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.
14/865,136	09/25/2015	Brian J. Skerry	P74345	9799

96162 7590 11/13/2019

Law Office of R. Alan Burnett, PS
c/o CPA Global
900 Second Avenue South, Suite 600
Minneapolis, MN 55402

EXAMINER	
SCHEIBEL, ROBERT C	

ART UNIT	PAPER NUMBER
2467	

NOTIFICATION DATE	DELIVERY MODE
11/13/2019	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

alan@patentlylegal.com
docketing@cpaglobal.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte BRIAN J. SKERRY, THOMAS M. SLAIGHT, REN WANG, and KAPIL SOOD

Appeal 2018-009081
Application 14/865,136
Technology Center 2400

Before CAROLYN D. THOMAS, MICHAEL J. STRAUSS, and NABEEL U. KHAN, *Administrative Patent Judges.*

STRAUSS, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE[1]

Pursuant to 35 U.S.C. § 134(a), Appellant[2] appeals from the Examiner's decision to reject claims 1, 2, and 4–25. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part and enter a new ground of rejection pursuant to 37 C.F.R. § 41.50(b).

CLAIMED SUBJECT MATTER

The claims are directed to securely measuring end-to-end quality of service in a network. Spec., Title. Claims 1 and 14, reproduced below, are illustrative of the claimed subject matter:

> 1. A method for securely measuring end-to-end Quality of Service (QoS) in a network, comprising:
>
> at a first physical Ethernet controller or physical Network Interface Controller (NIC) at a first endpoint,
>
> detecting a first packet marked for QoS measurement;
>
> generating, using a tamper-resistant secure clock, a first timestamp for the first packet;
>
> determining packet identifying metadata for the first packet;
>
> reporting the first timestamp and the packet identifying metadata for the first packet to an external monitor;
>
> at a second physical Ethernet controller or physical NIC a second endpoint,

[1] We refer to the Specification, filed September 25, 2015 as amended June 29, 2017 ("Spec."); Final Office Action, mailed August 29, 2017 ("Final Act."); Appeal Brief, filed May 8, 2018 ("Appeal Br."); Examiner's Answer, mailed July 27, 2018 ("Ans."); and Reply Brief, filed September 25, 2018 ("Reply Br.").

[2] 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 Intel Corporation. Appeal Br. 3.

detecting the first packet is marked for QoS measurement;

generating, using a tamper-resistant secure clock, a second timestamp for the first packet;

determining packet identifying metadata for the first packet;

reporting the second timestamp and the packet identifying metadata for the first packet to the external monitor; and

employing the first and second timestamps and the packet identifying metadata for the first packet to measure a latency incurred by the first packet from the first endpoint to the second endpoint.

14. An Ethernet controller, comprising:

a plurality of ports including input ports and output ports;

one of a secure clock or an interface for receiving timestamp data generated by a secure clock;

an interface for communicating with an external monitor when the Ethernet controller is operating; and

embedded logic configured to perform operations when the Ethernet controller is operating, including,

in response to receiving a first packet at a first port,

detecting the first packet is marked for QoS measurement;

generating, using the secure clock, a first timestamp for the first packet or receiving a first timestamp for the first packet via the interface for receiving timestamp data generated by a secure clock;

determining packet identifying metadata for the first packet;

reporting the first timestamp and the packet identifying metadata for the first packet to the external monitor;

at a second port,

detecting the first packet is marked for QoS measurement;

generating, using the secure clock, a second timestamp for the first packet or receiving a second timestamp

for the first packet via the interface for receiving timestamp data generated by a secure clock;

determining packet identifying metadata for the first packet;

reporting the second timestamp and the packet identifying metadata for the first packet to the external monitor,

wherein the first and second timestamps and the packet identifying metadata for the first packet are configured to enable the external monitor to measure a latency incurred by the first packet as it traverses a packet processing path between the first port and the second port.

