



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/251,144	04/11/2014	Nikolaos Anerousis	YOR920130170US1	6629
98841	7590	12/20/2019	EXAMINER	
Otterstedt, Wallace & Kammer, LLP			HENRY, MATTHEW D	
P.O. Box 381			ART UNIT	PAPER NUMBER
Cos Cob, CT 06807-0381			3683	
			MAIL DATE	DELIVERY MODE
			12/20/2019	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte NIKOLAOS ANEROUSIS, SHANG Q. GUO,
DANIELA ROSU, and FREDERICK Y. WU

Appeal 2019-002830
Application 14/251,144
Technology Center 3600

Before DONALD E. ADAMS, JEFFREY N. FREDMAN, and
RACHEL H. TOWNSEND, *Administrative Patent Judges*.

ADAMS, *Administrative Patent Judge*.

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant¹ appeals from Examiner's decision to reject claims 1, 2, 4–11, 13–19, and 21–28 (*see* Final Act.² 2).

We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

¹ We use the word “Appellant” to refer to “applicant” as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as “International Business Machines Corporation” (Appellant’s November 20, 2018 Appeal Brief (Appeal Br.) 2).

² Examiner’s April 18, 2018 Final Office Action.

STATEMENT OF THE CASE

Appellant’s disclosure “relates to the electrical, electronic and computer arts, and, more particularly, to information technology (IT) services management and analytics, and the like” (Spec.³ 1:12–13). Claim 1 is representative and reproduced below:

1. A method comprising:

executing a system management tool, with a risk assessment mode enabled, within an execution infrastructure on a management computer system, to manage a target computer system in a production situation;

during execution of said system management tool with said risk assessment mode enabled, when said execution of said tool reaches a risk segment which is not deemed safe:

informing a user of said tool of at least one action to be executed in said risk segment;

if said user agrees, allowing said tool to execute said risk segment;

otherwise, overriding said risk segment with one or more alternate operations; and

at least when said risk segment is executed, obtaining feedback from said user regarding whether said risk segment is deemed safe;

repeating said executing, informing, allowing, and obtaining steps for a plurality of additional risk segments until all of said risk segments are deemed safe; and

once all of said risk segments are deemed safe, transitioning said system management tool from said risk assessment mode to an automatic mode of operation;

wherein a given one of said risk segments is conditionally executed until said given one of said risk segments is deemed safe;

³ Appellant’s April 11, 2014 Specification.

Appeal 2019-002830
Application 14/251,144

wherein said given one of said risk segments is automatically executed once said given one of said risk segments is deemed safe; and

wherein said given one of said risk segments is conditionally executed at least once and then is automatically executed at least once.

(Appeal Br. 42 (emphasis added).)

Grounds of rejection before this Panel for review:

Claims 1, 2, 4–11, 13–19, and 21–28 stand rejected under 35 U.S.C. § 101.

Claims 1, 2, 4, 5, 9–11, 13, 14, 18, 19, 21, 22, and 24–28 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of Bassin (US 2011/0067005 A1; Mar. 17, 2011) and Hirsave (US 2007/0033445 A1; Feb. 8, 2007).

Claims 6–8, 15–17, and 23 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of Bassin, Hirsave, and Burrell (US 2010/0205673 A1; Aug. 12, 2010).

Subject Matter Eligibility:

ISSUE

Does the preponderance of evidence of record support Examiner’s finding that Appellant’s claimed invention is directed to patent ineligible subject matter?

PRINCIPLES OF LAW

An invention is patent-eligible if it claims a “new and useful process, machine, manufacture, or composition of matter.” 35 U.S.C. § 101. However, the Supreme Court has long interpreted 35 U.S.C. § 101 to include

Appeal 2019-002830
Application 14/251,144

implicit exceptions: “[l]aws of nature, natural phenomena, and abstract ideas” are not patentable. *E.g.*, *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Supreme Court’s two-step framework, described in *Mayo* and *Alice*. *Id.* at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is “directed to.” *See Alice*, 573 U.S. at 219 (“On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk.”); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) (“Claims 1 and 4 in petitioners’ application explain the basic concept of hedging, or protecting against risk.”).

