

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

HEADWATER RESEARCH LLC,

Patent Owner

IPR2026-00271

Patent No. 9,491,564

PATENT OWNER'S PRELIMINARY RESPONSE TO THE PETITION

TABLE OF CONTENTS

I.	Introduction	1
II.	Overview of the '564 Patent	2
III.	Level of Ordinary Skill in the Art	6
IV.	Claim Construction	7
V.	The Petition fails to establish a reasonable likelihood of success with respect to any challenged claim.....	7
A.	The Petition's Ground 1 fails to show the obviousness of independent claims 1 and 14.....	8
1.	The Petition's combination does not satisfy the requirement of "allowing access to the bus only for software components identified by the access authorization information."	9
2.	The Petition offers no obviousness rationale to arrive at the claim requirements.	17
B.	The Petition's Grounds 2A, 2B, and 2C likewise fail.	20
VI.	Conclusion	21

TABLE OF AUTHORITIES

Cases

<i>Xerox Corp. v. ByteMark, Inc.</i> , IPR2022-00624, Paper 12 (PTAB Feb. 10, 2023)	11
--	----

Statutes

37 C.F.R. § 42.108(c)	11
-----------------------------	----

PATENT OWNER'S EXHIBIT LIST

No.	Description
2001	Confidential License Agreement
2002	March 20, 2026 text order regarding motion to dismiss Google's declaratory judgment complaint in <i>Google LLC v. Headwater Research LLC</i> , No. 3:26-CV-01460 (N.D. Cal)
2003	Headwater Research LLC's Opposition to Google's Motion for Leave to File Amended Answer and Counterclaims, <i>Google LLC v. Headwater Research LLC</i> , No. 3:26-CV-01460 (N.D. Cal. Apr. 9, 2026)
2004	U.S. Patent No. 10,140,827, issued to Google LLC
2005	U.S. Patent App. Pub. No. 2010/0192212
2006	Declaration of Dr. Michael C. Brogioli in Support of Patent Owner's Response
2007	<i>Curriculum Vitae</i> of Dr. Michael C. Brogioli
2008	Computer Desktop Encyclopedia, Alan Freedman, The Computer Language Company Inc. (1996)

I. Introduction

The Petition fails to establish a reasonable likelihood of success because it does not address a requirement present in every challenged claim. Both independent claims (claims 1 and 14) require an inter-process software communication bus that provides “secure communication” by “allowing access to the bus only for software components identified by the access authorization information.” Ex. 1001, 167:11–19 (limitation [1B]); *id.*, 168:37–43 (limitation [14B]). The Petition’s invalidity theory is entirely premised on an allegation that this limitation is satisfied by transmitting a message on the bus only if an identified software component has been verified to be present (so that the message reaches at least the correct software component). *See* Pet. 31–32.

However, ensuring that “software components identified by the access authorization information” will receive a message transmitted over a bus (as the Petition’s theory entails) is not the same thing as “*allowing access to the bus **only for** software components identified by the access authorization information*” as the claims require. This is clear from the plain meaning of the claim limitation; ensuring that identified software components can access the bus to receive a message does not mean that those components are the *only* software components that can access the bus. It is *also* clear from the surrounding claim language, which *separately* recites “rout[ing] messages... via the inter-process software communication bus

to... the [identified] software component[s].” *See* Ex. 1001, 167:32–37 (limitation [1F]); *id.*, 168:56–61 (limitation [14E]). In other words, the claims themselves confirm that routing messages to identified software components is a *distinct* and *separate* requirement from “allowing access to the bus only for software components identified by the access authorization information.”

Because the Petition identifies no mechanism in the art that restricts which software components may access the bus (and no reason a person of ordinary skill in the art would have supplied one), the Petition fails to demonstrate a reasonable likelihood of prevailing as to any claim. Patent Owner thus respectfully requests that institution be denied.

II. Overview of the ’564 Patent

The ’564 patent is directed to techniques including securing inter-process communications on a mobile end-user device. In the patented architecture, the mobile device has “an inter-process software communication (IPC) bus that provides secure communication between a device link agent and software component processes.” Ex. 1001, Abstract. A “device link object maintains a secure message link to a message link server that receives messages from plural network functions, identified for delivery to respective software components on the mobile device, and conveys them to the device link agent.” *Id.* The device link agent, in turn, delivers

those received messages to the processes of the authorized software components. *Id.* Ex. 2006, ¶33.

