent Owner arguing, “Mr. Hurlbut effectively contradicted his declaration and admitted that information such as usernames and passwords were just data and were not communication protocols.” (citing Ex. 2002, 108:9–24; Ex. 2003 ¶ 149)).

Petitioner replies that “Mr. Hurlbut further testified a ‘user name and password’ is not a communication protocol, *but that they are ‘transmitted using a communication protocol,’*” and argues that “[t]he user name and password is the data being transferred, and one communication protocol (*i.e.*, the method of communicating) is the user input or responses—which is exactly what Mr. Hurlbut testified is the communication protocol.” PO Resp. 18–19 (citing Ex. 2002, 108:13–24) (emphasis added). Petitioner argues “Jones [Figure] 9 diagrams the ‘User Input/ Responses’ and then shows an arrow 812 labeled ‘username / password’ showing the transfer of

the user name and password data via the ‘User Input / Responses.’” *Id.* at 19 (citing Ex. 1004, Fig. 9). Petitioner argues, “even to the extent Jones’ alphanumeric indicators are data, [the skilled artisan] would understand that Jones’ alphanumeric indicators are representations of communication protocols because such data is transferred by a communication protocol.” *Id.* at 19 (citing Ex. 2002, 108:13–24).

Patent Owner responds that “Jones does not actually disclose any communication protocols and yet Petitioner (and Mr. Hurlbut) used the Jones reference as allegedly teaching or suggesting diagramming of a communication protocol between two threat model components where the communication protocol includes an alphanumeric indicator.” PO Sur-reply 15. We find Patent Owner’s arguments unavailing and not commensurate with the scope of claim 19.

Claim 19 recites diagramming a communication protocol between two diagrammed threat model components, and the ’008 patent depicts this as a line with an arrow between two such components. *See* Ex. 1001, 16:58–17:11, 38:33–38, Fig. 10. Petitioner points to lines with arrows between such components and identifies such lines by their labels, namely “User Input/Responses,” “Auth N token,” and “ITAR file request.” Pet. 52–54 (referring to Ex. 1004, Fig. 9). Claim 19 also recites that the diagrammed communication protocol “include[es] an alphanumeric indicator,” without more, and without limiting such “indicator” to identifying the communication protocol itself or any other information. *See* Ex. 1001, 38:33–38. Petitioner points to the aforementioned text labels as alphanumeric indicators. Thus, we find Petitioner sufficiently evidences that

Jones (and the combination of asserted references) teaches or at least fairly suggests the features of dependent claim 19.

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 19 would have been obvious over the combination of Jones, Zheng, and Keenan.

h) Dependent Claims 11, 13–17, and 20

The parties agree (as do we) that the features of dependent claims 11, 13–17, and 20 are commensurate in scope with the features of limitation 1[f] and dependent claims 6–11, respectively, and both parties rely on the same arguments and evidence in addressing each of these parallel claims. *See* Pet. 48, 50–51, 54; PO Resp. 45–47; Pet. Reply 17–18; PO Sur-reply 13–14, 16. Thus, for the same reasons provided above for independent claim 1 (particularly limitation 1[f]) and dependent claims 6–11, we conclude that Petitioner has demonstrated by a preponderance of the evidence that dependent claims 11, 13–17, and 20 would have been obvious over the combination of Jones, Zheng, and Keenan.

i) Dependent Claims 5 and 18

Petitioner contends claims 5 and 18, which depend directly from independent claims 4 and 12, respectively, would have been unpatentable as obvious over the combination of Jones, Zheng, and Keenan. Pet. 44–45, 51–52. The Petition provides a detailed assessment of these claims, with references to the Petition’s analysis of claims 4 and 12, disclosures in the asserted combination of references, and the testimony of Petitioner’s expert, Mr. Hurlbut. *Id.* Patent Owner does not contend that the limitations in claims 5 and 18 are absent in the combination of Jones, Zheng, and Keenan, and therefore, has waived such arguments. *See* 37 C.F.R. § 42.23(a); *In re*

Nuvasive, 842 F.3d at 1379–82; *see generally* PO Resp.; PO Sur-reply.

As discussed above, we are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that independent claims 4 and 12 would have been unpatentable as obvious over the combination of Jones, Zheng, and Keenan, and also are persuaded that the cited evidence sufficiently shows claims 5 and 18 likewise obvious. For the same reasons provided above for independent claims 4 and 12, and the reasons set forth in the Petition (Pet. 44–45, 51–52), we conclude that Petitioner has demonstrated by a preponderance of the evidence that dependent claims 5 and 18 would have been unpatentable as obvious over the combination of Jones, Zheng, and Keenan.