Concepts determined to be abstract ideas, and thus patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 69 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as “molding rubber products” (*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)); “tanning, dyeing, making water-proof cloth, vulcanizing India rubber, smelting ores” (*id.* at 183 n.7 (quoting *Corning v. Burden*, 56 U.S. 252, 267–68 (1853))); and manufacturing flour (*Gottschalk*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Supreme Court held that “[a] claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a

Appeal 2019-002830
Application 14/251,144

mathematical formula.” *Diehr*, 450 U.S. at 176; *see also id.* at 191 (“We view respondents’ claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula.”). Having said that, the Supreme Court also indicated that a claim “seeking patent protection for that formula in the abstract . . . is not accorded the protection of our patent laws, . . . and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment.” *Id.* (citing *Gottschalk and Parker*); *see, e.g., id.* at 187 (“It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.”).

If the claim is “directed to” an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where “we must examine the elements of the claim to determine whether it contains an ‘inventive concept’ sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Alice*, 573 U.S. at 221 (quotation marks omitted). “A claim that recites an abstract idea must include ‘additional features’ to ensure ‘that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].’” *Id.* (quoting *Mayo*, 566 U.S. at 77). “[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention.” *Id.*

The PTO published revised guidance on the application of § 101. USPTO, *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (January 7, 2019) (“Revised Guidance”). Under that guidance, we first look to whether the claim recites:

- (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of

Appeal 2019-002830
Application 14/251,144

organizing human activity such as a fundamental economic practice, or mental processes); and

(2) additional elements that integrate the judicial exception into a practical application (*see* MPEP §§ 2106.05(a)–(c), (e)–(h)).

See Revised Guidance, 84 Fed. Reg. at 54–55. Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then look to whether the claim:

(3) adds a specific limitation beyond the judicial exception that is not “well-understood, routine, conventional” in the field (*see* MPEP § 2106.05(d)); or

(4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

See Revised Guidance, 84 Fed. Reg. at 51.

ANALYSIS

Applying the Revised Guidance to the facts on this record, we find that Appellant’s claims are directed to patent-eligible subject matter.

The Revised Guidance instructs us first to determine whether any judicial exception to patent eligibility is recited in the claim. The Revised Guidance identifies three judicially-expected groupings identified by the courts as abstract ideas: (1) mathematical concepts, (2) certain methods of organizing human behavior such as fundamental economic practices, and (3) mental processes.

Examiner finds that Appellant’s

claims are directed toward informing a user of said tool of at least one action to be executed in said risk segment, if said user agree allowing said tool to execute said risk segment, overriding said risk segment with one or more alternative options, obtaining feedback from said user said risk segment is deemed safe, repeating said executing, informing, allowing, and obtaining steps for plurality of additional risk segments, and

transitioning said system management tool from said risk assessment mode to an automatic mode of operation wherein a given one of said risk segments is conditionally executed until said given one of said risk segments is deemed safe and wherein said given one of said risk segments is automatically executed once said given one of said risk segments is deemed safe wherein said given one of said risk segments is conditionally executed at least once and then is automatically executed at least once . . . , which are considered to be abstract [mental processes].

(Final Act. 17.) In addition, Examiner finds that “the abstract concept of collecting and comparing known information and obtaining and comparing intangible data because the limitations are collecting the data regarding risk management then comparing that data to make a determination of [whether] the risk segments are safe” and “receiving information, analyzing it, and displaying it because risk management data is collected and analyzed to be determined if it is safe to run, where the results are then displayed to a user (e.g. annotating code with risk actions identified)” are abstract concepts, i.e., mental processes (*id.* at 17–18 (citing *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016), *Classen Immunotherapies, Inc. v. Biogen IDEC*, 659 F.3d 1057 (Fed. Cir. 2011), *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011))).

We find no error in Examiner’s finding that Appellant’s claimed invention involves mental processes, an abstract idea.

We note, however, that “[i]n cases involving software innovations, th[e] inquiry often turns on whether the claims focus on ‘the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an abstract idea for which computers are invoked merely as a tool.’” *Finjan, Inc. v. Blue Coat System, Inc.*, 879 F.3d 1299, 1303 (Fed.

Appeal 2019-002830

Application 14/251,144

Cir. 2018) (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016) (internal quotation marks omitted)).

