UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE INC.,
Patent Owner.

---

IPR2023-00656
Patent 10,713,366 B2

---

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

BELISLE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No 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. 10,713,366 B2 (Ex. 1001, “the ’366 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 ’366 patent on all grounds of unpatentability alleged in the Petition. Paper 7 (“Institution Decision” or “Dec.”).

After institution, Patent Owner filed a Response. Paper 19 (“PO Resp.”). Petitioner filed a Reply. Paper 24 (“Pet. Reply”). Patent Owner filed a Sur-reply. Paper 25 (“PO Sur-reply”). We held an oral hearing in this case on July 10, 2024, and a transcript of the hearing is included in the record. Paper 32 (“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, and constrained by the record before us, we determine Petitioner has not established by a preponderance of the evidence that any of claims 1–20 of the ’366 patent is unpatentable.

## II. BACKGROUND

### *A. Related Matters*

At the time of the Petition's filing, the parties indicated that the '366 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. 2; Paper 4, 2.

Petitioner also indicated that Patent Owner asserts related U.S. Patent No. 10,699,008 B2 against Petitioner in the District Court Case. Pet. 2. The '008 patent is the challenged patent in IPR2023-00821 now pending before the Board.

### *B. The '366 Patent*

The '366 patent is titled "Systems and Methods For Automated Threat Model Generation From Third Party Diagram Files," and issued July 14, 2020, from U.S. Patent Application No. 16/542,263, filed August 15, 2019, and claims priority through a series of continuations-in-part to four U.S. Provisional Patent Applications filed in 2017. Ex. 1001, codes (10), (21), (22), (45), (54), (63).

The '366 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, 1:51–62.

> Threat modeling systems include one or more computing devices communicatively coupled with one or more databases, the database(s) including threat model components and threats associated with one another. One or more mapping files coupled with the database(s) correlate the threat model components with visual diagram components of a third party software application.

> An import interface initiates reading of a third party generated data file by the computing device(s), the data file including a subset of the third party diagram components and relationships between the subset. An interface receiving input initiates a determination of threat model components correlated with the subset. A diagram interface displays a relational diagram using visual representations of threat model components correlated with the subset, the relational diagram defining a threat model. A threat report interface includes a threat report displaying each threat that is associated with one of the threat model components of the threat model.

*Id.* at code (57). According to the '366 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 8:67–9:5.

For example, in the context of computer networks, one threat may be "bluejacking" and one component, which would be correlated to this threat through the database, could be a "BLUETOOTH port." Ex. 1001, 9:55–59. In this scenario, if a user includes a BLUETOOTH port in a diagram of a computing system, the subject threat modeling system would identify that port as a relevant source for bluejacking in an associated threat model and threat report. *Id.* at 9:60–63. In this example, the component is a physical component of a computing device or system/network. *Id.* at 9:63–65. As another example, in the context of commuting to work safely, one threat may be a "freeway collision" and one component, which would be correlated to this threat through the database, could be "merging onto freeway." *Id.* at 9:66–10:3. In this scenario, "merging onto freeway" would be a relevant source for the threat of "freeway collision." *Id.* at 10:4–5.

In this latter example, the component (and relevant source) is defined as an action or step, and not as a physical component. *Id.* at 10:5–7.

### *C. Illustrative Claim*

The '366 patent includes twenty claims, all of which are challenged. Claims 1, 8, and 16 are the independent claims. Claim 1 is illustrative and reproduced below with labels, such as "[a]," added to limitations in the same manner as used by the parties.

> 1. [p] A threat modeling method, comprising:
>
> [a] providing one or more databases, the one or more databases comprising:
>
> [b] a plurality of threat model components stored therein; and
>
> a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases;
>
> [c] providing one or more mapping files communicatively coupled with the one or more databases, [d] the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter "third party diagram components"); and
>
> [e] in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:
>
> [f] using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;
>
> [g] determining using the one or more computing devices, for the subset of third party diagram components,

> correlated threat model components as defined in the one or more mapping files;
>
> [h] displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and
>
> [i] generating, using the one or more computing devices, and displaying, on the one or more user interfaces, a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.

Ex. 1001, 43:21–61.

### *D. Evidence of Record*

Petitioner relies on the following patent and published patent application evidence.

| Name | Patent Document | Exhibit |
|---|---|---|
| Keenan | US 11,200,228 B2, issued Dec. 14, 2021 | 1004 |
| Zheng | US 10,503,907 B2, issued Dec. 10, 2019 | 1005 |
| Baker | US 2014/0236665 A1, published Aug. 21, 2014 | 1006 |
| Jones | US 9,602,529 B2, issued Mar. 21, 2017 | 1007 |
| Galliano | US 10,681,068 B1, issued June 9, 2020 | 1008 |

Pet. 10–12, 14–21.

Petitioner also relies upon two Declarations of Robert Hurlbut (Exs. 1003, 1016).

Patent Owner relies upon two Declarations of Seth James Nielson, Ph.D. (Exs. 2009, 2010).

### *E. Asserted Challenges to Patentability*

We instituted *inter partes* review of claims 1–20 of the ’366 patent on the following grounds asserted by Petitioner. Dec. 2–3, 32; Pet. 11–12.

| Claims Challenged | 35 U.S.C. § | Reference(s)/Basis |
|---|---|---|
| 1–20 | 102[1] | Keenan |
| 1–4, 7–11, 15–18 | 103 | Zheng, Baker, Jones |
| 2, 9, 17 | 103 | Zheng, Baker, Jones, Galliano |
| 1–20 | 103 | Zheng, Baker, Jones, Keenan |
| 2, 5, 6, 9, 12–14, 17, 19, 20 | 103 | Zheng, Baker, Jones[2] |

## III. PATENTABILITY

### *A. Applicable Law*

Petitioner challenges the patentability of claims 1–20 of the ’366 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 Keenan, Zheng, Baker, Jones, and Galliano. “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.

[1] 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 ’366 patent is after March 16, 2013, the effective date of the relevant amendment, the AIA versions of §§ 102 and 103 apply.

[2] Petitioner’s obviousness challenge to the listed claims is based on the listed references (Zheng, Baker, Jones) “in further view of the knowledge of a POSITA,” where “POSITA” means a person of ordinary skill in the art. Pet. 12; *see also Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013) (providing that it is appropriate to consider such knowledge as part of an obviousness analysis).

§ 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).

To serve as an anticipatory reference under 35 U.S.C. § 102, "the reference must disclose each and every element of the claimed 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."[3] *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 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 grounds 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 '366 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. 12 (citing Ex. 1003 ¶ 33).

Patent Owner does not present an alternative definition in this proceeding. *See generally* PO 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;

[3] Patent Owner does not present objective evidence of non-obviousness.

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 may be 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 '366 patent, the background technical field, the prior art, and Petitioner's 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 (1) "threats," (2) "threat model components," (3) "visual representations of the threat model components," and (4) "mapping files." Dec. 12. The parties dispute the meanings of two of these claim limitations, namely, (1) "threats" and (4) "mapping files." PO Resp. 17–25, 28–29; Pet. Reply 3–7; PO Sur-reply 2–5. The parties otherwise do not contend that claim construction is necessary to resolve the controversy in this case. *See* PO Resp. 25–27; Pet. 12–14. To the extent necessary to resolve the controversy before us, we address claim interpretation in our patentability analysis below.

*D. Alleged Anticipation of Claims 1–20 by Keenan*

Petitioner contends claims 1–20 are unpatentable under 35 U.S.C. § 102 as anticipated by Keenan (Ex. 1004). Pet. 8, 14–17, 21–60; Pet. Reply 7–20. Patent Owner opposes Petitioner's contentions. PO Resp. 3–4, 29–49; PO Sur-reply 5–20. For the reasons expressed below, and based on the complete record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that any of claims 1–20 is unpatentable as anticipated by Keenan. We turn first to an overview of Keenan.

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

Keenan generally is directed to "an Integrated Object Environment (IOE) running in a graph database environment." Ex. 1004, 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. 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.