REFERENCES [3]

The prior art relied upon by the Examiner is:

Name	Reference	Date
Ghose et al.	US 2013/0329584 A1	Dec. 12, 2013
Newell	US 2015/0012737 Al	Jan. 8, 2015
Patwardhan et al.	US 2015/0089082 A1	Mar. 26, 2015
Djukic	US 2016/0301579 Al	Oct. 13, 2016
Yadav et al.	US 2016/0359872 Al	Dec. 8, 2016

REJECTIONS

Claims 1, 2, 4–8, and 10–13 stand rejected under 35 U.S.C. § 103 as being unpatentable over Ghose, Yadav, and Newell. Final Act. 4–10.

Claims 14–19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Ghose and Patwardhan. Final Act. 10–14.

Claims 20 and 22–25 stand rejected under 35 U.S.C. § 103 as being unpatentable over Ghose, Patwardhan, and Newell. Final Act. 14–19.

Claim 9 stands ejected under 35 U.S.C. § 103 as being unpatentable over Ghose, Yadav, Newell, and Djukic. Final Act. 19.

[3] All citations herein to these references are by reference to the first named inventor only.

Claim 21 stands rejected under 35 U.S.C. § 103 as being unpatentable over Ghose, Patwardhan, Newell, and Djukic. Final Act. 19–20.

ANALYSIS

Claims 1, 2, 4–13, and 20–25

In connection with claims 1, 2, 4–13, and 20–25, and except as otherwise noted, we adopt as our own (1) the findings and reasons set forth by the Examiner in the action from which this appeal is taken (Final Act. 2–21) and (2) the reasons set forth by the Examiner in the Examiner's Answer in response to Appellant's Appeal Brief (Ans. 3–11) and concur with the conclusions reached by the Examiner. We highlight the following for emphasis.

In rejecting independent claim 1, the Examiner finds Ghose teaches or suggests all of the recited limitations except (i) "Ghose does not disclose expressly the limitation that the method steps are performed at a first/second physical Ethernet controller or physical Network Interface Controller (NIC) at the first/second endpoints" (Final Act. 6, hereinafter the "physical controller" limitation) and (ii) "that the clock used to generate the timestamps is a tamper-resistant secure clock" (*id.* at 7, hereinafter the "secure clock" limitation). The Examiner addresses the first noted deficiency of Ghose, finding Yadav's disclosure of a network capture agent implemented within a physical NIC teaches the physical controller limitation. *Id.* at 6. The Examiner further finds Newell's "root-of-trust" clock teaches the secure clock limitation. *Id.* at 7.

Appellant's first contention of error is that the Examiner's claim interpretation in connection with the application of Ghose's NIC is overly broad. Appeal Br. 12. In particular, Appellant argues a physical controller is

a hardware device and is distinguishable over virtual controllers or virtual NICs implemented in software operating on a host platform. *Id.* at 12–13. "Any way you look at it, a virtual NIC [as taught by Ghose] is implemented via the execution of software on a host platform and would not be considered by a [person having ordinary skill in the art] . . . to be a physical hardware device." *Id.* at 13.

The Examiner responds, finding Appellant's argument does not address the rejection. Ans. 4. "Although [the] Examiner notes that even a virtual Ethernet controller or virtual Network Interface Controller is implemented in a physical device as indicated in Ghose, the rejection is based on modifying Ghose with Yadav to use an agent on a physical network interface card." *Id.*

Appellant's contention is unpersuasive for lack of sufficient evidence the physical controller limitation requires specific functionalities be included in hardware rather than in software or that the recited functionalities be directly implemented in hardware rather than in a virtual environment and, therefore, only indirectly in hardware. Appellant's citation to definitions attributable to Microsoft[4] and the IBM Knowledge Center[5] (Appeal Br. 12–13) are unhelpful[6] in delineating between what one skilled in the art at the

[4] "A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface, and by similar terms) is a computer hardware component that connects a computer to a computer network."
[5] "A physical network interface is the network adapter. A network adapter is a piece of hardware dedicated to capturing and pre-processing data packets arriving at a host computer."
[6] Appellant's belated citation to Wikipedia for still another definition (Reply Br. 20) is likewise unpersuasive.

