

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*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

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”). Petitioner identifies itself and IriusRisk SL as real parties in interest. Pet. 1. ThreatModeler Software, Inc. (“Patent Owner”) identifies itself as a real party in interest (Paper 3, 2), and timely filed a Preliminary Response to the Petition (Paper 6, “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b) (2018); 37 C.F.R. § 42.4(a) (2022). We may not institute an *inter partes* review “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential). When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim. 37 C.F.R. § 42.108(a).

Applying those standards, and upon consideration of the information presented in the Petition and Preliminary Response, we determine that Petitioner has demonstrated a reasonable likelihood of success in proving that at least one claim of the ’008 patent is unpatentable. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a). Accordingly, we institute an *inter partes* review

as to all Challenged Claims of the '008 patent on all grounds raised in the Petition.

II. BACKGROUND

A. *Related Matters*

The parties indicate that the '008 patent is 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 indicates that Patent Owner asserts related U.S. Patent No. 10,713,366 B2 against Petitioner in the District Court Case. Pet. 1. The '366 patent is the challenged patent in IPR2023-00656, now instituted and pending before the Board. *See IriusRisk Inc. v. ThreatModeler Software, Inc.*, IPR2023-00656, Paper 7 (PTAB Oct. 6, 2023).

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 continuations-in-part to four U.S. Provisional Patent Applications filed in 2017 (priority is not presently 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.

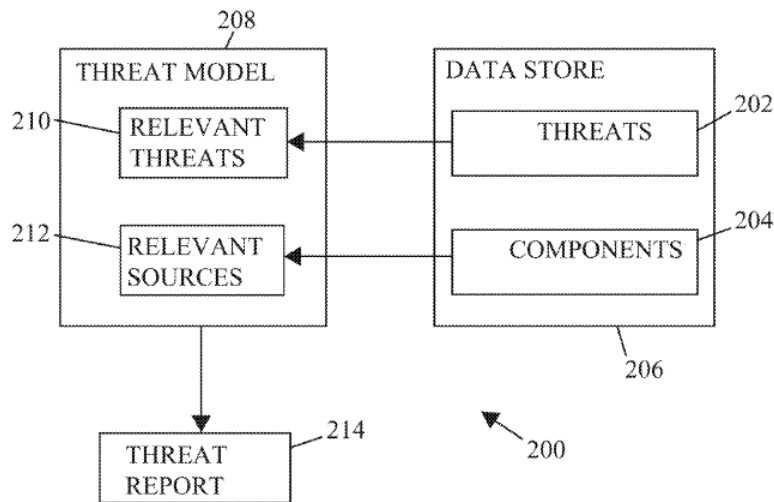


Figure 2 depicts a representative example of a threat modeling process.

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”).

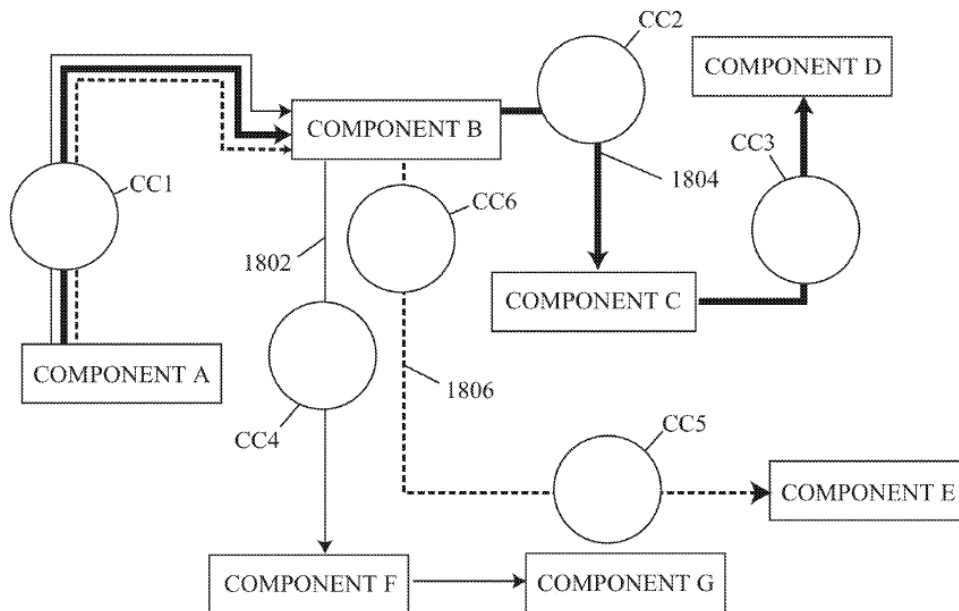


FIG. 19

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 challenged 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).