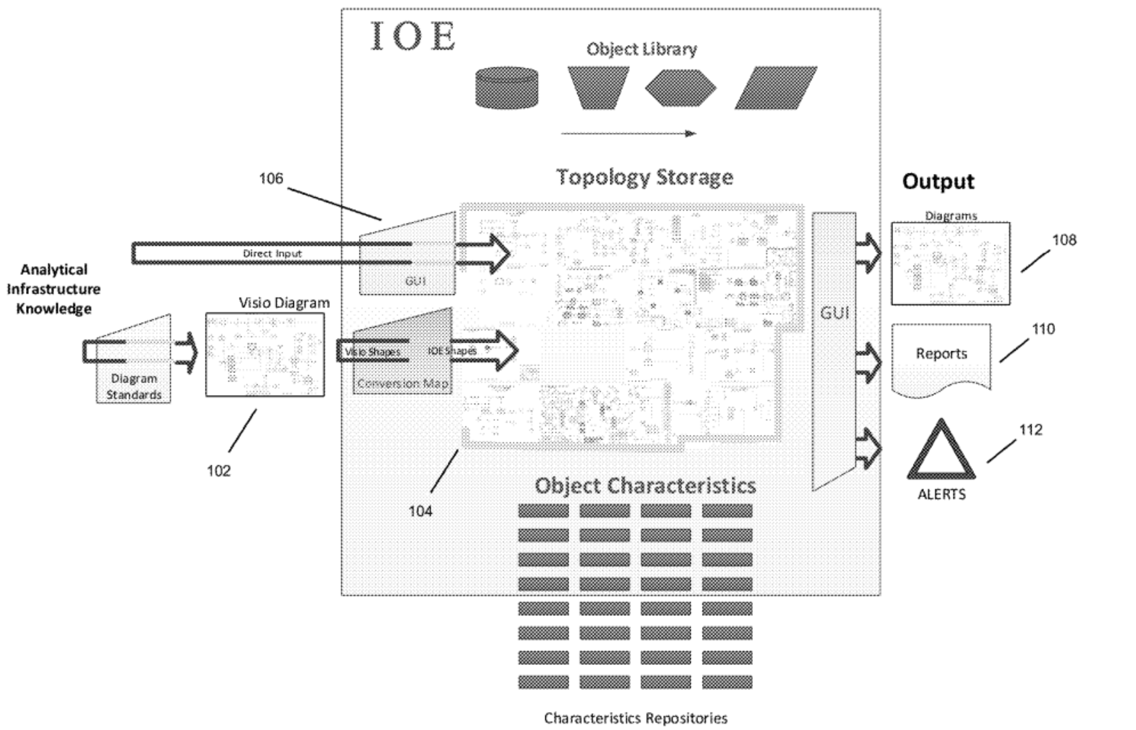


**FIGURE 1**

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

Ex. 1004, 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. 1004, 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.

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

#### 2. *Prior Art Status of Keenan*

The parties dispute the prior art status of Keenan (U.S. Patent No. 11,200,228 B2), which was filed April 19, 2018 (*after* the earliest possible effective filing date of the '366 Patent) and claims priority to U.S. Provisional Application No. 62/487,370, filed April 19, 2017 ("Keenan

Provisional") (*before* the earliest possible effective filing date of the '366 Patent). Ex. 1001, codes (10), (22), (60); Ex. 1004, codes (22), (60).

Patent Owner contends that, "[f]or Keenan to be considered as prior art with respect to the '228 patent, Petitioner must demonstrate that the alleged disclosure relied on by Petitioner was present in the Keenan Provisional," and "Petitioner has made no such showing (or even an allegation thereof)." PO Resp. 47–48. Petitioner replies that Patent Owner "is wrong for two reasons," namely (1) "Keenan's non-provisional is supported by [the Keenan Provisional]"; and (2) "the '366 patent is a CIP [i.e., continuation-in-part application] and is only entitled to a priority date as of its filing date of August 15, 2019—which is after Keenan's non-provisional filing date." Pet. Reply 8; *see id.* at 7–12. Patent Owner responds (1) "Petitioner improperly waited until its Reply to make an essential element of its anticipation contention – namely, that Keenan is prior art" (PO Sur-reply 5–8); and (2) prior to its Reply, "Patent Owner never argued that the '366 Patent was entitled to a different priority date other than the May 17, 2017, date relied upon in the Petition" (*id.* at 8–9).

Because we determine below in Section III.D.3 that Petitioner has not sufficiently shown that Keenan provides an anticipatory disclosure of any of the Challenged Claims, we need not and do not address herein whether Keenan's disclosures are sufficiently supported by the Keenan Provisional or whether the Challenged Claims are entitled to the benefit of any of the '366 patent's underlying provisional application filing dates.

### *3. Analysis*

#### *a) Independent Claim 1*

The parties dispute, *inter alia*, whether Petitioner has proven that Keenan explicitly or inherently discloses to the skilled artisan limitation 1[b], namely, "a plurality of *threat model components* stored [in one or more databases]; and a plurality of *threats* stored therein, wherein each of the threats *is associated with* at least one of the threat model components through the one or more databases." Pet. 25–28; PO Resp. 29–41; Pet. Reply 12–18; PO Sur-reply 9–16; Ex. 1001, 43:24–29 (emphases added).

In our Institution Decision, we preliminarily found that on the record at that time and, "for purposes of institution, Petitioner sufficiently show[ed] that Keenan discloses limitation 1[b]." Dec. 16–19. However, on further review of the Petition and further consideration of the parties' briefing on this issue and the relevant case law, and based on the complete record before us, we now conclude otherwise. *Cf. Fanduel, Inc. v. Interactive Games LLC*, 966 F.3d 1334, 1340 (Fed. Cir. 2020) ("There is nothing inherently inconsistent about the Board instituting IPR on obviousness grounds and then ultimately finding that the petitioner did not provide preponderant evidence that the challenged claim was obvious."); *see In re Magnum Oil Tools*, 829 F.3d at 1376 ("[T]he decision to institute and the final written decision are 'two very different analyses,' and each applies a 'qualitatively different standard.'" (quoting *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016))). In particular, we determine that Petitioner has not proven, by a preponderance of the evidence, that Keenan provides an anticipatory disclosure of limitation 1[b], as discussed below. We turn first to the meaning of "threat."

*(1) What is a "Threat"?*

Patent Owner proffers that "threat" is "a term of art within the field of threat modeling," and in the context of the '366 patent, should be construed to mean "one or more potential events that, if they occur, can cause adverse effects to a target system." PO Resp. 18 (citing Ex. 2009 ¶ 78). Patent Owner emphasizes that "threats" and "risks" are "distinct concepts," where "'risk' is the potential impact on a system *due to a threat* that occurs coupled with the likelihood that a threat will occur." *Id.* at 19 (emphasis added). Patent Owner relies upon both intrinsic evidence (Specification, prosecution history) and extrinsic evidence (expert testimony, publications) to support its proposed construction. *See id.* at 18–25; PO Sur-reply 2–3.

Petitioner proffers that "threat" should be construed to mean an "undesirable event that may happen." Pet. Reply 3. Petitioner argues, *inter alia*, (1) "there is no meaningful difference between an 'undesirable event' and 'potential events that … can cause adverse effects to a target system'"; (2) "[Patent Owner's] definition is slightly incorrect because the words 'if they occur' remove all consideration of whether the event is likely to occur, leading to the absurdity that an event that is impossible can still be considered a 'threat' because the words 'if they occur' requires one to ignore that impossibility"; and (3) "[t]his aspect of [Patent Owner's] construction is directly contrary to the testimony of [Patent Owner's] expert, Dr. Nielson, and the specification of the '366 patent." *Id.* at 3. Despite these protestations, Petitioner does not meaningfully address Patent Owner's cited intrinsic and extrinsic evidence. *See id.* at 3–5.

Patent Owner responds that Petitioner is construing "threat" in a vacuum, because "Petitioner's construction is not tied to threat modeling or threat models." PO Sur-reply 2. Patent Owner explains that its proposed construction "specifies that threats, when realized, 'can cause adverse effects to a target system,'" and that "[t]he phrase in [its] construction that reads 'if they occur, can cause adverse effects to a target system' merely recognizes that the 'potential event' cannot cause adverse effects to a target system unless it occurs." *Id.* Patent Owner argues that the Specification supports this construction by disclosing, *inter alia*, that "threats" are stored in a data store and a threat model pulls only "relevant" threats from that data store, thus plainly showing that "not every threat is necessarily included in [a given] threat model." *Id.* at 2–3, Fig. 2. We find Petitioner's arguments unpersuasive, and find Patent Owner's proposed construction of the subject limitation to be sufficiently supported on the complete record before us.

*(a) Claims*

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, databases storing threat model components and threats associated with those threat model components, where the threat model components are correlated to third-party diagram components, and generating a threat report for a threat model comprising only a "subset" of the third-party diagram components. *See* Ex. 1001, 43:21–61. Contrary to Petitioner's arguments (Pet. Reply 3–5), this "subset" feature shows that the "threats" stored in databases in claim 1 represent "potential events" that may or may not occur depending on the composition of a given system undergoing threat modeling—a system may implicate all stored threats, some of them, or even just one of them, leaving the remaining stored threats for use in preparing threat models for other systems. *See* PO Sur-reply 2–3 (discussing Figure 2 and arguing that "not every threat is necessarily included in the threat model"). We find the claim language itself supports interpreting "threats" as "potential events that, if they occur, can cause adverse effects to a target system."

*(b) Specification*

We next turn to disclosures in the Specification relevant to the subject limitation. *See E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003) (Claims must be interpreted "'in view of the specification' without unnecessarily importing limitations from the specification into the claims." (citing *Texas Digital Sys., Inc. v. Telegenix, Inc.*, 308 F.3d 1193, 1203–1204 (Fed. Cir. 2002))).

The Specification explicitly discloses, in discussing process 200 as depicted in Figure 2, selecting "relevant" sources (components) and their associated "relevant" threats from a data store of components and threats. *See, e.g.*, Ex. 1001, 9:17–54; *see id.* at 9:31–32 ("The threat model thus includes relevant threats and the relevant sources of those threats.").
We find the Specification also supports interpreting "threats" as "potential events that, if they occur, can cause adverse effects to a target system," because the Specification plainly contemplates storing a pool of "threats"

and selecting and preparing threat models using only "threats" relevant to a given system under examination.