The '564 patent additionally discloses *restricting* which software components may access the bus to receive a given message. The “software processes are allowed to access the bus based on access authorization information from a secure server that identifies those components.” Ex. 1001, Abstract. Consistent with that design, the specification describes “agent level access authorization, which only allows access to the agents that are on the secure authorization list,” where “the list is provided by the secure server and signatures are provided by the secure server.” *Id.*, 43:5–9. In this manner, the “bus is... protected from unauthorized monitoring or usage.” *Id.*, 42:28–30. Ex. 2006, ¶34.

The '564 patent thus does not merely ensure that messages are routed to the software component that is identified by the access authorization information; it ***additionally*** teaches that software components that are ***not*** identified by the access authorization information are ***prevented*** from reading messages intended for the components that are identified by that information. The specification makes the point expressly, describing “a set of secure messages that can only be decoded or observed by the agents they are intended for.” Ex. 1001, 42:44–45. By confining who may “decode[]” or “observe[]” a message to the “agents they are intended for,” agents

that are *not* intended to receive the message are prevented from doing so. *See* Ex. 2006, ¶35.

The claims capture this requirement in a limitation that is separate from, and additional to, the requirement of routing messages to identified components. Independent claims 1 and 14 recite, in relevant part:

1. A mobile end-user device comprising:

...

[1B] an inter-process software communication bus providing secure communication between an executing device link agent and respective executing processes for a plurality of software components, wherein providing secure communication comprises receiving access authorization information from a secure server, and ***allowing access to the bus only for software components identified by the access authorization information....***

[1C] the device link agent, configured to...

[1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.

Ex. 1001, claim 1 (emphases added).

Claim 14 similarly recites:

14. A method of operating a mobile end-user device having a wireless modem to connect to a wireless network, the method comprising:

[14A] receiving access authorization information from a secure server;

[14B] operating an inter-process software communication bus to provide secure communication between an executing device link agent and respective executing processes for a plurality of software components, the secure communication comprising *allowing access to the bus only for software components identified by the access authorization information*;

...

[14E] for software components identified by the access authorization information, routing messages identified for delivery to a given one of those software components via the inter-process software communication bus from the device link agent to a software process corresponding to the given software component.

Ex. 1001, claim 14.

As shown above, both claims require that the bus “provid[e] secure communication” by “allowing access to the bus only for software components identified by the access authorization information.” Ex. 1001, 167:11–19 (limitation [1B]); *id.*, 168:37–43 (limitation [14B]). This requirement is in *addition* to “rout[ing]

messages identified for delivery to” identified software components. *Id.*, 167:32–37 (limitation [1F]); *id.*, 168:56–61 (limitation [14E]).

The access-control limitations [1B] and [14B] therefore are not satisfied by merely routing the message to software components identified by the access authorization information. Instead, they require that access to the bus be confined to the identified software components, so that components *not* identified by the access authorization information cannot access the bus to read messages intended for the identified software components. As explained below, the Petition fails to establish this requirement is satisfied in its proposed combination of references. *See* Ex. 2006, ¶36.

III. Level of Ordinary Skill in the Art

The Petition proposes that a POSITA in the field of the ’564 patent “would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or a related field, and (2) 3–5 years of experience in services and application implementation in communication networks. Additional graduate education could substitute for professional experience, and vice versa.” Pet. 3 (citing Ex. 1003, ¶¶30–34). For purposes of this preliminary response, Patent Owner does not challenge that definition.

IV. Claim Construction

The Petition does not propose any terms for construction. *See* Pet. 4. For purposes of this preliminary response, Patent Owner agrees that no terms need be expressly construed. *See* Ex. 2006, ¶32.

V. The Petition fails to establish a reasonable likelihood of success with respect to any challenged claim.

The Petition alleges that the only two independent challenged claims—claims 1 and 14—are obvious based on four grounds, Ground 1 involving TS-23.140 (which the Petition refers to as “MMS” because it describes a version of an MMS standard) in view of Rakic, and Grounds 2A, 2B, and 2C involving MMS-Rakic in view of Cole, Sathish, or Cole and Sathish together, respectively. Both independent claims recite “allowing access to the bus only for software components identified by [received] access authorization information.” *See* Ex. 1001, 167:11–19 (limitation [1B]); *id.*, 168:37–43 (limitation [14B]).