At this stage of the proceeding, Patent Owner does not rely upon a declarant of its own.

E. Asserted Challenges to Patentability

Petitioner challenges the patentability of claims 1–20 of the '008 patent on the following bases (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) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

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)).

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 Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). When evaluating a

⁴ At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

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)).

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 at this stage of the proceeding. *See generally* Prelim. Resp.

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) (citation omitted). 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, at least at this stage of the proceeding, 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))).

Petitioner proffers constructions for two terms, namely, (1) “threat model components” and (2) “attack paths,” as recited, for example, in independent claim 4. Pet. 12. Petitioner submits that it defines these two terms “consistent with the ’008 patent specification and applies the plain and ordinary meaning that [the skilled artisan] would attribute to the remaining terms.” Pet. 12. “Patent Owner submits that the Board need not engage in any pre-institution claim construction of these [two] terms.” Prelim. Resp. 11. Based upon our consideration of the record at this stage of the proceeding, we conclude that it is unnecessary to interpret expressly any term in the ’008 patent claims for which we institute *inter partes* review. *See Nidec*, 868 F.3d at 1017.

Nevertheless, we determine that briefing during the trial on the proper interpretation of certain claim terms may assist us in resolving issues presented in this case. In particular, we invite 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, and to provide evidentiary

support therefor (the parties should focus particularly on defining the full scope of what it means to “redefine” the first threat model and to “include” a second threat model “in” a first threat model). To the extent that a party proposes that this limitation should have its ordinary and customary meaning, we encourage the party to explicitly identify such meaning(s) and the evidentiary support therefor. In addition, the parties should consider whether *Ex parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential) applies to limitations of the challenged claims, such as claim 1’s recital of “configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model.”

D. Alleged 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. Patent Owner opposes Petitioner’s contentions. Prelim. Resp. 11–17. Based on our review of the record before us, we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1 and 3 are unpatentable as anticipated by Jones, as discussed below. 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 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.

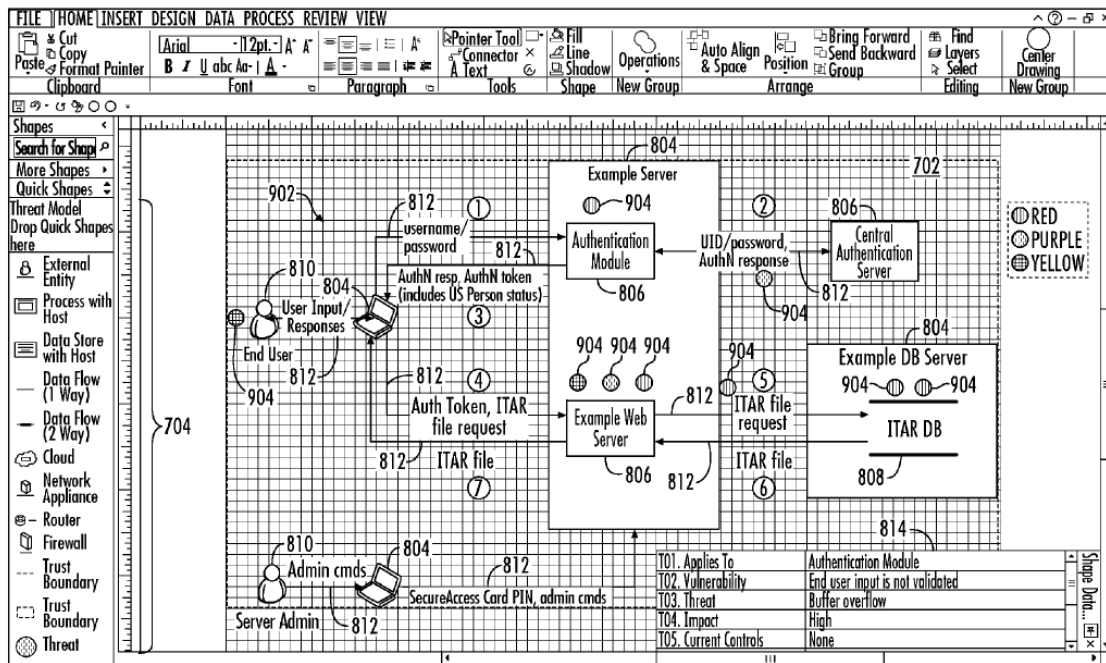


FIG. 9

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.