*(c) Prosecution History*

During prosecution of the Challenged Claims, the applicant (Patent Owner) submitted an article titled, "Threat Modeling Approaches for Securing Cloud Computing." Ex. 1002, 480–495; Ex. 1001, code (56). As noted by Patent Owner (PO Resp. 21), this article includes definitions of both "threat" and "risk." "Threat" is defined as "harm or unauthorized access that *might* occur due to vulnerability and destroy organization assets, organization operations or system information." Ex. 1002, 482 (emphasis added). The article cites to the Open Web Application Security Project ("OWASP"), which according to the article, defines "risk" as "Risk = Likelihood x Impact" (Ex. 1002, 493), where "'likelihood' is the probability that a threat may occur, and 'impact' is the damage that may occur to a system or organization if the threat occurs" (Ex. 2009 ¶ 83). We find this contemporaneous article, submitted during prosecution, at least supports interpreting "threats" as "potential events that, if they occur, can cause adverse effects to a target system."

We find that the intrinsic evidence compels a more tailored definition of "threat" than that proffered by Petitioner (an "undesirable event that may happen"), namely one that contemplates adverse effects to a target system rather than mere "undesirability," and recognizes that not every "threat" stored in a database is necessarily included in a given threat model.

Based on the intrinsic evidence before us, we agree with Patent Owner's proposed definition of "threat" and construe "threat" to mean "one or more potential events that, if they occur, can cause adverse effects to a target system." We also have considered Patent Owner's extrinsic evidence concerning the meaning of "threat" (*see* PO Resp. 21–25), and agree that such evidence further supports our interpretation of "threat." For example, the Draft National Institute of Standards and Technology ("NIST") Special Publication 800-154, Guide to Data-Centric System Threat Modeling ("NIST 800-154") (Ex. 2004), which is "a well-accepted and widely-consulted standard in the field of threat modeling" according to Patent Owner's expert (Ex. 2009 ¶ 84), references NIST Special Publication 800-30 ("NIST 800-30") which defines "threat" as:

> Any circumstance or *event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets,* individuals, other organizations, or the Nation through an information system *via unauthorized access, destruction,* disclosure, or modification of information, and/or denial of service.

Ex. 2006, 63 (NIST 800-30) (quoted at PO Resp. 21–22) (emphasis added); Ex. 2004, 11 ("A *threat* is defined in [NIST 800-30]."), 25; Ex. 2009 ¶ 84.

*(d) "Threats" versus "Risks"*

To be clear, our construction of "threat" to mean "one or more potential events that, if they occur, can cause adverse effects to a target system" does not encompass "risk," which at least in the context of the Challenged Claims and the '366 patent are distinct from each other. For example, as argued by Patent Owner (PO Resp. 19), Figure 8 of the '366 patent plainly depicts "threats" and "risk" as distinct concepts. Patent Owner's expert, Dr. Nielson, agrees and testifies persuasively in this regard:

> A "threat" is a potential event. Whereas "risk" is the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur. The terms "risk" and "risk level" are used synonymously in the '366 Patent, as they are

> typically used in the threat modeling field. In Figure 8, the "risk" for the various threats are categorized as medium, high, or very high. There is not necessarily a one-to-one correspondence between "threats" and "risk." Indeed, the same threat can have different risk levels depending on the system in which the threat may occur. Similarly, knowing the risk level does not identify a particular threat. In Figure 8, a "very high" risk could correspond to any one of six different threats. EX-1001, Fig. 8.

Ex. 2009 ¶ 80 (cited at PO Resp. 19); Ex. 1001, Fig. 8.

NIST 800-30, discussed above, also defines "risk" as distinct from "threat," specifically defining "risk" as:

> A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Ex. 2006, 59. Referring to the definitions of "threat" and "risk" in NIST 800-30, Patent Owner's expert, Dr. Nielson, testifies persuasively:

> [A] "threat" is the "circumstance or event." The "risk" is the "measure of the extent to which an entity is threatened" by the threat. "Risk" is a function of the impact of the potential threat (if it were to occur), and the likelihood that the threat may occur.

Ex. 2009 ¶ 84 (cited at PO Resp. 22).

Further, the parties' experts do not disagree on this distinction, and particularly, that "risk" is not a "threat," but rather represents the *likelihood* of a threat occurring compounded by the *impact* of such a threat on a given system. *See* Ex. 2002, 24:3–25:5 (Petitioner's expert, Mr. Hurlbut, testifying, "Risk is a – essentially a product or in general relation to threat modeling is a product of probability, the possibility, probability of a threat being realized as well as the impact of that threat."), 31:5–33:2 (Mr. Hurlbut agreeing that "Risk = Likelihood x Impact"); Ex. 2009 ¶ 80 (Patent Owner's expert, Dr. Nielson, testifying, "'risk' is the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur.").

*(e) Construction*

Based on the complete record before us, we determine that "threat" means "one or more potential events that, if they occur, can cause adverse effects to a target system," and that this definition does not encompass "risk" within its scope.

*(2) Limitation 1[b]: "a plurality of threat model components stored [in one or more databases]; and a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases"*

*(a) No Inherency Argument*

Before turning to the parties' arguments concerning limitation 1[b], we note that Petitioner's anticipation challenge here is based only on the express disclosure of Keenan, and not on any inherent disclosure. *See* Tr. 27:10–15 ("[Judge]: So, to be clear, Petitioner is not making an inherent anticipation argument in this case . . . with respect to Keenan? [Petitioner's Counsel]: Yes, Your Honor. *Petitioner did not argue inherency in the petition.*" (emphasis added)), 26:23–27:9; *see generally* Pet. Thus, we need not and do not consider whether Keenan provides any inherent disclosure relevant to limitation 1[b] or other aspects of claim 1. *See SAS Inst., Inc. v. Iancu*, 584 U.S. 357, 363–364 (2018) ("[I]n an inter partes review the petitioner is master of its complaint," and "the statute envisions that a petitioner will seek an inter partes review of a particular kind—one guided by a petition describing 'each claim challenged' and 'the grounds on which the challenge to each claim is based.'"'; *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1330 (Fed. Cir. 2019) ("Because of the expedited nature of IPR proceedings, [i]t is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify 'with particularity' the 'evidence that supports the grounds for the challenge to each claim.'" (internal quotation marks altered)).

*(b) The Petition*

Petitioner argues Keenan discloses limitation 1[b] by describing an Integrated Object Environment (IOE) that represents "'a dynamic map of an enterprise's analytic infrastructure, preferably including ***all physical assets*** that contribute to . . . analysis.'" Pet. 26 (quoting Ex. 1004, 5:27–44); *see* Ex. 1003 ¶ 81. Petitioner argues:

> Each asset or "real world component," *i.e.*, physical asset, is defined by an object within the IOE and is associated with risk and characteristics (*e.g.*, risk characteristics and the relationship to other objects). [Ex. 1004, 5:27–44.] The IOE allows a user to select views that display the associated risk and consequences for specific assets using threat vectors and models. *Id.*, 4:64–67, 16:1–29; *see also* 1:31–52, 7:41–59, 13:4–22, 14:35–39, 14:61–63, 16:40–63, 17:32–40, 18:6–22, 20:34–51, Figs. 1, 7. Keenan further explains that certain Views use color to "represent different types of risk (e.g., cyber, environmental, accidental, etc.)." *Id.*, 16:40–51.

Pet. 26 (citing Ex. 1003 ¶¶ 81–83).

Petitioner argues that, although Keenan may not use the identical terminology as the '366 patent, Keenan nevertheless explicitly discloses limitation 1[b] *to the skilled artisan*. Pet. 28. In particular, Petitioner argues the skilled artisan would understand Keenan to disclose the following:

(1) "the assets/objects in Keenan are 'relevant sources of threats' and thus threat model components, as defined by the '366 patent, because the assets/objects in Keenan are subject to risks that Keenan's system measures" (Pet. 28 (citing Ex. 1003 ¶ 82));

(2) "Keenan's 'risk' includes threats because measuring risk includes a determination of threats, and Keenan discloses that Views may use color to 'represent different types of risk (e.g., cyber, environmental, accidental, etc.)'" (*id.* (citing Ex. 1004, 16:40–51; Ex. 1003 ¶ 82)), where "'types of risk' are threats because the described examples are threats (cyber/environmental/accidental)" (*id.*; *see* Ex. 1003 ¶ 79 (emphasis added));

(3) "'each of the threats is associated with at least one of the threat model components' because Keenan discloses associating risk with each asset" (Pet 28 (citing, *inter alia*, Ex. 1004, 1:33–38, 1:47–52; Ex. 1003 ¶ 82)); and

(4) "Keenan's threats and threat model components are 'stored therein' in the database, and that the threats and threat model components are associated 'through the one or more databases' because Keenan discloses a method and system that is run in a 'graph database environment'" (*id.* (citing Ex. 1003 ¶ 83)).