time of the invention would have understood to be and what is not a *physical* NIC. For example, neither definition explains whether the interfaces are exclusively hardware or some combination of hardware and software and/or firmware. Standing alone, Appellant's arguments and conclusory statements, which are unsupported by factual evidence, are entitled to little probative value. *In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997); *In re De Blauwe*, 736 F.2d 699, 705 (Fed. Cir. 1984). Attorney argument is not evidence. *In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974). Nor can such argument take the place of evidence lacking in the record. In contrast to Appellant's argument, the Examiner finds

> Ghose clearly discusses measurements from a physical network. For example, in the summary, Ghose describes the invention as a system which "provides techniques for determining latency in a physical network that includes a number of network devices over which packets travel" (Ghose, para. 0004). The latency information is used to identify issues in the physical network ("[u]sing a collection of such latency information, the virtual network controller can identify places in the physical network that are slow or where bottlenecks in traffic are occurring" (Ghose, para. 0006)).

Ans. 4 (emphasis omitted). For the reasons discussed, and in the absence of sufficient evidence that the recited physical controller limitation is entitled to a narrow construction, we conclude a reasonable but broad interpretation of the limitation includes an Ethernet or NIC controller that (i) is implemented directly or indirectly using hardware alone or in combination with software and/or firmware; or (ii) supports (i.e., provides services to or integrates with) a physical network. Under either of these definitions, Ghose teaches or suggests the physical controller limitation.

Furthermore, Appellant's argument is unpersuasive because, as explained by the Examiner, the rejection relies on Yadav for teaching the physical controller limitation. Ans. 5. In effect, Appellant's argument is an attack on Ghose individually when the rejection is based on the combination of Ghose, Yadav, and Newell. "Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

Appellant further contends the combination of references is improper because "the Examiner makes conclusory statements based on inadequate evidence, and does not explain how Ghose, Yadav[,] and Newell would be combined to obtain the inventions claimed herein, nor why a PHOSITA would have a reasonable expectation of success in making such a combination." Appeal Br. 19 (emphasis omitted). In connection with Ghose, Appellant quotes the various paragraphs of the reference cited by the Examiner and concludes there is neither motivation to provide a physical controller nor a reasonable expectation of succeeding in making the modification. *Id.* at 23. Appellant makes similar arguments in connection with modifying Ghose to include Yadav's physical NIC. *Id.* at 24.

The Examiner responds, finding Ghose routes packets and detects latency issues in a physical network including physical devices. Ans. 6. The Examiner finds Yadav discloses a similar type of data center using sensor or network capture agents on physical network gear installed as part of a physical network switch or NIC. *Id.* at 7. The Examiner provides two alternative reasons for combining the references. First, the Examiner finds

modifying Ghose's virtual NIC implementation to use Yadav's physical or hardware implementation is a "[s]imple substitution of one known element for another to obtain predictable results." *Id.* (citing MPEP § 2143; *see also KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (holding that it is likely obvious to apply a known technique to "improve similar devices in the same way".)) Secondly, the Examiner finds a reason to install Ghose's agents on Yadav's physical NICs is to provide additional data with which to identify physical network problems. *Id.*

Appellant's contention is unpersuasive of reversible Examiner error. Appellant provides insufficient evidence or reasoned argument that the subject technology, i.e., computer networks, is unpredictable or that there was no reasonable expectation of success in making the combination. In contrast, the Examiner has articulated reasoning with rational underpinnings sufficient to justify the legal conclusion of obviousness. Final Act. 6–7, Ans. 7–8. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds . . . must [include] . . . some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."), *cited with approval in KSR*, 550 U.S. at 418.

Appellant further contends Newell fails to teach the secure clock limitation, arguing, rather than being secure or tamper-resistant, Newell's clock merely detects tampering after the fact. Appeal. Br. 27. Appellant further argues the monitored clocks are separate from and are not part of Newell's field programmable gate array (FPGA). *Id.* Appellant still further argues Newell's clock cycle is neither a clock nor related to a timestamp. *Id.* Appellant also argues the Examiner's stated motivation for combining the references is deficient. *Id.*