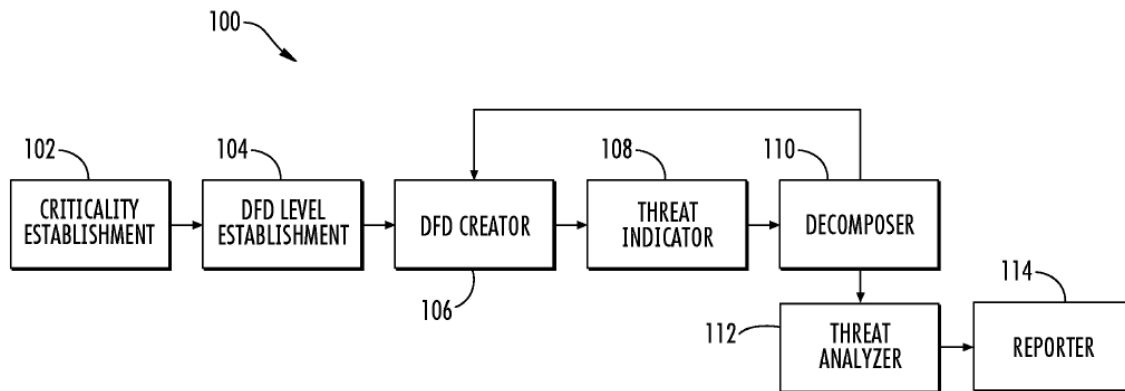


FIG. 1

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 explicitly or inherently discloses to the skilled artisan limitation 1[f], namely, “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. 35–40; Prelim. Resp. 11–17.

(1) *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*”

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).

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).

Patent Owner responds, in sum, that “Jones fails to disclose any ‘second threat model’ as claimed, and the entire Element 1[f] directed to this claimed feature is neither disclosed nor suggested by Jones.” Prelim. Resp. 11–12; *see id.* at 11–17. Based on the record before us at this stage of the proceeding, we disagree and preliminarily find Patent Owner’s arguments unavailing, as further discussed below.

In particular, Patent Owner argues:

Nowhere does Petitioner identify a “second threat model” in Jones. Petitioner argues that this feature is satisfied by Jones “creating a level n+1 threat model with one or more nested components.” Pet., 36. But Petitioner identifies no “second threat model” in this discussion, and identifies no instance in which Jones redefines a first threat model by including in it a second threat model.

Prelim. Resp. 13–14. But Patent Owner appears to attack only select portions of Petitioner’s cited disclosure in Jones, and not the full weight of the totality of such cited disclosure.

For example, 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*.

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. Based on the record before us, we find Petitioner’s arguments persuasive.

In addition, although Patent Owner argues the Board need not construe any limitations at this stage of the proceeding (Prelim. Resp. 11), it appears that Patent Owner bases its above arguments on a narrow, *and not yet proffered*, construction of the limitation “*redefine* the first threat model by *including in it* a second threat model associated with the component group.” As we stated above in Section III.C, the parties during trial should focus particularly on defining the full scope of what it means to “redefine” the first threat model and to “include” a second threat model “in” a first threat model.

Patent Owner also argues Petitioner’s reliance on Figure 9 “is not explained cogently,” and regardless, “Jones’s disclosure of a level n DFD 902 including threats 904 [as shown in Figure 9] is not tantamount to “redefine[ing] the first threat model by including in it a second threat model associated with the component group.” Prelim. Resp. 15. But as we understand Petitioner’s argument (and its expert’s testimony), Petitioner argues Jones’ Figure 9 shows that its system “allows for user input through a graphical user interface GUI” (Pet. 39), which discloses at least the limitation 1[f] feature of “in response to receiving one or more user inputs.” Patent Owner also faults Petitioner’s reliance on Figure 9 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.” Prelim. Resp. 15–16, n.10. 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) thereof, 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. As such, Petitioner argues Jones' Figure 9 and supporting description discloses the limitation 1[f] feature of a "component group compris[ing] a predefined interrelated group of two or more of the threat model components." Pet. 36. Based on the record before us, we find Petitioner's arguments persuasive.