#### *(c) Patent Owner's Response*

Patent Owner responds that "Keenan does not disclose threats at all," because "Keenan is directed to viewing and analyzing risk," and "[i]t is immaterial to Keenan's system whether a threat (or group of threats) gave rise to the risk," as "Keenan is focused on assessing the risk." PO Resp. 29–30 (citing Ex. 2009 ¶ 103). In particular, Patent Owner argues:

> Keenan also does not expressly or inherently determine a threat that may be associated with the risk. EX-2009, ¶104. As explained above, risk is a calculated value based on properties (likelihood of occurrence and impact) that may be associated with a threat. Thus, to the extent that one or more threats gave rise to a risk, the risk is a *downstream* product of properties associated with the one or more threats. As explained above, in the context of a threat, risk is equal to the likelihood of the threat occurring multiplied by the impact that the threat may have if it occurs. <u>Keenan starts with the risk and thus, has no need to determine or otherwise know what, if any, threat(s) gave rise to the risk</u>. EX-2009, ¶104.

PO Resp. 30 (underlining added); *see id.* at 35–36 ("Neither generally nor in the context of Keenan does risk 'include threats.' Risk might be based on a threat. But risk does not include a threat and determining risk does not require identifying or determining a threat." (citing Ex. 2009 ¶ 112)).

Patent Owner argues that, although Keenan uses the word "threat" two times, both in the context of a "technical threat vector," Keenan describes use of that "vector" only in a screen view in which "color fills the object shapes based on the value [of] the technical *risk ranking* characteristic of that object." PO Resp. 30–31 (quoting Ex. 1004, 14:61–63). According to Patent Owner, "'[r]isk ranking' refers to one of two things[:]"

> "Risk ranking" either means a risk value, such as a value between 0 and 100. Alternatively (and less likely), "risk ranking" refers to the amount of risk for a particular object relative to the amount of risk for other objects in the view. In either case, the "technical threat vector" is just a risk ranking and *has nothing to do with the identification or determination of a threat associated with the risk*. EX-2009, ¶105; *see* EX-2002 [Hurlbut depo], 77:5-11 ("technical risk ranking is actually equivalent to a risk level").

PO Resp. 31. Patent Owner submits that "the risk of a loss can be known without ever determining the threat or threats that may have contributed to the risk" (*id.* at 31–32 (citing Ex. 2009 ¶ 106)), and "knowing the risk to a system alone does not allow one to determine the threat that may have given rise to the risk (*id.* at 32 (citing Ex. 2009 ¶ 107). Patent Owner argues "[n]either Petitioner nor its expert provide any reasoned explanation allegedly why 'measuring risk includes a determination of threats.'" *Id.* at 34 (citing Ex. 2009 ¶ 109); *see id.* ("Not only does Keenan <u>not</u> disclose a determination of threats, Keenan certainly does <u>not</u> disclose storing a plurality of threats in a database." (citing Ex. 2009 ¶ 110)).

*(d) Petitioner's Reply*

Petitioner replies that, allegedly, "there is no dispute that a [skilled artisan] would understand that 'a ***risk analysis requires some form of threat analysis***,"[4] and "although threats and risk are different concepts, it is undisputed by the parties' experts that Keenan's risk analysis requires an underlying threat analysis." Pet. Reply 12 (citing Ex. 1015, 9:22–10:7). Petitioner argues, in various forms, "[the skilled artisan] would understand that Keenan calculates this risk by multiplying 'the potential impact on a system ***due to a threat*** that occurs' with 'the ***likelihood that a threat will occur***,'" and notes that "[a]n understanding of the 'threat' is on both sides of this equation—and thus an integral part of Keenan's risk analysis." Pet.

[4] Patent Owner persuasively argues that "[p]erhaps the most egregious example of an unsupported statement is the (partial) quote from Dr. Nielson repeated multiple times in the Reply which reads 'a risk analysis requires some form of threat analysis.'" PO Sur-reply 13. "[T]his statement is key to Petitioner's newly minted inherency argument because Petitioner needs evidence that to analyze risk, [the skilled artisan] must analyze (and thus determine [and store]) threats. This new theory should not be accepted by the Board." *Id.*

Reply 14 (citing Ex. 1015, 61:8–62:12; Ex. 2002, 24:3–25:5, 31:5–33:2). Petitioner adds that "Keenan further discloses that all parts of its analysis are stored in its system." *Id.*

Petitioner replies that "[a] close review of Keenan further confirms that Keenan discloses threats as part of its analysis":

> For example, Keenan discloses using color to categorize risk based on the type of risk (*i.e.*, cyber, environmental, accidental). EX-1004, 16:40-51; Petition, 28; EX-1003, ¶79. These "types of risk" stem from the underlying threat—*i.e.*, cyber threats, environmental threats, and accidental threats. In other words, as discussed above, "risk" does not exist in a vacuum, and therefore specific types of risk stem from specific types of threats. EX-1015, 101:21-133:4. Indeed, like Keenan, the '366 patent discloses organizing the composition of threats by the type of risk. EX-1001, 24:53-58 ("the composition of threats by risk type").

Pet. Reply 15. Petitioner argues "[Patent Owner] notably ignores that the use of color in Keenan is not merely identifying 'risk level'—it is identifying 'the ***generic nature of a risk***,' which identifies the nature of the threat, as discussed above," and "identifying 'types of risk' serves to also identify the underlying type of threat."[5] *Id.* at 15–16 (citing Ex. 1003 ¶¶ 79, 82). Petitioner argues Keenan's disclosure of "different types of risk (e.g., cyber, environmental, accidental, etc.)" discloses, at the least, generic threats or non-specific threats, and claim 1 does not require any level of specificity of such threats. *Id.* at 16–18; *see id.* ("Keenan discloses a model identifying

[5] Patent Owner persuasively argues that "this assertion assumes that knowing risk allows [the skilled artisan] to determine risk [sic: threats] which [Patent Owner] has shown to be wrong." PO Sur-reply 14.

a specific threat: European windstorms. And since the European windstorm is part of Keenan's analysis, this threat is stored in Keenan's system.").

Petitioner replies that "[y]et another way that Keenan discloses threats is Keenan's disclosure of mitigating resulting risk," because "[the skilled artisan] would understand that risks cannot be mitigated without mitigating the threat." Pet. Reply 18 (citing Ex. 1004, 20:22–33; Ex. 1015, 75:1–17). Petitioner adds "a still further way that Keenan discloses threats is through 'risk characteristics'— one of which is threats." *Id.* (citing, *inter alia*, Ex. 1003 ¶ 82).[6]

*(e) Patent Owner's Sur-Reply*

Patent Owner responds by returning to home base—the language of claim 1, particularly limitation 1[b]: "The claims do not merely require a 'determination' of threats or merely a disclosure of threats," rather, limitation 1[b] requires "a plurality of threats stored [in "one or more databases"], wherein each of the threats is associated with at least one of the threat model components through the one or more databases." PO Sur-reply 9 (citing Ex. 1001, 43:22–29, 44:24–33, 45:24–33); *id.* at 11 ("[D]etermining threats is not sufficient to anticipate the claims of the '366 Patent. The claims require a storing of threats in a database and an association of each threat with at least one threat model component through the database."). Patent Owner argues that Petitioner's premise that "risk"

[6] Patent Owner persuasively argues that "Petitioner's expert admitted in his deposition that knowing risk does not allow one to determine the threat that may have given rise to the risk." PO Sur-reply 9–10 (citing Ex. 2002, 61:7–24, 64:14–25, 66:2–9; Ex. 2009 ¶ 81).

includes "threats" or knowing risk allows for determination of threats is *false*:

> In the Petition, the lynchpin of Petitioner's argument was that "[the skilled artisan] would further understand that Keenan's 'risk' includes threats because measuring risk includes a determination of threats, and Keenan discloses that Views may use color to 'represent different types of risk (e.g., cyber, environmental, accidental, etc.).'" Petition, 28. But Petitioner's expert admitted in his deposition that knowing risk does not allow one to determine the threat that may have given rise to the risk. EX-2002, 61:7-24; see also 64:14-25, 66:2-9, EX-2009, ¶81. This deposition testimony contradicted Mr. Hurlbut's declaration testimony. EX-1003, ¶82.

PO Sur-reply 9–10.

Similarly, Patent Owner argues that Petitioner proffers another *false* premise, namely that "in order to analyze risk (as in Keenan), [the skilled artisan] must know the 'impact' of a threat and the 'likelihood' that the threat will occur, and thus, must determine the threat, in order to calculate the risk." PO Sur-reply 10. Patent Owner argues "Keenan never discloses a need to 'calculate risk'":

> Keenan's system <u>*starts with the risk levels already calculated*</u> for each object in each View. Keenan explains that "each object is defined by a fixed set of characteristics." EX-1004, 11:19-20. "Characteristics" are defined in Keenan to include a "risk measurement." EX-1004, 4:64-66. In Keenan's user interface for the IOE, a box "allows a user a quick way to calculate the risk <u>*of the selected View*</u>." EX-1004, 18:6-8 (emphasis added), *see also* EX-1004, 18:8-22. In Keenan, a user can "calculate" the aggregate risk in a View or aggregate risk in a path within a View based on a formula (not disclosed) or an aggregation formula (not disclosed). EX-1004, 18:6-22, *see also* 1:47-52, 2:1-2, 4:64-67, 5:33-44. Keenan never calculates the risk of an individual object within a View, which is the premise of the argument in the Reply. *E.g.*, Reply, 14.