The Examiner responds, finding the secure clock limitation is not specifically defined and is broadly and "reasonably . . . interpreted to include all clocks which are *not* easily tampered with and insecure." Ans. 8. The Examiner further finds "a clock which detects tampering [as is taught by Newell] is reasonably interpreted as a tamper-resistant clock because the ability to detect tampering will deter tampering." *Id.* The Examiner further disagrees there is insufficient motivation to combine Newell, Ghose, and Yadav, finding "[i]t would have been obvious to consider different types of clocks and to select a more tamper-resistant and secure type if not cost prohibitive to increase the system reliability." *Id.*

Appellant replies, arguing Ghose is concerned with identifying bottlenecks in a network using timestamps that, according to the Examiner, are reliable. Reply Br. 16. In such a benign environment, Appellant argues "[w]hy would it matter whether the timestamps were obtained using a tamper-resistant secure clock or an ordinary clock capable of generating timestamps?" *Id.* In contrast, according to Appellant, the claimed invention is directed to securely measuring end-to-end QoS performance where there is an enhanced need to maintain a high level of security. *Id.* at 16–17.

Appellant's contention is unpersuasive of reversible Examiner error. Although the Specification does not include a specific definition for a "tamper-resistant secure clock," it discloses

> the main functionality provided by the secure clock is a "tamper proof" way of getting a reliable measure of time. Such a hardware-based secure clock *usually* has a power backup that keeps it going, and the time cannot be adjusted on the platform without proper authorization (or possibly not adjusted at all).

Spec. ¶ 55 (emphasis added). The Specification continues, disclosing "[i]n case of physical tampering, some secure clocks can detect physical tampering and be disabled by associated logic circuitry." That is, a secure clock provides a tamper proof functionality that usually (i.e., does not necessarily) inhibit unauthorized time adjustment and may detect tampering so as to disable associated circuitry. Thus, Newell's clock that detects tampering (i.e., one of the disclosed functions of Appellant's secure clock) teaches or suggests a secure clock.

Claim 1 further prefaces the secure clock as being "tamper-resistant" (notably, not "tamper-proof"). Although the Specification does not include a formal definition of "tamper-resistant" it discloses "since the source of the timestamp data is secure and tamper-resistant, there is no way that the clock data can be compromised." Spec. ¶ 69. Although inhibiting unauthorized clock adjustments preemptively prevents compromising clock data, so does detecting unauthorized adjustments to detect comprised clock data, although the latter does it reactively. Accordingly, under a broad but reasonable interpretation, Newell's tamper-resistant clock in combination with Ghose's clock used for generating a timestamp teaches or suggests the disputed tamper-resistant secure clock.

We are also unpersuaded by Appellant's argument Newell's monitored clocks are separate from and are not part of Newell's field programmable gate array (FPGA). Appeal Br. 27. Newell is relied upon only for teaching a tamper-resistant clock such that the combination of Ghose's clock used for generating a timestamp and Newell's secure clock teach or suggest the secure clock limitation. Likewise, Appellant's

argument that Newell's clock cycle is not related to a timestamp (*id.*) is unpersuasive as Ghose, not Newell, is cited for the timestamp limitation.

We are also unpersuaded the Examiner's motivation for combining Ghose and Newell is inadequate to support the rejection under 35 U.S.C. § 103. That the Examiner's reason for combining the cited references is not the same as Appellant's reason for combining them is insufficient to establish reversible error. *KSR*, 550 U.S. at 420 (explaining that any need or problem known in the art can provide a reason for combining the elements in the manner claimed). *See also In re Kemps*, 97 F.3d 1427, 1430 (Fed. Cir. 1996) (the motivation or reason to combine the prior art references need not be the same as that of applicants). Here, in the absence of sufficient argument to the contrary, we find the Examiner has articulated reasoning with rational underpinnings sufficient to justify the legal conclusion of obviousness. Final Act. 7, Ans. 8. For similar reasons, we are unpersuaded the Examiner erred in rejecting claims 9 and 21 over combinations of Ghose, Yadav (claim 9) and Patwardhan (claim 21), Newell, and Djukic. Appeal Br. 44–45; *cf.* Final Act. 19–20; Ans. 10–11.