In contrast to Examiner’s analysis, on this record, we find that Appellant’s claimed invention recites additional elements that integrate the judicial exception into a practical application, i.e., an improvement in computer capabilities. Integration into a practical application is evaluated by identifying whether there are additional element individually, and in combination, which go beyond the judicial exception. *See* Revised Guidance, 84 Fed. Reg. 54–55. As explained in the October 2019 Update to Subject Matter Eligibility⁴ “first the specification should be evaluated to determine if the disclosure provides sufficient details such that one of ordinary skill in the art would recognize the claimed invention as providing an improvement” (PEG Update 12). As the PEG Update explains, although the “specification need not explicitly set forth the improvement, . . . it must describe the invention such that the improvement would be apparent to one of ordinary skill in the art” (*id.*).

On this record, Appellant discloses that “[o]ne or more embodiments provide a method for controlled execution of system management tools that identifies and prevents the execution of unsafe code” (Spec. 8:13–14). In this regard, Appellant discloses:

One or more embodiments maximize exploitation of productivity tools while risk assessment is still in progress. At least some instances model risk as a collection of risk actions which, when executed, cause or increase the likelihood that a high-risk system failure occurs. For example, “remove a file known to be relevant for an application when the application is

⁴ Available at https://www.uspto.gov/sites/default/files/documents/peg_oct_2019_update.pdf (last accessed Nov. 15, 2019) (“PEG Update.”)

running,” “reboot a server when users are logged on.” A risk action involves a specific operation and one or more managed resources (or configuration items, CI).

One or more embodiments identify risk conditions, i.e., situations when a risk action is likely to execute, and track whether the action executed or not, providing reports and documentation to support the user in performing risk assessment. If tool execution completes automatically, the [System Administrator (SA)] . . . knows that risk conditions either did not occur on the targeted resources, or that the risk actions corresponding to those conditions had already been validated. In at least some instances, the tool executes in fully automated mode after the tool is validated for all of the materialized risk conditions, and the tool executes in semi-automated mode when it is not validated for all of the risk actions. The SA is provided a description, and possibly emulation, of the risky code segment, and has to decide if execution should proceed or stop. He or she provides feedback on the actual tool level of safety.

One or more embodiments support incremental risk assessment at the granularity of risk conditions. Some risk conditions occur more frequently, while others are rare events. Delaying fully-automated execution until all execution-constraints are validated limits the realization of expected benefits. SAs learn about the degree of risk relative to each risk condition from reports on how the tool executes under risk conditions. SAs can assess the tool as risk-free for some types of risk actions after repeated correct execution. This acknowledges that the tool can execute in fully automated mode when no other risk conditions are materialized.

(*Id.* at 7:6–31; *see also id.* at 5:18–29, 10:1–6, 19:22–20:28, 22:29–23:8.)

In sum, we find that, on this record, Appellant’s claimed invention recites additional elements that integrate the judicial exception into a practical application, i.e., an improvement in computer capabilities (*see generally* Appeal Br. 18 (referring to the “transitioning” step); *see also* Reply Br. 5). *See Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d

Appeal 2019-002830
Application 14/251,144

1143, 1150 (Fed. Cir. 2019) (“software inventions [are] . . . patent-eligible where they have made non-abstract improvements to existing technological processes and computer technology”).

Finding that Appellant’s claims integrate the judicial exception into a practical application concludes the eligibility analysis on this record. Therefore, we need not address the contentions on this record concerning what was, or was not, “well-understood, routine, conventional” in the field. *See generally* Ans.⁵ 18–19; *cf.* Revised Guidance, 84 Fed. Reg. at 51.

CONCLUSION

The preponderance of evidence of record fails to support Examiner’s finding that Appellant’s claimed invention is directed to patent ineligible subject matter. The rejection of claims 1, 2, 4–11, 13–19, and 21–28 under 35 U.S.C. § 101 is reversed.

Obviousness:

ISSUE

Does the preponderance of evidence relied upon by Examiner support a conclusion of obviousness?

FACTUAL FINDINGS (FF)

FF 1. Bassin “relates to a system and method of defect analysis, and more particularly, to a method and system to determine defect risks in software solutions” (Bassin ¶ 2; *see generally* Final Act. 23).