PO Sur-reply 11; *see* Ex. 2009 ¶ 112.

In response to Petitioner's argument that "there is simply no requirement in the claims of the '366 patent that a specific threat must be identified" (Pet. Reply 16), Patent Owner argues that "[t]his statement is true as far as it goes," because "[t]he claims do not require a literal 'determination' of a threat," rather "the claims do require the storing of specific threats in one or more databases and the association of each of those threats with at least one threat model component through the one or more databases." PO Sur-reply 14–15. But, Patent Owner argues, "a 'determination' of threats is as far as Petitioner attempted to go with Keenan." *Id.* at 15 (citing Pet. 28 ("measuring risk includes a determination of threats")); Pet. Reply 13 ("[the skilled artisan] must determine the threat").

*(f) Analysis*

We have considered Petitioner's arguments and cited evidence concerning whether Keenan explicitly discloses limitation 1[b] to the skilled artisan, and find them unpersuasive on the complete record before us. Rather, we find Patent Owner's arguments and cited evidence persuasive, and more than sufficient to defeat Petitioner's challenge, given Petitioner's burden to show invalidity by a preponderance of the evidence.

Put simply, we find Keenan explicitly discloses, *inter alia*, *risk* modeling, not *threat* modeling as recited in claim 1, and whether Keenan may inherently disclose such threat modeling is not before us. *See* Ex. 2009 ¶ 103 ("Keenan does not disclose threats at all. Keenan is all about viewing and analyzing risk." (cited at PO Resp. 29–30)), ¶ 111 ("[A]t best, Keenan discloses a *risk* modeling system/method."). This comports with our construction of "threat," which we find in the context of the '366 patent does not encompass "risk." *See supra* § III.D.3.a.1 (discussing "'Threats' versus 'Risks'"). We agree with Patent Owner that Petitioner's premise that "risk" includes "threats" or knowing risk allows for determination of threats is *false*, and belied by the parties' experts who do not disagree on this distinction, namely that "risk" is not a "threat," but rather represents the *likelihood* of a threat occurring compounded by the *impact* of such a threat on a given system (discussed above). *See* Ex. 2002, 24:3–25:5, 31:5–33:2 (Petitioner's expert, Mr. Hurlbut, agreeing that "Risk = Likelihood x Impact"); Ex. 2009 ¶ 80; PO Sur-reply 9–10. Thus, we find unavailing Petitioner's attempt to walk backwards from Keenan's explicit disclosure of "risk" modeling into an anticipatory (explicit) disclosure of stored "threats" that may give rise to such risk.

Viewing Keenan in the light agreed upon by the parties' experts, where "risk" is *a product of* the "likelihood" of a threat occurring and the "impact" of such a threat on a given system, persuades us that although Keenan discloses "risk," "types of risk," and "risk ranking" (*see, e.g.*, Ex. 1004, 16:21–63), Keenan uses such "risk" as a given value without explicitly disclosing any underlying stored threats or use thereof. *See* Ex. 2009 ¶ 112 ("Keenan does not disclose a system for measuring risk. The risk for objects is determined before the objects are imported into the [Integrated Object Environment]. Keenan does not make that measurement."). Indeed, in order to "store" "threats" in "one or more databases" as recited in claim 1, such "threats" must be identified (i.e., known) at some level of specificity to the system. Petitioner does not direct us to any persuasive evidence that Keenan explicitly discloses using "threats" or "storing" an identified "threat," let alone storing such "threat" in a database along with its association with a particular threat model component, and even more so with a threat model component that itself is correlated with a third-party diagram component as recited in claim 1.

Again, Petitioner unpersuasively attempts to show limitation 1[b] by working backwards from what Keenan does disclose—*risk*, arguing that given the "formula" for "risk" agreed upon by the parties' experts (discussed above), Keenan must know and store threat "likelihood" and "impact" information. But Petitioner's argument here is based on the unproven premise that Keenan explicitly discloses "calculating risks" for a particular object based on stored "threats" associated not only with such "risks" but also threat model components—there is no persuasive evidence of record that Keenan explicitly discloses measuring or calculating "risk" for a particular object, let alone whether such "risk" in fact is calculated based on stored "threats" associated with threat model components. *See* Ex. 2009 ¶ 68 ("Keenan refers to the 'risk' as a property. . . . Keenan also refers to the risk as a 'value.'. . . Keenan also refers to 'risk' as a characteristic that is 'preset.'. . . These portions of Keenan make it clear that 'risk' in Keenan is a preset value as property of an object. Keenan does not identify any 'threats' as claimed."), 112 ("I disagree that 'the risk' [in Keenan] 'includes threats.' Neither generally nor in the context of Keenan does risk 'include threats.' Risk might be based on a threat. But risk does not include a threat and determining risk does not require identifying or determining a threat.").

As for Keenan's statement that "[a] Technical Risk Measurement view 708 uses color to represent different types of risk (e.g., cyber, environmental, accidental, etc.)" (Ex. 1001, 16:45–48), based on the complete record now before us, we find unpersuasive Petitioner's argument that the "types of risk" are "threats" as recited in claim 1 (*see* Pet. 26–28). Indeed, given our construction of "threat" (*see supra* § III.D.3.a.1) and the parties' experts' agreement that "risk" and "threat" are distinct, as discussed above, we find this disclosure in Keenan means precisely what it says, namely that "types" of "risk" include cyber risk, environmental risk, and accidental risk, and does not explicitly disclose to the skilled artisan anything about threats or storing of threats associated with threat model components. *See* Ex. 2009 ¶ 121 ("[Petitioner's expert's] conclusion ignores the plain language in Keenan. The cited portion of Keenan expressly says that 'cyber, environmental, accidental, etc.' are all different types of *risk* – not threats. Again, [Petitioner's expert] simply assumes that knowing risk determines a threat or that 'risk' is synonymous with 'threat.' That is incorrect.").

For the foregoing reasons, and based on the complete record before us, we conclude that Petitioner has not sufficiently evidenced that Keenan explicitly discloses limitation 1[b], namely, "a plurality of threat model components stored [in one or more databases]; and a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases," as recited in independent claim 1.

*(3) Conclusion for Independent Claim 1*

For the foregoing reasons, and based on the complete record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that independent claim 1 is unpatentable as anticipated by Keenan.

*b) Independent Claims 8 and 16 and Dependent Claims 2–7, 9–15, and 17–20*

Petitioner contends independent claims 8 and 16 are substantially the same as independent claim 1, except that features of "method" claim 1 are variously embodied in "system" claims 8 and 16. Pet. 48–54 (citing Ex. 1003 ¶¶ 119–130), 58–59. As for the subject matter of limitation 1[b] as recited in claims 8 and 16, Petitioner relies on its same arguments proffered for claim 1. *See id.* Petitioner's evidentiary showing for independent claims 8 and 16, as well as for dependent claims 2–7, 9–15, and 17–20, does not remedy the deficiencies in its evidentiary showing for independent claim 1. *See supra* Section III.D.3.a; *see also* Pet. 41–60; Pet. Reply 7–20. Thus, we determine that Petitioner has not demonstrated by a preponderance of the evidence that any of independent claims 8 and 16 and dependent claims 2–7, 9–15, and 17–20 is unpatentable as anticipated by Keenan.

*E. Alleged Obviousness of Claims 1–4, 7–11, and 15–18 over the Combination of Zheng, Baker, and Jones*

Petitioner contends claims 1–4, 7–11, and 15–18 would have been unpatentable under 35 U.S.C. § 103 as obvious over the combination of Zheng (Ex. 1005), Baker (Ex. 1006), and Jones (Ex. 1007). Pet. 17–20, 60–85; Pet. Reply 20–25. Patent Owner opposes Petitioner's contentions. PO Resp. 49–52; PO Sur-reply 20–26. For the reasons expressed below, and based on the complete record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that any of claims 1–4, 7–11, and 15–18 would have been unpatentable as obvious over the combination of Zheng, Baker, and Jones. We turn first to overviews of Zheng and Baker (Jones is not implicated in our discussion below).

*1. Overview of Zheng (Ex. 1005)*

Zheng generally is directed to "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*." *Id.* at 1:48–53 (emphases added). 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 (emphases added). On its face, Zheng uses the term "map" consistently in the context of cartography, i.e., creating a digital view of components and their interconnections (like drawing for someone a map of how computer network components are interconnected).

Zheng's Figure 2 is reproduced below.

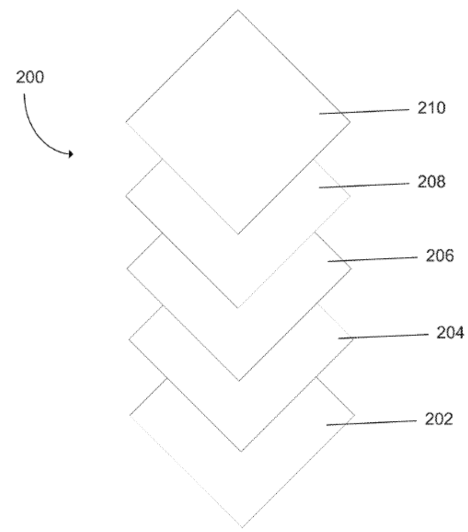


FIG. 2

Figure 2 depicts a multi-layered structure that can be rendered in a computer display by the visualization module.