Patent Owner further argues Petitioner "overlooks that claim 1 is a method claim," and "identifies no way in which Jones allegedly discloses the claimed method step of [limitation 1[f]]." Prelim. Resp. 17. That is the full extent of Patent Owner's conclusory attorney argument here. *See In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974) ("Attorney's argument in a brief cannot take the place of evidence."). We find this argument unavailing for the reasons outlined above concerning limitation 1[f] and independent claim 1 as a whole.

Accordingly, on the current record and for purposes of institution, Petitioner sufficiently shows that Jones discloses limitation 1[f], namely, "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,” as recited in independent claim 1.

(2) Undisputed Limitations at This Stage of the Proceeding

For the reasons stated in the Petition at pages 20–35, Petitioner sufficiently establishes for purposes of institution that Jones discloses the further limitations of independent claim 1. Patent Owner does not contend otherwise at this stage of the proceeding.

(3) Conclusion

At this stage of the proceeding and based on the record before us, we are persuaded that the cited evidence adequately supports Petitioner’s contention that independent claim 1 is unpatentable as anticipated by Jones.

b) Dependent Claim 3

Petitioner contends dependent claim 3 is unpatentable as anticipated by Jones. Pet. 40–41. The Petition provides a detailed assessment of this claim, with references to the Petition’s analysis of claim 1, disclosures in Jones, and the declaration testimony of Mr. Hurlbut. Pet. 40–41. At this stage of the proceeding, Patent Owner does not present any separate arguments that are distinct to this claim. Rather, Patent Owner generally is of the view its alleged deficiencies in the Petition with respect to claim 1 are also applicable to dependent claim 3. *See, e.g.*, Prelim. Resp. 17.

As discussed above, on the present record and at this stage of the proceeding, we are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that independent claim 1 is unpatentable as anticipated by Jones. For the reasons set forth in the Petition (Pet. 40–41),

we also are persuaded that the current record sufficiently supports Petitioner’s challenge to dependent claim 3 for purposes of institution.

c) Summary

For the foregoing reasons, and the reasons stated in the Petition (Pet. 20–41), we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1 and 3 are unpatentable as anticipated by Jones.

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

Petitioner contends claims 1–20 are 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. 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 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. Prelim. Resp. 17–20. Based on our review of the record before us, we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1–20 are unpatentable as obvious over the combination of Jones, Zheng, and Keenan, as discussed below. We turn first to an overview of Zheng and Keenan.

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.