Despite the Petition relying on four references across Grounds 1, 2A, 2B, and 2C, the Petition does not allege that **any** reference standing alone discloses “allowing access to the bus only for software components identified by the access authorization information.” Instead, the Petition’s analysis of this limitation alleges only that the **combination** of TS-23.140 with Rakic would satisfy the limitation. But as explained in the following subsections, the Petition’s analysis is wholly conclusory, and even if the prior art were combined in the manner the Petition alleges, the Petition’s

combination *still* does not satisfy the requirements of limitations [1B] and [14B].
See Ex. 2006, ¶¶37–50.

A. The Petition’s Ground 1 fails to show the obviousness of independent claims 1 and 14.

As noted in Section II above, both challenged independent claims recite “allowing access to [a] bus only for software components identified by [received] access authorization information” in limitations [1B] and [14B], and recite this as a *distinct* limitation from “for software components identified by the access authorization information, rout[ing] messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component” as recited in limitations [1F] and [14E]. In other words, the claim requires not only routing messages to the identified software components, but *also* “allowing access to the bus *only* for” the identified software components. Ex. 2006, ¶36.

The Petition, however, fails to articulate how the prior art satisfies (or would be modified to satisfy) this limitation. As explained below, the prior art, even if modified to operate exactly how the Petition alleges it would operate, would not satisfy this claim requirement, and the Petition identifies nothing that would even arguably provide a motivation to arrive at that claim requirement.

1. The Petition’s combination does not satisfy the requirement of “allowing access to the bus only for software components identified by the access authorization information.”

The Petition’s only analysis of the requirement of “allowing access to the bus only for software components identified by the access authorization information” is at pages 31–32 of the Petition, which is reproduced below in its entirety (with the Petition’s original emphases):

Moreover, in MMS-Rakic, “access to the bus” is “allow[ed]... only for software components identified by the access authorization information,” as claimed. EX-1003, ¶120. MMS-Rakic’s User Agent incorporates the signature validation functionality of Rakic’s secure push message client. *Supra* §VII.C.4. After receiving the signed message, MMS-Rakic’s User Agent generates a key by creating a hash of the administrator code (which was previously provisioned during destination application registration) and the destination application’s identifier. EX-1003, ¶120; EX-1007, [0110]-[0111]. After the key is generated, MMS Rakic’s User Agent signs the data block of the message with the key and compares the resulting signature to the signature of the message. EX-1003, ¶120; EX-1007, [0112]. ***If the signatures match***, the message is deemed valid and routed by MMS-Rakic’s User Agent to the identified destination application. EX-1003, ¶120; EX-1007, [0112]-[0119], [0122], [0131]; EX-1004, 54-56.

MMS-Rakic’s User Agent (“device link agent”) thus routes the message to the destination application (“software component”) over MMS-Rakic’s bus (*supra* §VII.D.1.c.iii) ***only if the signature*** (which,

as discussed, is generated using the identifier that identifies the destination application) *is valid*. EX-1003, ¶121. This meets [1B2]’s “allowing access to the bus only for software components identified by the access authorization information” requirement because the User Agent is an end-point of MMS-Rakic’s inter-process software communication bus, over which application-specific data received from the network is “transported without alteration” (EX-1004, 14) to a destination application on the device. EX-1003, ¶121.

Pet. 31–32 (emphases in original).

As can be seen from the excerpt above, the Petition contends that conditionally “rout[ing]” a “message to the destination application (‘software component’)” over a bus “only if [a] signature... is valid” (which signature verifies that the correct and verified destination application is resident on the device) constitutes “allowing access to the bus only for software components identified by the access authorization information” as required by limitations [1B] and [14B]. *See id.*

The Petition’s allegation in this regard is conclusory and unsupported. Although the Petition describes a signature-validation mechanism in detail, it never explains *why* Petitioner believes that conditionally transmitting a message over a bus (i.e., conditioning the transmission of the message on a valid signature being present) would mean that bus access is allowed *only* for software components identified by