Ex. 1005, 3:3–5, Fig. 2. Referring to Figure 2, Zheng discloses multilayered structure 200 includes four different overlaying layers, with base layer 202 representing at least a portion of a company's application architecture. *Id.* at 3:66–4:2. Zheng explains:

> [T]he base layer 202 can visualize application components and relationships as a map to facilitate data extraction. The base layer 202 serves as the foundational piece of the security risk analysis system 100. The additional layers of the system 100 (akin to terrains, traffics, etc. of a map) include a layer representing threat modeling 204 of perceived threats, a layer representing security controls 206, a layer representing real-time (or near real-time) actual threats 208, and a layer representing simulated data flow 210 throughout the application ecosystem. These additional layers 204-210 can overlay the foundational map layer 202, similar to how traffic and other information (in addition to basic cartographical details) is represented on maps.

> These additional layers 204-210 can overlay the base layer 202 in the order as illustrated in FIG. 2 or any other order.

*Id.* at 4:3–18.

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

*2. Overview of Baker (Ex. 1006)*

Baker discloses an "automated risk management system," where a user is able to build a risk management flowchart (or multiple flowcharts) that "utilizes symbols of various shapes to indicate actions, determinations, or other elements of an activity or evaluation so that respective personnel of an organization can understand actions to be taken to successfully manage an activity or avoid a negative outcome." Ex. 1006 ¶¶ 5, 20, 25. "[R]isk management or control flowcharts may be imported . . . from third party software such as that marketed as Microsoft Office Visio®." *Id.* ¶ 25.

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

*3. Analysis*

*a) Independent Claim 1*

The parties dispute, *inter alia*, whether Petitioner has proven that the combination of Zheng, Baker, and Jones teaches limitations 1[c] and 1[d], namely, 1[c] "providing one or more *mapping files* communicatively coupled with the one or more databases," and 1[d] "the one or more mapping files *correlating* [1] the threat model components *with* [2] visual diagram components of a third party software application (hereinafter 'third party diagram components')." Pet. 63–65; PO Resp. 28–29, 49–52; Pet. Reply 5–7, 20–23; PO Sur-reply 4–5, 20–22; Ex. 1001, 43:30–35 (emphases added). The parties also dispute whether Petitioner has proven that the skilled artisan would have had a rational reason to combine these three references to achieve the invention recited in claim 1 (and in claims 2–4, 7–11, and 15–18). Pet. 83–85; PO Resp. 51–52; Pet. Reply 23–25; PO Sur-reply 23–26. We turn first to the meaning of "mapping file."

*(1) What is a "Mapping File"?*

Patent Owner proffers that "mapping file" should be construed to mean "a file or one or more tables that correlate threat model components with visual diagram components of a third party software application." PO Resp. 28–29 (citing Ex. 2009 ¶¶ 97–99). Patent Owner submits:

> During prosecution of the '366 Patent, the applicant explained that "[t]he mapping file correlates the internal threat model components with the external third party diagram components so that the system can read a file created with the third party software program and generate its own diagram using internal components that are, through the mapping file, correlated to the external third party components." EX-1002, 506; EX-2009, ¶97.

PO Resp. 28. Petitioner proffers that "mapping file" is a "general term[] that [is] well known to [the skilled artisan] in the field of threat modeling," and should be given its plain and ordinary meaning, namely "a file or other representation that correlates data from a source to a target." Pet. Reply 5–6. Petitioner disputes that the meaning of "mapping file" itself should include reference to threat model components and third party diagram components. *See id.* at 6–7. Patent Owner responds that "Petitioner's criticisms are irrelevant because Petitioner concedes that the language it complains about is already a requirement of the independent claims." PO Sur-reply 4–5.

Claim 1 recites, in part, "the one or more mapping files correlating the threat model components with ["third party diagram components"]."

Ex. 1001, 43:30–35. Generally, from the standpoint of what claim 1 requires, the parties' views of "mapping file" are in alignment. Claim 1 plainly recites that a "mapping file" (where a "file" in the context of computer systems is data itself) *correlates* data A *with* data B, and when construed in the context of the subject claim language, *correlates* threat model components (i.e., data A) *with* third party diagram components (i.e., data B). We find that this interpretation of "mapping files" is sufficient to resolve the controversy between the parties. *See Nidec Motor*, 868 F.3d at 1017.

*(2) Limitations 1[c]/1[d]: "providing one or more mapping files communicatively coupled with the one or more databases, the one or more mapping files correlating the threat model components with ["third party diagram components"]*

*(a) The Petition*

Petitioner argues Zheng discloses limitation 1[c], namely, "providing one or more mapping files communicatively coupled with the one or more databases." Pet. 63. In particular, Petitioner argues "Zheng's 'mapping techniques' and its 'map' convey, and necessarily include, a 'mapping file' as claimed because a mapping file would be required to perform mapping techniques." Pet. 63 (citing Ex. 1003 ¶ 162). Petitioner also argues "the one or more mapping files in Zheng are communicatively coupled with the one or more databases because Zheng discloses 'at least one ***database*** table is used to ***store data*** for ***each layer*** and ***for each possible combination/ interaction*** of the layers.'" Pet. 63 (citing, *inter alia*, Ex. 1005, 8:25–27; Ex. 1003 ¶ 163).

Petitioner then turns to Baker for allegedly disclosing limitation 1[d], namely, "the one or more mapping files correlating the threat model components with visual diagram components of a third party software application." Pet. 64–65. Petitioner argues Baker discloses "visual diagram components of a third party software application" based on its disclosure of importing flowcharts from Visio, discussed above. Pet. 64. Petitioner also argues:

> Baker allows a user to select the option to "***import***" the Visio visual diagram components to Baker's system, such that "a mapping file or the like as claimed in the claims," such as the mapping file of Zheng, "would be useful to map between elements of the two software applications," as defined in the file history.

Pet. 64–65 (citing, *inter alia*, Ex. 1003 ¶ 164).[7]

*(b) Patent Owner's Response*

Patent Owner first directs us to Zheng's disclosure of its system for "real-time (or near real-time) *visualization* of at least a portion of a company's application architecture and performing security risk analysis and threat detection based on the *visualization*," in which Zheng explains:

> [B]y utilizing a *visualization approach like cartography*, application architecture can be represented in a compressible view that enhances security and risk analysis. For example, *mapping techniques* and concepts can be used *in the context of*

[7] This quoted language of "a mapping file or the like as claimed in the claims would be useful to map between elements of the two software applications" comes from the prosecution history of the '366 patent, and are *the inventor's words used in explaining the claimed invention* to the Examiner and, in particular, in clarifying how "third party" is used in the claims. *See* Ex. 1002, p. 8 (Response to Office Action dated Nov. 18, 2019) (page citation is to exhibit page numbering).

> *data visualization to create a graphical representation of application connectivity and security*.

Ex. 1005, 3:24–34 (emphases added); *see* PO Resp. 49. Patent Owner argues "Zheng uses the term 'map' consistently in the context of cartography, *i.e.*, creating a digital view of components and their interconnections (like drawing a map of how computer network components are interconnected). PO Resp. 49 (citing Ex. 2009 ¶ 135). Patent Owner argues, although Zheng uses the words "mapping techniques" which at least sound like the words "mapping files" in the subject limitation, "Zheng's 'mapping techniques' are related to visualization of the application architecture, 'like cartography,' and have nothing to do with 'correlating the threat model components with visual diagram components of a third party software application' as recited in the claims." *Id.* at 49–50; *see* Ex. 2009 ¶ 136. Also, contrary to Petitioner and its expert (Pet. 63), Patent Owner argues "Zheng's generic disclosure of 'mapping techniques . . . in the context of data visualization' does not necessarily require any 'mapping files' as claimed." PO Resp. 50 (citing Ex. 2009 ¶ 136).

As for Baker, Patent Owner observes initially that, "[b]y relying on [Zheng for "mapping files" but] Baker for the 'correlating' feature, Petitioner implicitly acknowledges that Zheng itself does not disclose 'mapping techniques' in the context of 'correlating' components in the claimed manner." PO Resp. 50 (citing Ex. 2009 ¶ 137); *but see* Pet. Reply 24 (Patent Owner arguing to the contrary). Patent Owner again argues "Zheng does not disclose any mapping file, either expressly or inherently, and even considered in view of Baker, fails to disclose or suggest *the claimed correlations* based on mapping files." *Id.* at 51 (citing Ex. 2009 ¶ 139) (emphasis added). Patent Owner argues:

> Baker's process has no need or use for any "mapping files" as recited in the claims. Baker stores the "text and shape of each element of the flowchart . . . in the process database 30" and "automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts." Baker, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any "mapping files" providing correlations as recited in the claims. EX-2009, ¶139.