Claims 14–19

In connection with claims 14–19, the Examiner finds Ghose teaches the limitations of independent claim 14 but does not expressly disclose the steps of Ghose's method are "performed by an Ethernet controller comprising a plurality of ports including input ports and output ports or the limitation that the latency is measured between a first and second port on the Ethernet controller." Final Act. 12 (emphasis omitted). To cure this deficiency, the Examiner finds Patwardhan's virtual switch (DVS) 14

includes the recited plurality of input and output ports. *Id.* According to the Examiner, "it would have been obvious . . . to modify Ghose to use a DVS as disclosed by Patwardhan and similarly measure the latency of packets processed by [Patwardhan's] DVS . . . to provide increased configurability and flexibility in optimizing network performance by an operator." *Id.* at 12–13. Notably, the "secure clock" of claim 14 is not a *tamper-resistant* secure clock as recited by claim 1. Accordingly, the Examiner omits the Newell reference in the rejection of claims 14–19.

Appellant contends Ghose fails to teach or suggest a secure clock, presenting argument similar to that presented in connection with claim 1 and discussed above. Appeal Br. 34–35. The Examiner responds:

> [M]easurements are assumed reliable and thus the clock is secure. Appellant argues that this merely discloses a reliable and not a secure clock. Examiner respectfully disagrees. The claim phrase "secure clock" is quite broad and reasonably describes the class of clocks including all clocks that are not "insecure". Many clocks fall into the category of "secure clock". If a system relies upon the measurements taken by a clock for critical processing, it is reasonable to assume that the clock is physically (and otherwise) secure. A clock that is physically (or otherwise) insecure and relatively likely to fail as a result would not be reasonably categorized as a "secure clock". However, [the] Examiner maintains that many clocks used for purposes of obtaining critical latency measurements are reasonably secure.

Ans. 9. According to the Examiner, Appellant's arguments improperly attempt to read details about the secure clock from the Specification into the claims. *Id.*

Appellant's contention is persuasive of Examiner error. Although the term "secure clock" taken out of context might otherwise be broadly construed as alleged by the Examiner, it must be interpreted in light of

Appellant's Specification. In particular, during examination, claims are to be given their broadest reasonable interpretation consistent with the specification, and the language should be read in light of the Specification as it would be interpreted by one of ordinary skill in the art. *In re Amer. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations omitted). However, "[e]ven when guidance is not provided in explicit definitional format, 'the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the [disclosure] . . . documents."' *Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1300 (Fed. Cir. 2004) (internal single quotation marks and citations omitted).

As discussed above in connection with claim 1, Appellant discloses several features indicative of a secure clock including being tamper-proof and having the ability to detect tampering. *See, e.g.*, Spec. ¶ 55. Based on this interpretation, we agree with the Examiner in finding the combination of Ghose *and Newell* teach or suggest, not only a secure clock, but a tamper-resistant secure clock. However, because the rejection of claim 14 does not include Newell, it is deficient in teaching or suggesting the argued secure clock. In particular, the Examiner provides insufficient evidence Ghose's clock exhibits any features, characteristics, or functionality that would make it a *secure* clock. Although, as argued by the Examiner, "measurements are assumed reliable" (Ans. 9), that assumption neither makes the measurements reliable in fact nor does the assumption of reliability render a clock secure in fact. Therefore, absent application of the Newell reference, the Examiner fails to provide sufficient persuasive evidence that Ghose standing alone teaches or suggests a secure clock. Accordingly, we do not sustain the

Examiner's rejection of claim 14 under 35 U.S.C. § 103 as being unpatentable over Ghose and Patwardhan or the rejection of claims 15–19 which stand with claim 14.

NEW GROUND OF REJECTION
35 U.S.C. § 103(a)

Pursuant to our authority under 37 C.F.R. § 41.50(b), we reject claims 14–19 under 35 U.S.C. § 103(a) as being obvious over Ghose and Patwardhan further in view of Newell. The combination of Ghose and Patwardhan teaches or suggests the limitations of claims 14–19 as set forth in the Final Action at pages 10–14 except for the requirement of a secure clock.