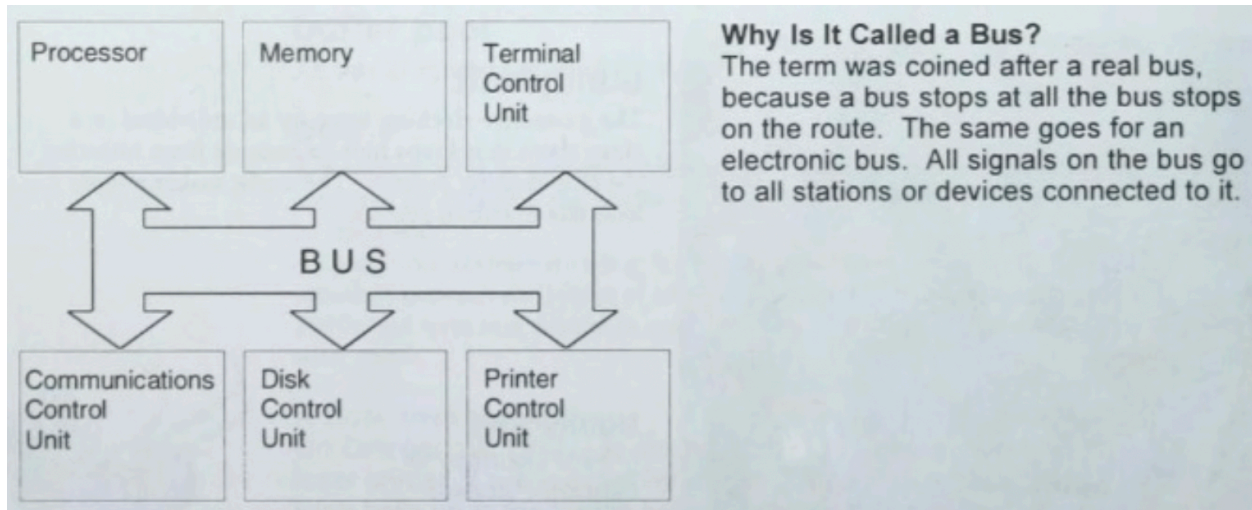
the access authorization information. Nor does the Petition’s supporting declaration supply that explanation; it does no more than repeat the Petition’s assertion. *See* Ex. 1003, ¶¶120–121. Such conclusory testimony is entitled to little weight. *See* 37 C.F.R. § 42.108(c); *Xerox Corp. v. ByteMark, Inc.*, IPR2022-00624, Paper 12 at 5 (PTAB Feb. 10, 2023) (Director Review decision affirming PTAB’s denial of institution: “[T]he Board was correct in giving little weight to Petitioner’s expert because the expert declaration merely offered conclusory assertions without underlying factual support and repeated, *verbatim*, Petitioner’s conclusory arguments.”).

Furthermore, as explained by Patent Owner’s expert, conditional transmission of a message, dependent on a valid signature being present, does ***not*** allow access to the bus only for software components specifically identified by the signature. At most, it prevents message transmission when the identified software component is not present on a device, but does nothing to prevent *additional* (unidentified) software components from accessing the bus to retrieve a message transmitted to an identified software component. Ex. 2006, ¶39.

For instance, consider a bus (like the communication path 310 in Rakic’s FIG. 3) to which various system components have access. These system components might include three different applications (A, B, and C), each one of which has a unique application identifier. Under the Petition’s theory, when a signature

identifying application A is received, the signature will be verified, and the MMS User Agent in the combined system would transmit the message intended for application A along the bus. But the bus is *also* accessible to applications B and C; no security mechanism is disclosed by TS-23.140 or Rakic to *prevent* applications B and C from *also* receiving the message intended for application A, and the Petition does not even articulate such a security mechanism (much less establish its obviousness). Ex. 2006, ¶40.

This understanding is confirmed by documentary evidence, including Google's own evidence. For example, the dictionary definition of "software bus" provided by Google indicates that the term describes a "programming interface that allows software modules to transfer data to each other," with no discussion of disallowing access to any connected components. Ex. 1049 at 3. And while Google declined to provide the definition of "bus" from which "software bus" derives its origin, an earlier version of the same dictionary that Patent Owner was able to obtain indicates that "[a]ll signals on the bus go to all stations or devices connected to it." Ex. 2008 at 4 (additional explanation and diagram accompanying the definition reproduced below). In other words, unless specific, non-standard features are added to a bus, a bus will transmit data to *all* connected components, as shown in the diagram below. Ex. 2006, ¶41.



Ex. 2008 at 4.

The fact that a “bus” by default broadcasts to *all* recipients is true even where a transmission is addressed to a particular recipient; for example, even when a “data packet... contains the address of the destination station,” it “is broadcast to all nodes at the same time, and the recipient computer responds by accepting it.” *Id.* In other words, addressing does not *restrict* access to any component; it merely *identifies* which connected component is the intended recipient of a message that all connected components receive. And tellingly, the Petition identifies no mechanism (either in the prior art relied upon or in buses more generally) that would restrict which connected components can read data transmitted over the bus. Ex. 2006, ¶42.