*Id.* Patent Owner submits that, in order to reach the claimed "mapping files" *correlations* recited in claim 1, "Petitioner first has to create a mapping file to capture the threat actor/threat target association of Zheng, and then has to create a modification to repurpose the associations." *Id.* at 51–52 (citing Ex. 2009 ¶ 140). Patent Owner argues "[t]he motivations for these additions are hindsight-based creations of features not disclosed or suggested by the art": "Neither Baker nor Zheng teaches 'correlating' (a) threat model components with (b) visual diagram components of a third party software application, let alone doing so using 'mapping files.'" *Id.* We find Patent Owner's arguments persuasive.

*(c) Petitioner's Reply*

Petitioner, in its Reply, argues in various forms that Zheng discloses "mapping techniques" (mapping files) *beyond the cartography context* discussed above. *See* Pet. Reply 20–23. Petitioner points to Zheng's disclosure that "additional layers 204-210 can overlay the foundational map layer 202, similar to how traffic and other information (*in addition to basic cartographical details*) is represented on maps" (Ex. 1005, 4:3–18 (emphasis added)), and argues the "in addition to basic cartographical details" language allegedly means at least some information in other layers is "mapped" (correlated) via mapping files to foundational map layer 202. *See* Pet.

Reply 21–23. Petitioner argues "a visualization structure that uses overlaying layers is quite different than the simple practice of drawing a cartographic map," and "[i]t is this overlay linkage between layers or 'map' that the Petition relied upon for Zheng's mapping because it is the threat modeling layer that overlays the threats and threat actors on the base layer." *Id.* at 22. According to Petitioner, "Zheng discloses the use of a mapping file for interactions between the layers." *Id.* at 22–23.

*(d) Patent Owner's Sur-Reply*

Patent Owner responds that "[t]he arguments presented in the Reply expressly ignore recited claim elements":

> The claims expressly recite "one or more mapping files *correlating the threat model components with visual diagram components of a third party software application*." While Petitioner alleges that the prior art teaches mapping various elements, these allegations fail to demonstrate a mapping of "threat model components with visual diagram components of a third party software application."

PO Sur-reply 20. We agree, as discussed below in our analysis section.

As for Petitioner's arguments concerning alleged mapping between certain additional layers and foundational map layer 202 of Zheng (*see* Pet. Reply 20–23), Patent Owner argues each such layer represents a cartographical representation of elements relevant to that layer, and Zheng discloses overlaying one or more of such layers on foundational map layer 202 using a visualization module to render those overlapped layers on a computer display, without disclosing use of the claimed "mapping files" to do so. *See* PO Sur-Reply 21 ("Zheng explains that '[g]enerally, data in the threat modeling layer 204 can be organized into threat agents, vectors, and targets.' This is a cartographic representation of the elements in Zheng's threat modeling layer. This does not describe the claimed "mapping files." (internal citation omitted); "Zheng never explains that overlaying active attacks (such as those in the threat update layer 208 or any other overlaid layer) uses a claimed 'mapping file.'").

Patent Owner also disputes that Zheng's description of "at least one database table is used to store data for each layer *and for each possible combination/interaction of the layers*" (Ex. 1005, 8:25–27 (emphasis added)) discloses use of the claimed mapping files to do so:

> While Zheng teaches that it can store data in a database for a combination/interaction of multiple layers, Zheng discloses that the data from each of two or more layers is simply combined into a single database table. EX-1005, 8:25-38. There is no disclosure that a claimed "mapping file" is used. In fact, the teaching that a single database table includes data from multiple layers eliminates the need for a mapping file to correlate the data from two or more different layers.

PO Sur-reply 21–22.

*(e) Analysis*

We have considered Petitioner's arguments and cited evidence concerning whether limitations 1[c] and 1[d] would have been taught or suggested by the combination of Zheng, Baker, and Jones, and find them unpersuasive on the complete record before us. Rather, we find Patent Owner's arguments and cited evidence persuasive, and more than sufficient to defeat Petitioner's challenge, given Petitioner's burden to show invalidity by a preponderance of the evidence.

Put simply, we find Petitioner does not sufficiently show, for example, how Zheng, Baker, or the combination thereof teaches or even fairly suggests "*correlating*" (a) threat model components *with* (b) visual diagram components of a third party software application, let alone doing so using "mapping files." We agree with Patent Owner and its expert, Dr. Nielson, that Zheng's "mapping techniques" are related to visualization of the application architecture, like cartography, and "have nothing to do with 'correlating the threat model components with visual diagram components of a third party software application'" as recited in claim 1. Ex. 2009 ¶ 136; *see* PO Resp. 49–50. Even if one were to consider Zheng to teach or at least fairly suggest some form of correlation between its overlaid layers via mapping files, unlike the features of the subject limitations, such correlations would be only between layers *all within the same Zheng system*. *See* PO Sur-reply 22 ("The layers relied upon in the Reply are layers created within the Zheng system and are not third party diagram components in a data file that is read by Zheng's system.").

In sum, we agree with Dr. Nielson's (Patent Owner's expert) general characterization of Petitioner's challenge to limitations 1[c] and 1[d]: "To reach the claimed correlations recited in claim 1, Petitioner and Mr. Hurlbut first have to create a mapping file that exists in neither reference [i.e., Zheng or Baker] in order to capture the threat actor/threat target association of Zheng, and then have to create a modification to the non-existent/created mapping file to repurpose the associations" to account for mapping internal data with external (imported) data (Ex. 2009 ¶ 140). We are unpersuaded that this exercise is sufficient to show that these references together would have taught the subject limitations to the ordinarily skilled artisan.

##### *(3) No Reason to Combine Zheng, Baker, and Jones but for Impermissible Hindsight*

Petitioner argues the skilled artisan would have combined the relevant teachings from Baker with the system of Zheng "to enable the importation of diagrams from Microsoft Visio into the threat modeling software of Zheng such that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams." Pet. 65 (citing Ex. 1003 ¶ 166); *see* Pet. 83–85 (alleged reasons to combine Zheng and Baker). Petitioner argues "Zheng provides express motivation" to combine the teachings of Zheng, Baker, and Jones, because Zheng states, "there is a need for *improved systems*, methods and apparatuses for a *more effective and efficient threat modeling approach* in the context of application architecture and infrastructure."[8] Pet. 83 (quoting Ex. 1005, 1:37–40) (emphases altered); *see id.* at 83–84 ("[T]he ability to import existing diagrams from Visio, as taught in Baker, and the ability to generate threat reports, as taught in Baker and Jones, would reduce amount of tedious and unmanageable work that human operators would otherwise need to handle and provide commonplace, easy-to-understand visualizations."[9]).

---

[8] Patent Owner persuasively responds that "Zheng's background lays the foundation for the solution described by Zheng itself. The background does not provide [the skilled artisan] with a motivation to look elsewhere for the solution." PO Sur-reply 25.

[9] Patent Owner persuasively responds that "faster speed is an unsupported assumption by Petitioner. . . . [T]he system architecture has to be defined one place or the other. There is no evidence that defining the architecture in a third party application is faster than defining it directly in Zheng." PO Sur-reply 25–26.

Petitioner argues "Microsoft Office Visio was a well-known software tool for generating flowcharts and diagrams at the time the patents were filed," and thus the skilled artisan "would have been motivated to allow users to take existing diagrams already prepared in Visio and import those diagrams into the system of Zheng," which "would allow users to create threat models from diagrams already created in Visio to save time of creating those same diagrams using a native interface in the Zheng system." Pet. 84 (citing Ex. 1007, 18:30–43; Ex. 1003 ¶ 213); *see id.* at 84–85 (discussing that "compatibility between software programs is a positive improvement that users appreciate").

Patent Owner responds that Petitioner's alleged motivations for combining the subject references to achieve limitations 1[c] and 1[d] and claim 1 as a whole are based solely on impermissible hindsight. *See* PO Resp. 51–52 (citing Ex. 2009 ¶ 140 (Patent Owner's expert testifying: "I have reviewed the alleged motivations to combine . . . and find no technical explanations or motivations for creating the mapping file, nor for modifying the mapping file if it existed. Rather, the motivations for these additions appear to be hindsight-based creations of features not disclosed or suggested by the art.")).

Petitioner replies that the skilled artisan would have combined the teachings of Zheng and Baker because "Baker's system also discloses a mapping file," and "[t]he ability to import visual diagram components of a third party software [was] well known in the art." Pet. Reply 23–25.

Patent Owner responds that "[Petitioner's] cited portions of Baker do not teach or suggest 'mapping files correlating the t[h]reat model components with visual diagram components of a third party software application,' as required by the claims." PO Sur-reply 23.

> Instead, at most, Baker discloses importing "risk management or control flowcharts" from a third party software application, such as Visio, and "automatically assign[ing] or associat[ing] predetermine[d] objectives or controls according to the shapes of the imported flowcharts." EX-1006, [0025]. Baker never explains what "objectives" are beyond stating that the system memory "incudes process flowchart data indicative of an organization's process objectives and controls." EX-1006, [0005], *see also* [0005], [0011]-[0013]. Baker never teaches that the "objectives" or "controls" are threat model components, as required by the claims. Further, as explained in the Response, Baker has no need for "mapping files." Response, 51.

*Id.*

Patent Owner argues that Petitioner's argument that "Baker discloses 'correlating Visio shapes to native shapes'" is flat "wrong." PO Sur-reply Reply, 24.