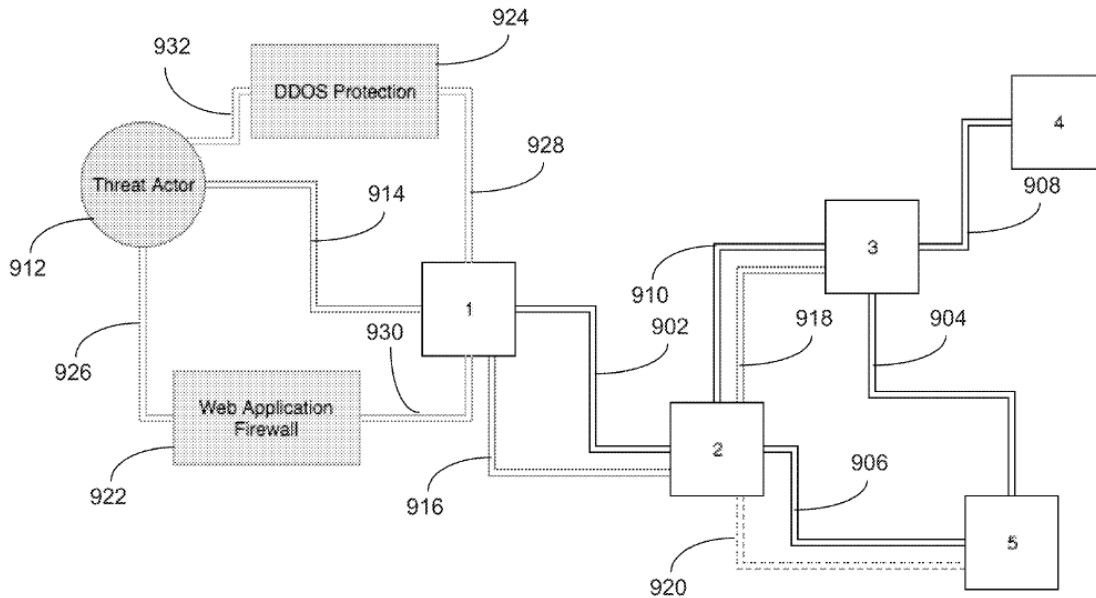


FIG. 8

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 (emphases added).

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

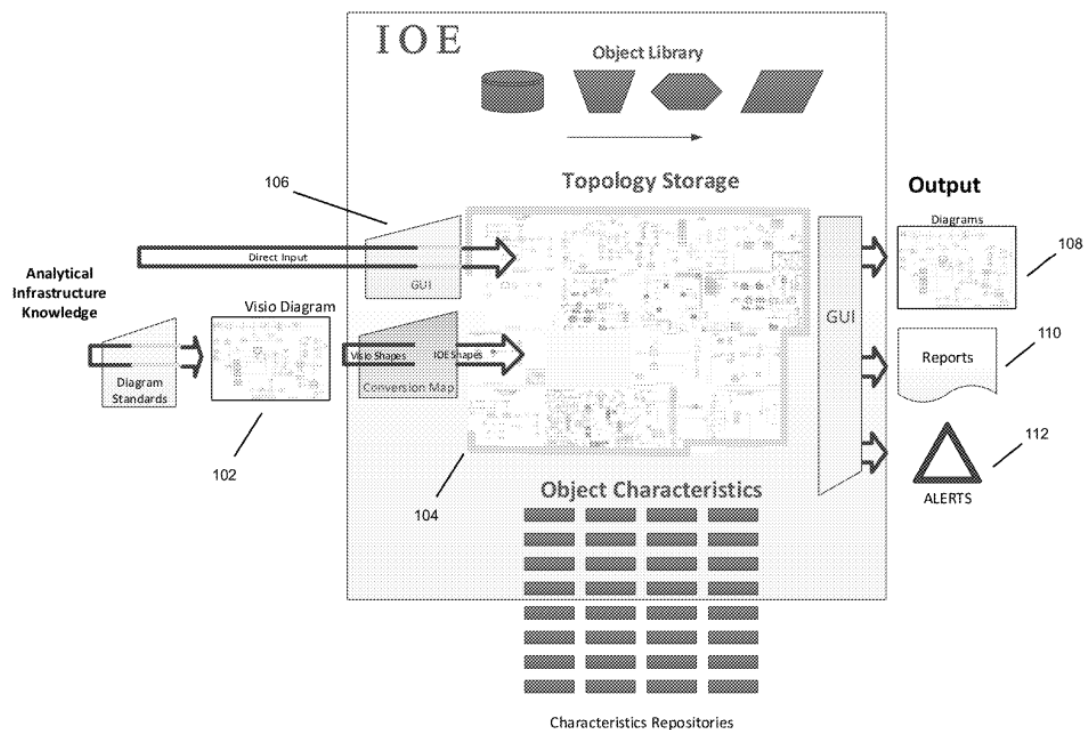


FIGURE 1

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 (emphases added), 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 (emphases added). 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; Prelim. Resp. 17–20.

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* Prelim. Resp. 17–20. Thus, we likewise turn to dependent claim 2 to consider the parties’ arguments concerning the foregoing limitations.

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, Petitioner argues “adding the visual features of

Zheng and Keenan . . . to the system of Jones would improve the overall user experience.” Pet. 56 (citing Ex. 1003 ¶ 120).

For example, Zheng’s disclosure of displaying attack paths would enhance the system of Jones by allowing the user to view attack paths in manner described in Zheng, which would enhance the user’s understanding of the potential threats. 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. [The 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).