Ghose discloses timestamp information indicating a time a packet was processed by the network device. Ghose ¶ 5. According to Ghose, the timestamp information is sent by the network device to an analytics engine for determining the time taken by specific packets to traverse the physical network. *Id.* Ghose further discloses "[n]ear consistency of the timestamp is assumed to allow the clock drifts." Ghose ¶ 81. One skilled in the art at the time of the invention would have understood the timestamp is generated by a clock.

Newell discloses a root of trust chip that detects clock tampering including on-chip oscillator 56 that provides a secure clock source (46) and detection of clock tampering (54). Newell ¶¶ 21, 34, 39, 47. Appellant discloses a secure clock that is tamper proof and has the ability to detect tampering. Accordingly, consistent with Appellant's Specification, Newell's on-chip oscillator teaches a secure clock. At the time of the invention, it would have been obvious to one of ordinary skill in the art to

modify Ghose to utilize a secure clock source as taught by Newell. The rationale for doing so would have been to improve the tamper resistance of the timestamping hardware as taught by Newell.

We are unpersuaded by and herein address Appellant's other arguments that the rejection of claim 14 is improper. In particular, Appellant contends Patwardhan discloses a distributed virtual switch including virtual Ethernet modules, not Ethernet controllers as claimed. Appeal Br. 33. Appellant argues "[i]f the scope of claim 14 was intended to cover a virtual Ethernet controller, the term 'virtual' would be used in either the independent claim (14), or a dependent claim would include a limitation such as, 'wherein the Ethernet controller is a virtual Ethernet controller.'" *Id.* at 34. Appellant concludes, in the absence of such a limitation, "the intent of the claim [14] limitation 'Ethernet controller' is directed toward a physical Ethernet controller." *Id.* Appellant argues "[t]he present application clearly distinguished between embedded logic implemented in hardware, such as an Ethernet controller, and a virtual switch implemented in software." *Id.* at 36 (citing Spec. ¶¶ 31–33). Appellant further argues the Examiner's stated motivation for combining the references is deficient because "[the] alleged motivation is entirely unrelated to the purpose of the claimed invention of claim 14." *Id.* at 39.

The Examiner responds finding that, because Ghose's and Patwardhan's devices control Ethernet functionality, they are interpreted as Ethernet controllers. Ans. 9. The Examiner dismisses Appellant's argument attempting to distinguish the claims over the prior art's software embodiment implemented by a hardware processor, finding Appellant's argument is not commensurate in scope with the claim. *Id.* "Nothing in the

claim requires that the controllers are conventional Ethernet controllers as there is no claimed structure besides the input and output ports, a secure clock (or interface to a secure clock), and an interface for communicating. All of this is taught by Ghose and Patwardhan." *Id.* The Examiner addresses Appellant's argument that the prior art fails to disclose embedded hardware-based logic, arguing Appellant is improperly attempting to read limitations from the Specification into the claims. *Id.* at 10.

Appellant's contentions are unpersuasive. Appellant fails to provide sufficient evidence or reasoning to persuade us the Examiner's interpretation of the recited Ethernet controller is improper. Furthermore, the argued Ethernet controller term as recited in the preamble of the claim is merely a non-limiting name representing the collection of elements recited in the body of claim 14. That is, the claimed Ethernet controller is completely and entirely defined by the recited limitations. It would be improper to import additional limitations from the Specification into the claim including, for example, an overall physical structure of the controller as argued and, in particular, the exclusion of software elements. Furthermore, even if otherwise, Appellant fails to explain why functionality provided by a virtual Ethernet controller according to the prior art is not applicable to and therefore teaches or suggests functionality that can be provided in whole or in part by hardware.

We also find unpersuasive Appellant's argument the Examiner's reason for combining the references is deficient because the motivation is unrelated to the purpose of Appellant's invention. *Kemps*, 97 F.3d at 1430 (the motivation or reason to combine the prior art references need not be the same as that of applicants).

Because we find Newell cures the noted deficiency of Ghose and Appellant's other arguments alleging the rejection of claim 14 to be improper are unpersuasive, we reject claim 14 under 35 U.S.C. § 103(a) as being obvious over Ghose and Patwardhan further in view of Newell.