> Baker discloses "assign[ing] or associat[ing] predetermine[d] objectives or controls according to the shapes of the imported flowcharts." EX-1006, [0025]. Baker makes no mention of correlating Visio shapes to native shapes. In fact, Baker says the opposite. It says it assigns or associates the objectives or controls "to the shapes of *<u>the imported flowcharts</u>*." EX-1006, [0025] (emphasis added). No correlation or substitution of one set of shapes for another set of shapes occurs in Baker.

*Id.*

As for Petitioner's argument that systems were known to import visual diagram components of third party software into another system, Patent Owner responds that "the novelty of that feature is not the question. The question is whether there is evidence supporting [Petitioner's] argument that [the skilled artisan] would have been motivated to combine Zheng with

Baker." PO Sur-reply 25. Patent Owner argues Petitioner's general hand waiving arguments about "ease of use and general improvements" lack "proper and sufficient evidentiary support." *Id.*

We agree with Patent Owner and find Petitioner's arguments unpersuasive, because Petitioner's proffered reasons for combining Zheng and Baker are plagued by impermissible hindsight. *See InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) ("It appears that [the expert] relied on the . . . patent itself as her roadmap for putting what she referred to as pieces of a 'jigsaw puzzle' together."). Although "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton" (*KSR*, 550 U.S. at 421), the Federal Circuit has observed that "'the prejudice of hindsight bias' often overlooks that the 'genius of invention is often a combination of known elements which in hindsight seems preordained.'" *Polaris Industries, Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068 (Fed. Cir. 2018). Here, we determine Petitioner's overarching rationale for combining Zheng and Baker, namely, "to enable the importation of diagrams from Microsoft Visio into the threat modeling software of Zheng such that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams" (Pet. 65), is gleaned only from applicant's disclosure, not the art.

We further discuss this determination below and begin by summarizing the disclosures of Zheng and Baker:

(1) Zheng discloses a threat modeling and visualization system having a base layer and multiple other selectable layers each revealing different types of information that can be overlaid onto each other and shown together on a computer display, where these various layers all come to life within

Zheng's system itself (i.e., there is no importation of third-party diagram components subsequently correlated with threat model (internal) components) (*see supra* § III.E.1; PO Sur-reply 22);

(2) Zheng does not disclose that its layers are overlaid for display using mapping files (e.g., through correlation of components within different layers), and to the contrary, Zheng's disclosed use of a *single* database table that includes data for multiple layers eliminates the need for a mapping file to correlate the data for two or more different layers (*see supra* § III.E.3.a.2.e);

(3) even if Zheng were to fairly suggest some form of correlation between its overlaid layers via mapping files, such correlations would be only between layers *all within the same Zheng system* (i.e., the correlations would not be between imported third-party diagram components and threat model (internal) components) (*see supra* § III.E.3.a.2.e);

(4) Baker discloses importing risk management flowcharts from a third-party software application, such as Visio, for analysis (*see supra* § III.E.2); and

(5) Baker discloses storing the text and shape of each element of the flowchart in a process database, and automatically assigning or associating predetermined objectives or controls according to the shapes of the imported flowcharts (i.e., Baker searches for flowchart shapes without disclosing use of any mapping files providing correlations between imported third-party diagram components and threat model (internal) components) (*see supra* § III.E.3.a.2.e; Ex. 1006 ¶ 25; Ex. 2009 ¶ 139 ("Baker's process has no need or use for any 'mapping files' as recited in the claims.")).

In sum, Zheng does not disclose mapping files, but even if it did, Zheng still does not disclose importation of third-party diagram components subsequently correlated with threat model (internal) components using such mapping files. Baker discloses importation of third-party diagram components via Visio, but does not disclose mapping files or at least mapping files correlating the third-party diagram components with threat model (internal) components. Given this context, we find no evidence of record sufficiently showing why the skilled artisan would have taken the fabric of Zheng and stitched it together not only with imported third-party diagram components along with mapping files, but mapping files that correlated the third-party diagram components with threat model (internal) components. We find Petitioner's reach to reasons to do so like improving threat modeling systems or creating more effective, efficient, or faster threat modeling systems to be insufficiently supported (if at all) and unpersuasive. We also find this context shows that Petitioner's proffered reasons for combining Zheng and Baker (and Jones) to achieve the subject limitations lack rational underpinning, and that Petitioner's proposed combination of teachings plainly takes into account knowledge gleaned only from applicant's disclosure, i.e., impermissible hindsight. *See In re McLaughlin*, 443 F.2d 1392, 1313–14 (CCPA 1971).

*(4) Conclusion for Independent Claim 1*

For the foregoing reasons, and based on the complete record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that independent claim 1 would have been unpatentable as obvious over the combination of Zheng, Baker, and Jones.

#### *b) Independent Claims 8 and 16 and Dependent Claims 2–4, 7, 9–11, 15, 17, and 18*

Petitioner contends independent claims 8 and 16 are substantially the same as independent claim 1, except that features of "method" claim 1 are variously embodied in "system" claims 8 and 16. *See supra* § III.D.3.b. As for the subject matter of limitations 1[c] and 1[d] as recited in claims 8 and 16, Petitioner relies on its same arguments proffered for claim 1. *See* Pet. 76, 82. Petitioner's evidentiary showing for independent claims 8 and 16, as well as for dependent claims 2–4, 7, 9–11, 15, 17, and 18, does not remedy the deficiencies in its evidentiary showing for independent claim 1. *See supra* Section III.E.3.a. Thus, we determine that Petitioner has not demonstrated by a preponderance of the evidence that any of independent claims 8 and 16 and dependent claims 2–4, 7, 9–11, 15, 17, and 18 would have been unpatentable as obvious over the combination of Zheng, Baker, and Jones.

### *F. Alleged Obviousness of (1) Claims 2, 9, and 17 over the Combination of Zheng, Baker, Jones, and Galliano; (2) Claims 1–20 over the Combination of Zheng, Baker, Jones, and Keenan; and (3) Claims 2, 5, 6, 9, 12–14, 17, 19, and 20 over the Combination of Zheng, Baker, Jones and "the knowledge of a POSITA"*

Petitioner contends certain claims are unpatentable under 35 U.S.C. § 103 as obvious over the following combinations: (1) claims 2, 9, and 17 over the combination of Zheng (Ex. 1005), Baker (Ex. 1006), Jones (Ex. 1007), and Galliano (Ex. 1008); (2) claims 1–20 over the combination of Zheng, Baker, Jones, and Keenan (Ex. 1004); and (3) claims 2, 5, 6, 9, 12–14, 17, 19, and 20 over the combination of Zheng, Baker, Jones and "the knowledge of a POSITA." Pet. 12, 85–89.

As for combination (1) above, Petitioner applies this combination only to dependent claims 2, 9, and 17, and does not apply Galliano in any manner that would cure any deficiencies in Petitioner's challenges identified herein in Section III.E above, particularly to independent claims 1, 8, and 16. *See* Pet. 85–87.

As for combination (2) above, Petitioner applies this combination only to dependent claims 5, 6, 12–14, 19, and 20, and does not apply Keenan, in this obviousness context, in any manner that would cure any deficiencies in Petitioner's challenges identified herein in Section III.E above, particularly to independent claims 1, 8, and 16. *See* Pet. 87–88. Although we recognize that Petitioner alleges Keenan anticipates claims 1–20, as discussed above in Section III.D, we discern no arguments *in the Petition* as to which teaching(s) of Keenan are applied in conjunction with teachings of Zheng, Baker, and Jones to arrive at claims 1–4, 7–11, and 15–18.

As for combination (3) above, Petitioner applies this combination only to dependent claims 2, 5, 6, 9, 12–14, 17, 19, and 20, and does not apply any alleged "knowledge" of the skilled artisan, in this obviousness context, in any manner that would cure any deficiencies in Petitioner's challenges identified herein in Section III.E above, particularly to independent claims 1, 8, and 16. *See* Pet. 88–89.

Accordingly, based on the record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that any of the foregoing claims would have been obvious over the noted combinations (1), (2), and (3) discussed above.

## IV. CONCLUSION

Petitioner has not proven, by a preponderance of the evidence, that any of the Challenged Claims is unpatentable.

## V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–20 of U.S. Patent No. 10,713,366 B2 have not been shown, by a preponderance of the evidence, to be 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.

In summary:

| Claim(s) | 35 U.S.C. § | Reference(s)/ Basis | Claim(s) Shown Unpatentable | Claim(s) Not Shown Unpatentable |
|---|---|---|---|---|
| 1–20 | 102 | Keenan | | 1–20 |
| 1–4, 7–11, 15–18 | 103 | Zheng, Baker, Jones | | 1–4, 7–11, 15–18 |
| 2, 9, 17 | 103 | Zheng, Baker, Jones, Galliano | | 2, 9, 17 |
| 1–20 | 103 | Zheng, Baker, Jones, Keenan | | 1–20 |
| 2, 5, 6, 9, 12–14, 17, 19, 20 | 103 | Zheng, Baker, Jones[10] | | 2, 5, 6, 9, 12–14, 17, 19, 20 |
| **Overall Outcome** | | | | 1–20 |

[10] *See supra* n.2.

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