Thus, transmitting a message across a bus conditioned upon verification of a signature does not satisfy the challenged claims’ recitation of “allowing access to the bus only for software components identified by the access authorization

information.” *Even if* transmission of the message occurs only when a verified software component on the device is identified by a signature, that does not disclose or imply that *other, non-identified* software components would be disallowed from accessing or receiving the message transmitted on the bus, as the claim requires. *See* Ex. 2006, ¶45.

In essence, Google rewrites the claims’ recitation of “allowing access to the bus only for software components identified by the access authorization information,” to instead require “~~allowing access to~~ transmitting information across the bus only ~~for~~ when software components are identified by the access authorization information.” Nowhere does the Petition provide any explanation why these are equivalent to one another. And as explained above, they are *not* equivalent, because transmitting a message across a bus only when the signature matches with an identified software component on the device does nothing to *disallow other* software components from accessing the bus.

The references themselves confirm the Petition’s deficiency. TS-23.140 does not describe *any* inter-process software communication bus; instead, it is *explicit* that “[d]etails of these applications or how an MMS User Agent or an MMS VAS Application would interface with them are outside the scope of this specification.” Ex. 1004, 54. Accordingly, TS-23.140 fails to disclose any mechanism that would restrict certain software components from accessing any bus. Ex. 2006, ¶43.

Rakic also fails to disclose any such mechanism. Rakic is directed to validating a “secure push message” that a client device receives, and its signature techniques serve only to “verify that an intended recipient of the secure push message is the client device, and that the client device includes a correct component.” Ex. 1007, [0041]. The only feature of Rakic that the Petition contends relates to a “bus” is a “communication path” 310 which “provide[s] an interface through which components of device 300 can communicate with each other” as shown in Figure 3 of Rakic. *See* Ex. 1007, [0058] (cited by Pet. 15). And consistent with the definition of “bus” provided above, Rakic’s communication path 310 links numerous system components, with no disclosure that any system component would be prevented from reading a message transmitted over the bus. Ex. 2006, ¶44.

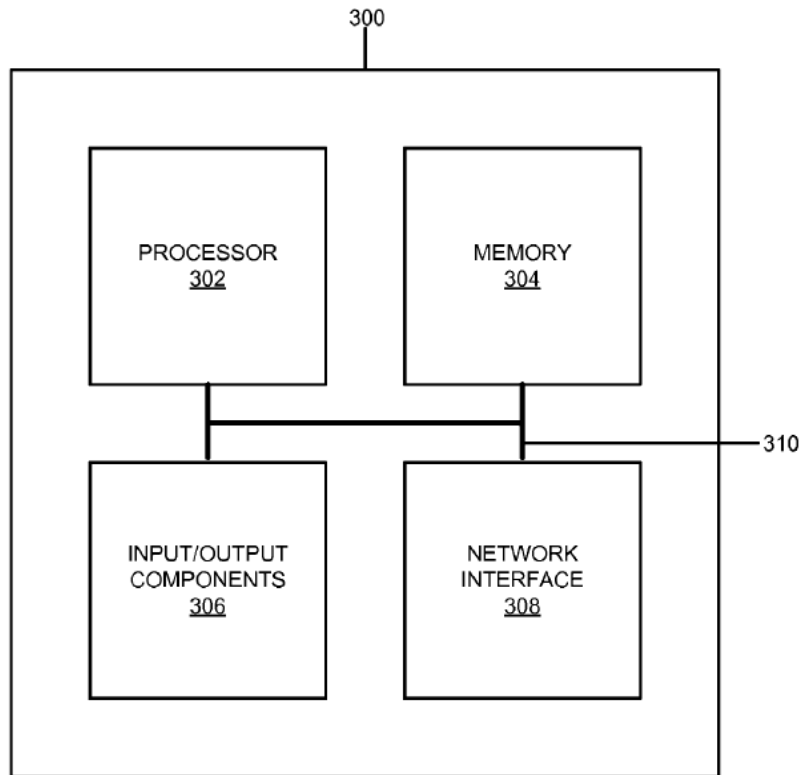


Fig. 3

Ex. 1007, FIG. 3 (showing “communication path 310” connecting several device components with no disclosure or suggestion that any component would be restricted from accessing any data sent across the path). Rakic’s disclosure of confirming that a message is destined for the correct device, and that the device includes the correct component, does not disclose or render obvious disallowing any *other* components resident on that device from accessing the message once it is placed on the bus. Ex. 2006, ¶44.

In sum, neither TS-23.140 nor Rakic discloses preventing unidentified software components from accessing messages transmitted across a bus, and the

Petition does not articulate any modification to the prior art that would involve such a mechanism. Ex. 2006, ¶¶43–45.