In addition to arguing the rejection of independent claim 14, Appellant argues the rejection of dependent claim 15 is improper. Appeal Br. 39–40. Claim 15 recites "[t]he Ethernet controller of claim 14, wherein the embedded logic includes at least one processor and memory to store instructions configured to be executed by the at least one processor to effect the operations." The Examiner finds Ghose's computing device 190 including processor(s) 200 and storage device(s) 208 depicted in Figure 8 teach or suggest the limitations of claim 15. Final Act. 13. Appellant contests the rejection, arguing the Examiner's finding is inconsistent with the position taken in connection with claim 14:

> In the rejection of claim 14, the Examiner asserts that the software is the embedded logic (either the virtual network controller of Ghose or the virtual Ethernet modules of Patwardhan, both of which are software): "the broadest reasonable interpretation of embedded logic includes logic embedded within software as well as logic embedded in hardware." But to be consistent with claim 15, the software (which is alleged to meet the embedded logic limitation in claim 14) would need to include at least one processor and memory. That is a physical impossibility – software isn't a physical entity to begin with.

Appeal Br. 39–40 (emphasis omitted).

Appellant's contention is unpersuasive. As recognized by Appellant, it is the Examiner's position that embedded logic includes logic embedded within software as well as in hardware. Thus, the Examiner's position does

not exclude hardware from the definition of embedded logic, e.g., in combination with software. Thus, we see no inconsistency in the Examiner's position regarding the embedded logic of claims 14 and 15.

Appellant does not provide separate argument in connection with dependent claims 16–19. Accordingly, we reject claims 15–19 under 35 U.S.C. § 103(a) as being obvious over Ghose and Patwardhan further in view of Newell as applied above in connection with claim 14 and as further applied by the Examiner in the Final Action at pages 13–14, adopting the Examiner's findings and reasons as our own.

CONCLUSION

We affirm the Examiner's decision to reject claims 1, 2, and 4–13, and 20–25 under 35 U.S.C. § 103(a).

We reverse the Examiner's decision to reject claims 14–19 under 35 U.S.C. § 103(a).

Pursuant to our discretionary authority under 37 C.F.R. § 41.50(b), we newly reject claims 14–19 under 35 U.S.C. § 103(a) as being unpatentable over Ghose, Patwardhan, and Newell.

Rule 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review." 37 C.F.R. § 41.50(b) also provides:

> When the Board enters such a non-final decision, the [A]ppellant, within two months from the date of the decision, must exercise one of the following two options with respect to the new ground[s] of rejection to avoid termination of the appeal as to the rejected claims:
>
> (1) *Reopen prosecution*. Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered

> by the examiner, in which event the prosecution will be remanded to the examiner. The new ground[s] of rejection [are] . . . binding upon the examiner unless an amendment or new Evidence not previously of Record is made which, in the opinion of the examiner, overcomes the new ground[s] of rejection designated in [this] . . . decision. Should the examiner reject the claims, appellant may again appeal to the Board pursuant to this subpart.
>
> (2) *Request rehearing*. Request that the proceeding be reheard under §41.52 by the Board upon the same Record. The request for rehearing must address any new ground of rejection and state with particularity the points believed to have been misapprehended or overlooked in entering the new ground of rejection and also state all other grounds upon which rehearing is sought.

Further guidance on responding to a new ground of rejection can be found in the Manual of Patent Examining Procedure § 1214.01 (9th Ed., Rev. 08.2017, Jan. 2018).

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**	**New Ground**
1, 2, 4–8, 10–13	103	Ghose, Yadav, Newell	1, 2, 4–8, 10–13		
14–19	103	Ghose, Patwardhan		14–19	
14–19	103	Ghose, Patwardhan, Newell			14–19
20, 22–25	103	Ghose, Patwardhan, Newell	20, 22–25		
9	103	Ghose, Yadav, Newell, Djukic	9		
21	103	Ghose, Patwardhan, Newell, and Djukic	21		
Overall Outcome			1, 2, 4–13, 20–25	14–19	14–19

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2017).

AFFIRMED-IN-PART; 37 C.F.R. § 41.50(b)