FF 2. Bassin’s “invention is operable to execute [a] risk model,” wherein “the execution of the risk model may be repeated for each stage of the software life cycle” and “testing is performed through each stage of the software lifecycle” (Bassin ¶ 97; *see* Final Act. 24–25).

⁵ Examiner’s December 26, 2018 Answer.

FF 3. Bassin discloses, as an aspect of its invention,

a system implemented in hardware comprises a risk factor receiving (RFR) tool operable to receive one or more risk factors and a context receiving (CR) tool operable to receive: one or more contexts, one or more context relationships and associations of the one or more contexts with the one or more risk factors. Additionally, the system comprises a mapping tool operable to map the one or more risk factors for an associated context to a software defect related risk consequence to determine a risk model and a software break-down (SB) tool operable to break-down software into risk evaluation units. Further, the system comprises a risk annotation tool operable to evaluate and annotate a software solution with selected risk factors for the risk evaluation units and a risk-based testing tool operable to execute a risk-based testing on the software based on the risk model to determine a defect related risk evaluation for a software development project and collect test results and a test process from the risk-based testing.

(Bassin ¶ 11.)

FF 4. Bassin's

system comprises first program instructions to receive one or more risk factors, second program instructions to receive one or more contexts and identify one or more context relationships and third program instructions to associate the one or more contexts with the one or more risk factors. Furthermore, the system comprises fourth program instructions to map the one or more risk factors for an associated context to a software defect related risk consequence to determine a risk model, wherein the mapping the one or more risk factors comprises determining a dimension where the one or more risk factors generates a risk impact. The dimension comprises at least one of a failure possibility dimension, which indicates a likelihood that a defect will occur within a specific context and a failure damage dimension, which indicates a consequence of an occurrence of the defect in production. Additionally, the system comprises fifth program instructions to execute a risk-based testing based on the risk model to determine a defect related risk evaluation for a software development project. The first, second, third,

fourth and fifth program instructions are stored on the computer readable storage media for execution by the CPU via the computer readable memory.

(Bassin ¶ 13.)

FF 5. Bassin’s Figure 13 is reproduced below:

1305	Test Activities	High level requirement or design review	Detailed requirement or design review	Code review	Unit test	System test	System integration test	User acceptance test
1310	Test design reference	Client needs and features	High level requirements or design	Detailed requirement or design, Code	Detailed requirement or design, Code	Application requirement	System requirement, Design	Client needs and features, requirements
1315	Artifacts under test	High level requirement or design	Detailed requirement or design	Code	Code	Application	System	System

FIG. 13

Bassin’s “FIG. 13 shows an exemplary table illustrating the test activities that can be performed, and the related test design reference and artifacts that are the targets under test in accordance with aspects of . . . [Bassin’s] invention” (Bassin ¶ 25; *see also* ¶ 67 (“the steps of the flow diagram[] may be implemented and executed from either a server, in a client server relationship, or they may run on a user workstation with operative information conveyed to the user workstation”); *see* Final Act. 23–25).

FF 6. Bassin “provides a risk analysis system and method, which is orthogonal, defines risk contexts and associates risk factors with those contexts, and dynamically updates risk as project requirements change with the use of actual test results as feedback to adjust and tune throughout the life cycle” (Bassin ¶ 32; *see id.* ¶ 34 (Bassin’s “invention is operable to produce a break-down structure of the software under test, allows a user to map risk factors to different levels of granularity and provides a mechanism for accurately updating risk dynamically”); *see generally* Final Act. 23–24).

FF 7. Bassin’s system “includes a risk annotation tool . . . operable to evaluate and annotate the software solution with the selected risk factors for the risk evaluation units” and “a risk-based testing tool . . . operable to perform risk-based testing using the output of the risk annotation tool” (Bassin ¶¶ 59 and 60; *see* Final Act. 23 and 30).

FF 8. Bassin discloses that the evaluation of risk factors “may be performed manually, or (at least partially) automatically via an expert system” (Bassin ¶ 74; *see* Final Act. 25).

FF 9. Bassin’s “risk annotation tool . . . is operable to evaluate and annotate (or enable a user to evaluate and annotate) the software solution with the selected risk factors for the risk evaluation units” and “assess each risk factor that is associated with each risk evaluation unit, and determine a risk factor value” (Bassin ¶ 104; *see* Final Act. 30).