Patent Owner responds that, although “Zheng can visualize ‘each security threat as a threat actor, a threat target and a displayable vector connecting the threat actor to the threat target,’” “Zheng does not disclose or suggest any scenario where ‘all threats’ associated with a selected threat model component are displayed.” Prelim. Resp. 19 (citing Ex. 1005, 2:36–42). Patent Owner adds, “Petitioner hides behind the disingenuous statement that ‘Zheng does not limit itself to identifying less than all threats,’” and argues “there is no indication in Zheng whether a displayable vector constitutes all threats to a component or whether there are other vectors that are not displayed, because Zheng discloses nothing about

displaying ‘all threats’ associated with a component.” *Id.* We find Patent Owner’s arguments unavailing.

Given (1) Zheng explicitly 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 (emphasis added)); (2) Petitioner’s expert, Mr. Hurlbut, testifies that the skilled artisan “would understand that Zheng’s system may show attack paths of ‘all’ threats” (Ex. 1003 ¶ 87); (3) “all” threats includes even a “single” threat, where only one threat exists; (4) Zheng does not disparage or otherwise teach away from displaying attack paths of “all” threats; and (5) Patent Owner disputes Mr. Hurlbut’s testimony here with attorney argument (*see In re Pearson*, 494 F.2d at 1405 (“Attorney’s argument in a brief cannot take the place of evidence.”)), we find Petitioner’s position persuasive, namely, that Zheng (or more specifically, the combination of Jones, Zheng, and Keenan) teaches *or at least fairly suggests* to the skilled artisan the limitation of visually displaying attack paths of “all” threats. *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.”). Indeed, we preliminarily find it incredible (i.e., not credible) that the ordinarily skilled artisan at the relevant time would have considered it desirable (or feasible) to visually display attack paths of only “some” threats but not “all” threats.

Patent Owner also responds that “Zheng does not disclose any component selection as causing the displayable vector to be displayed,” and so “Zheng fails to disclose at least a diagram interface visually displaying attack paths of all threats associated with the selected threat model

component upon receiving a user selection of the threat model component.” Prelim. Resp. 19; *see id.* (“Zheng does not disclose how to activate the visual display of any displayable vector, much less displaying the attack paths of all threats associated with a selected component upon receiving a user selection of the component.”). But as we understand Petitioner’s *obviousness* argument, Petitioner also contends Zheng and Keenan both teach visual features and user selection features that “would improve the overall user experience” with Jones. *See* Pet. 56 (cited at Pet. 42); *see id.* at § X.C.19.

For example, Petitioner argues “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.” Pet. 56. In this regard, 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). Petitioner also argues “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.” Pet. 56. In this regard, 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).

Based on the record before us, and at this stage of the proceeding, we find Petitioner's position persuasive, namely, that the combination of Jones, Zheng, and Keenan teaches *or at least fairly suggests* to the skilled artisan the limitation of visually displaying attack paths “in response to receiving a user selection of one of the diagrammed threat model components of the first threat model.” *See In re Keller*, 642 F.2d at 425 (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, 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.*).

Further, to the extent that Patent Owner attempts to controvert obviousness by identifying deficiencies in the disclosure of individual references (*see, e.g.,* Prelim. Resp. 19), we are not persuaded. *See In re Keller*, 642 F.2d at 426 (One cannot show nonobviousness by attacking references individually where invalidity is based on the teachings of a combination of references.); *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

At this stage of the proceeding and based on the record before us, we are persuaded that Petitioner’s cited evidence provides sufficient rational reasons for purposes of institution to combine Jones, Zheng, and Keenan with a reasonable expectation of success, and sufficiently supports Petitioner’s contention that dependent claim 2 is unpatentable as obvious over the combination of Jones, Zheng, and Keenan.

b) Independent Claims 4 and 12 and Dependent Claims 5–11 and 13–20

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). At this stage of the proceeding, Patent Owner argues independent claims 4 and 12 and dependent claim 2 as a group. *See, e.g.,* Prelim. Resp. 20 (“[I]ndependent claims 4 and 12 recite substantially similar features as claim 2 For the same reasons that Zheng fails to disclose or suggest the features of claim 2, Zheng also fails to disclose or suggest Element 4[e] and Element 12[e].”); *see generally id.* We agree with the parties that independent claims 4 and 12 recite limitations commensurate in scope with dependent claim 2. Thus, on the present record, and at this stage of the proceeding, we are persuaded that the cited evidence adequately supports Petitioner’s contentions that independent claims 4 and 12 are unpatentable as obvious over the combination of Jones, Zheng, and Keenan, for similar reasons as discussed above regarding dependent claim 2 (and independent claim 1). *See* Ex. 1003 ¶¶ 89–94, 104–108.