4. *Summary*

For the foregoing reasons, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 1–20 would have been unpatentable as obvious over the combination of Jones, Zheng, and Keenan.

F. Obviousness of (1) Claims 1–20 over the Combination of Jones, Zheng, Keenan, and Yu; (2) Claims 1–20 over the Combination of Jones, Zheng, Keenan, Yu, and Reith; and (3) Claims 5–8 and 13–15 over the Combination of Jones, Zheng, Keenan, Yu, Reith and “the knowledge of a POSITA”

Petitioner contends (1) claims 1–20 would have been unpatentable under 35 U.S.C. § 103 as obvious over the combination of Jones, Zheng, Keenan, and Yu (Pet. 57–60 (“Ground 3”)); (2) claims 1–20 would have been unpatentable under 35 U.S.C. § 103 as obvious over the combination of Jones, Zheng, Keenan, Yu, and Reith (Pet. 60–62 (“Ground 4”)); and (3) claims 5–8 and 13–15 would have been unpatentable under 35 U.S.C.

§ 103 as obvious over the combination of Jones, Zheng, Keenan, Yu, and Reith and “the knowledge of a POSITA” (Pet. 62–63 (“Ground 5”)).

As discussed above in Sections III.D and III.E, we conclude that Petitioner has demonstrated by a preponderance of the evidence that all of the Challenged Claims (i.e., claims 1–20) are unpatentable under 35 U.S.C. §§ 102 or 103. Therefore, resolution of this proceeding does not require assessment of the foregoing additional challenges (i.e., (1), (2), and (3) above), and so for efficiency purposes, we need not and do not herein address these challenges. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359 (2018) (holding a petitioner “is entitled to a final written decision addressing all of the claims it has challenged”); *Boston Sci. Scimed, Inc. v. Cook Grp. Inc.*, 809 F. App’x 984, 990 (Fed. Cir. 2020) (non-precedential) (recognizing that the “Board need not address issues that are not necessary to the resolution of the proceeding” and, thus, agreeing that the Board has “discretion to decline to decide additional instituted grounds once the petitioner has prevailed on all its challenged claims”).

IV. CONCLUSION

Petitioner has met its burden to show, by a preponderance of the evidence, that all of the Challenged Claims (i.e., claims 1–20) would have been unpatentable under 35 U.S.C. §§ 102 or 103.¹³ Because of this

¹³ 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. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent

determination accounting for all Challenged Claims, we exercise our discretion to decline to decide Petitioner's additional challenges to the same claims.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–20 of U.S. Patent No. 10,699,008 B2 are unpatentable; and

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

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).

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 3	102	Jones	1, 3	
1–20	103	Jones, Zheng, Keenan	1–20	
1–20	103	Jones, Zheng, Keenan, Yu ¹⁴		
1–20	103	Jones, Zheng, Keenan, Yu, Reith ¹⁵		
5–8, 13–15	103	Jones, Zheng, Keenan, Yu, Reith ^{16,17}		
Overall Outcome			1–20	

¹⁴ We do not reach the ground based on Jones, Zheng, Keenan, and Yu as to claims 1–20 because we determined those claims would have been unpatentable as anticipated or obvious over other grounds.

¹⁵ We do not reach the ground based on Jones, Zheng, Keenan, Yu, and Reith as to claims 1–20 because we determined those claims would have been unpatentable as anticipated or obvious over other grounds.

¹⁶ *See supra* n.3.

¹⁷ We do not reach the ground based on Jones, Zheng, Keenan, Yu, Reith, “and the knowledge of a POSITA” as to claims 5–8 and 13–15 because we determined those claims would have been unpatentable as obvious over other grounds.

IPR2023-00821
Patent 10,699,008 B2

FOR PETITIONER:

Brent Yamashita
Blake Jackson
Matthew Middleton
DLA PIPER LLP (US)
brent.yamashita@us.dlapiper.com
blake.jackson@us.dlapiper.com
matthew.middleton@us.dlapiper.com

FOR PATENT OWNER:

Donald L. Jackson
Marc Kaufman
RIMON P.C.
donald.jackson@rimonlaw.com
marc.kaufman@rimonlaw.com