FF 10. Examiner finds that Bassin does

not specifically disclose if said user agrees, allowing said tool to execute said risk segment, overriding said risk segment with one or more alternative operations, and *once all of said risk segments are deemed safe, transitioning said system management tool from said risk assessment mode to an automatic mode of operation*, and wherein said given one of said risk segments is automatically executed once said given one of said risk segments is deemed safe and then is automatically executed at least once.

(Final Act. 25 (emphasis added).)

FF 11. Hirsave “provides a method, apparatus, and program for automatic risk assessment in a managed computer environment” (Hirsave ¶ 2).

FF 12. Hirsave discloses a method that “automatically assesses the risk of installing [a] patch on a managed endpoint” (Hirsave ¶ 19; *see* Final Act. 25–26).

FF 13. Hirsave discloses a method, wherein “[b]ased on the risk assessment . . . [the] managing server . . . can apply [a] patch immediately, schedule deployment of the patch for a later time, or notify the administrator of a high risk so the administrator may take appropriate measures” (Hirsave ¶ 35; *see also id.* ¶ 38 (Hirsave discloses that a “low risk [assessment] may indicate that the patch can be installed immediately without significantly affecting productivity of the managed endpoint”); *id.* ¶ 46 (Hirsave discloses that “[a] policy may specify that when a patch having a medium risk is deployed, the patch may be installed immediately with a notification being sent to the administrator so the administrator may monitor completion of the patch”); *see* Final Act. 25–26).

FF 14. Examiner finds that the combination of Bassin and Hirsave does not specifically disclose for each line of code in said system management tool, identifying actions based on specifications in a supporting database, and identifying configuration items related to said actions based on a recorded action model and for each set of consecutive ones of said actions and its related configuration items, determining risk actions defined in said supporting database, analyzing an annotated code to determine said risk segments as groups of consecutive risk actions and adjoining non-risk business processes and grouping said risk actions in to different ones of said risk segments and to group said risk actions with said adjoining non-risk code and annotating said code with said risk segments.

(Final Act. 31.)

FF 15. Burrell relates to a method of examining vulnerable areas of source code to identify “areas that are actually safe,” wherein “safe areas are filtered from the universe of code that receives security mitigations” and “[t]he remaining code receives security mitigations appropriate to the level of risk of the code” (Burrell, Abstract; *see* Final Act. 32).

FF 16. Burrell discloses that

identified areas of source code and identified variables may be classified into categories of risk (e.g., high risk, medium risk, low risk and no risk or other risk classification system) Varying levels of code protection may be inserted in an area of code based on the risk classification level of the area of source code. Risk determinations may be based on a combination of symbol allocation size, type and structure. . . . [A]reas within the identified areas are examined to determine if some of those areas do not need insertion of security mitigating code, that is, to identify areas that are safe. The universe of vulnerable source code is filtered to remove the areas that have been identified as not needing security mitigation code insertion, thereby creating a remaining subset of source code that will be mitigated.

(Burrell ¶ 29; *see* Final Act. 31–32.)

ANALYSIS

The rejection over the combination of Bassin and Hirsave:

Based on the combination of Bassin and Hirsave, Examiner concludes that, at the time Appellant’s invention was made, it would have been *prima facie*,

obvious to one of ordinary skill in the art at the effective filing date of the claimed invention to have modified the teachings of Bassin . . . to incorporate the teachings as taught by Hirsave . . . in order to ensure risk is being analyzed properly thereby ensuring accuracy of the results.

(Final Act. 27.) We are not persuaded.

We agree with Examiner’s finding that Bassin and Hirsave both disclose methodology for identifying risk associated with software (*see generally* FF 1 and 11). We note, however, that Appellant’s independent claims require, *inter alia*, that a management tool is executed with a risk assessment mode enabled and then, after all risk segments are deemed safe, the system management tool is transitioned from a risk assessment mode to

Appeal 2019-002830
Application 14/251,144

an automatic mode of operation (*see* Appeal Br. 42 (Appellant’s independent claim 1); *see also id.* at 42–43 (Appellant’s independent claim 10); *id.* at 46–47 (Appellant’s independent claim 18); *id.* at 49–50 (Appellant’s independent claim 25)).