Petitioner contends dependent claims 5–11 and 13–20 are obvious over the combination of Jones, Zheng, and Keenan. Pet. 44–48, 50–57. The Petition provides a detailed assessment of these claims, with references to the Petition’s analysis of independent claims 1, 4, and 12 and dependent claim 2, disclosures in Jones, Zheng, and Keenan, and the declaration testimony of Mr. Hurlbut. Pet. 44–48, 50–57. At this stage of the proceeding, Patent Owner does not present any separate arguments that are distinct to these claims. Rather, Patent Owner generally is of the view its alleged deficiencies in the Petition with respect to independent claim 1 and dependent claim 2 are also applicable to dependent claims 5–11 and 13–20. *See, e.g.*, Prelim. Resp. 20. As discussed above, on the present record and at this stage of the proceeding, we are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that independent claims 1, 4, and 12 and dependent claim 2 are unpatentable as obvious over the combination of Jones, Zheng, and Keenan. For the reasons set forth in the Petition (Pet. 44–48, 50–57), we also are persuaded that the current record sufficiently supports Petitioner’s challenge to dependent claims 5–11 and 13–20 for purposes of institution.

c) Summary

For the foregoing reasons, and the reasons stated in the Petition (Pet. 41–57), we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1–20 are unpatentable as obvious over the combination of Jones, Zheng, and Keenan.

F. Alleged 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 additionally contends (1) claims 1–20 are 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 are 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 are 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”)). At this stage of the proceeding, Patent Owner does not present any separate arguments that are distinct to these challenges and claims. *See* Prelim. Resp. 20–21 (Ground 3), 21–23 (Ground 4), 23 (Ground 5). Because we determine that Petitioner demonstrates a reasonable likelihood of success in establishing that (1) claims 1 and 3 are unpatentable under 35 U.S.C. § 102 as anticipated by Jones (*see supra* § III.D), and (2) claims 1–20 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Jones, Zheng, and Keenan (*see supra* § III.E), such that we institute this proceeding, and because we must therefore institute *inter partes* review on all claims and all challenges in the Petition (*see* 37 C.F.R. § 42.108(a)), for purposes of institution, we need not and do not herein address in detail Petitioner’s foregoing challenges to the noted claims. However, we do provide below certain guidance on these challenges to assist the parties in the upcoming trial.

We have reviewed Petitioner’s additional contentions (1) through (3) above (*see* Pet. 57–63), and based on the record before us, preliminarily find each of them persuasive. The Petition provides a detailed assessment of the challenged claims, with references to disclosures in Jones, Zheng, Keenan, Yu, and Reith (and discussion of the skilled artisan’s knowledge) and the declaration testimony of Petitioner’s expert, Mr. Hurlbut. Pet. 13–19, 57–63. At this stage of the proceeding and based on the record before us, we preliminarily are persuaded that the cited evidence sufficiently supports Petitioner’s contentions (1) through (3) for purposes of institution.

IV. CONCLUSION

Based on the evidence before us, we determine that Petitioner has established a reasonable likelihood that at least one claim of the ’008 patent is unpatentable. Accordingly, we institute trial on all the challenges in the Petition.

We base our factual findings and conclusions at this stage of the proceeding on the evidentiary record developed so far. This is not a final decision as to the construction of any claim term or the patentability of any claim. Any final decision shall be based on the full trial record, including any response timely filed by Patent Owner. Any arguments not raised by Patent Owner in a timely filed response may be deemed waived, even if they were presented in the Preliminary Response.

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–20 of the ’008 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '008 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2023-00821
Patent 10,699,008 B2

FOR PETITIONER:

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

FOR PATENT OWNER:

Wayne M. Helge
NOSSAMAN LLP
whelge@nossaman.com

Christopher H. Blaszkowski
RATNERPRESTIA
cblaszkowski@ratnerprestia.com