Examiner acknowledges that Bassin does not disclose, *inter alia*, a method, wherein “once all of said risk segments are deemed safe, transitioning said system management tool from said risk assessment mode to an automatic mode of operation” (FF 10). To make up for this deficiency in Bassin, Examiner relies on Hirsave’s disclosure of a system, wherein, based on the risk assessment, a managing server either applies a patch immediately, schedules deployment of a patch at a later time, or notifies an administrator to take appropriate measures (FF 13). According to Examiner, Hirsave discloses that a patch may be installed automatically, i.e., immediately, when the system detects a low risk (*see* Ans. 15–16).

Although Examiner’s rationale may be correct as to the automatic installation of a patch after a low risk assessment is made, Examiner failed to establish that this evidence supports a conclusion that the combination of Bassin and Hirsave suggests transitioning a management tool from a risk assessment mode to an automatic mode of operation after all risk segments are deemed safe as required by Appellant’s claimed invention. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992) (“[E]xaminer bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.”).

Thus, we find that the weight of evidence falls in favor of Appellant’s contention that although

Hirsave discuss[es] automatically assessing the risk associat[ed] with a patch, such that a patch with a low risk may be installed

Appeal 2019-002830
Application 14/251,144

immediately . . . , the skilled artisan would not glean, in this context, the concept of transitioning from risk assessment mode (e.g., with conditional execution) to an automatic mode of operation once all risk segments are deemed safe.

(Appeal Br. 32–33; *see also* Reply Br. 17–18)

Therefore, we find that Examiner failed to establish an evidentiary basis to support a conclusion with respect to Appellant’s claims 1, 2, 4, 5, 9–11, 13, 14, 18, 19, 21, 22, and 24–28.

The rejection over the combination of Bassin, Hirsave, and Burrell:

Appellant’s claims 6–8 depend directly or indirectly from Appellant’s independent claim 1. Appellant’s claims 15–17 depend directly or indirectly from Appellant’s independent claim 10. Appellant’s claim 23 depends directly or indirectly from Appellant’s independent claim 18.

Based on the combination of Bassin, Hirsave, and Burrell, Examiner concludes that, at the time Appellant’s invention was made, it would have been *prima facie*

obvious to one of ordinary skill in the art at the effective filing date of the claimed invention to have modified the teachings of Bassin . . . in view of Hirsave . . . to incorporate the teachings as taught by Burrell . . . in order to better represent areas of risk thereby ensuring the areas of risk are addressed.

(Final Act. 32.)

Examiner failed to establish an evidentiary basis on this record to support a conclusion that Burrell makes up for the deficiency in the combination of Bassin and Hirsave discussed above (*see* FF 15–16). *See In re Oetiker*, 977 F.2d at 1445 (“[E]xaminer bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.”). Therefore, we find that the weight of the evidence on this

record falls in favor of Appellant’s contention that “Bassin, alone or in combination with Burrell, fails to remedy the above issues related to Hirsave in the context of the presently claimed invention” (Appeal Br. 33; *see also* Reply Br. 18).

CONCLUSION

The preponderance of evidence relied upon by Examiner fails to support a conclusion of obviousness.

The rejection of claims 1, 2, 4, 5, 9–11, 13, 14, 18, 19, 21, 22, and 24–28 under 35 U.S.C. § 103(a) as unpatentable over the combination of Bassin and Hirsave is reversed.

The rejection of claims 6–8, 15–17, and 23 under 35 U.S.C. § 103(a) as unpatentable over the combination of Bassin, Hirsave, and Burrell is reversed.

DECISION SUMMARY

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 2, 4–11, 13–19, 21–28	101	Eligibility		1, 2, 4–11, 13–19, 21–28
1, 2, 4, 5, 9–11, 13, 14, 18, 19, 21, 22, 24–28	103	Bassin, Hirsave		1, 2, 4, 5, 9–11, 13, 14, 18, 19, 21, 22, 24–28
6–8, 15–17, 23	103	Bassin, Hirsave, Burrell		6–8, 15–17, 23
Overall Outcome				1, 2, 4–11, 13–19, 21–28

REVERSED