2. The Petition offers no obviousness rationale to arrive at the claim requirements.

As explained in the preceding subsection, even accepting the Petition’s explanation of how the prior art would be combined, that combination would not satisfy the requirements of limitations [1B] and [14B]. This is no accident or oversight, because the Petition provides no motivation to allow access to the bus only for the software component identified by access authorization information. Ex. 2006, ¶46.

The Petition’s alleged motivations in combining TS-23.140 with Rakic are limited to accomplishing the following results: (1) “implement[ing] the interface between TS-23.140’s MMS User Agent application and other applications using a software bus for interprocess communications” (Pet. 15), and (2) “to implement Rakic’s message signing and validation techniques” (Pet. 17). Even setting aside the fact that the Petition’s MMS-Rakic combination would *not* satisfy the claim requirements (because as discussed above neither MMS nor Rakic has any mechanism for disallowing software components other than the identified software component from accessing the bus), the Petition identifies no evidence that ensuring that *only* the intended destination application can access the bus to retrieve a

transmitted message would have been obvious. For instance, the Petition identifies no competent evidence that a POSITA would have recognized a need to restrict access to a bus when transmitting a message to an intended recipient. Instead, the art is focused on ensuring the *client device* (e.g., mobile phone) “is the client device,” and that the “client device includes a correct component.” Ex. 1007, [0041]. Rakic says nothing about preventing components that are *not* the “correct component” from accessing the bus, and the Petition identifies no evidence other than conclusory expert testimony that a POSITA as of the priority date of the ’564 patent would have been motivated to attempt to achieve such a result (much less that any specific implementation that might achieve such a result would have been obvious).¹ Ex. 2006, ¶47.

¹ And even if the *result* of “ensuring... that only the intended destination application receives the message” were obvious, as explained above in Section V.A above, the Petition’s description of how its combination would operate does not even achieve that result, because the Petition describes no mechanism in its combination for disallowing unidentified software components from accessing the bus while a message is being transmitted to the identified software component. Petitioner’s Discretionary Denial Opposition describes this as a “careful explanation of how the MMS-Rakic combination... prevent[s] communication

Furthermore, even if the Petition *had* provided an evidence-supported allegation that the solution would have been obvious, it would not matter because it is not grounded in the prior art of record. As Acting Director Stewart made clear in her July 31, 2025 Memorandum, “expert testimony, common sense, and other evidence that is ‘not prior art consisting of patents or printed publications’... may not be used to supply a missing claim limitation.”² Here, the Petition does not even allege that “allowing access to the bus only for software components identified by the access authorization information” is present in the prior art of record. Thus, even

with unauthorized software components.” Paper 8 at 16. But this is not a “careful explanation” at all—it is entirely conclusory allegation that the limitation is obvious, without explaining *how*. And that allegation is supported by no evidence other than equally conclusory expert testimony. Critically, neither the Petition nor Dr. Traynor describe any *mechanism* for how the allegedly obvious result would be accomplished. For instance, the Petition identifies no mechanism in either TS-23.140 or Rakic that would prevent applications coupled to a bus from reading messages transmitted over that bus if those applications are not identified by access authorization information, as discussed extensively herein.

² https://www.uspto.gov/sites/default/files/documents/aapa_memo_final_signed.pdf.

if the Petition *had* provided evidence that could even arguably bridge this gap, that evidence would not be “prior art consisting of patents or printed publications” and would thus be unable to satisfy the requirement of 37 C.F.R. § 42.104(b)(4) that a Petition “must specify where each element of the claim is found *in the prior art patents or publications relied upon*.”³

B. The Petition’s Grounds 2A, 2B, and 2C likewise fail.

The Petition additionally alleges that claims 1 and 14 are obvious based on combinations of TS-23.140, Rakic, and Cole (Ground 2A); TS-23.140, Rakic, and Sathish (Ground 2B); and TS-23.140, Rakic, Cole, and Sathish (Ground 2C). *See* Pet. 64–67. However, the Petition does not allege anything in its proposed combinations of Cole and/or Sathish that would cure the deficiencies identified above regarding the claims’ recitation of “allowing access to the bus only for software components identified by the access authorization information.” Ex. 2006, ¶48.

For instance, the Petition relies on Cole only for its teaching of “a modem to enable communications over 2G/3G networks.” Pet. 64–66. And while the Petition relies on Sathish for its disclosure of “a ‘D-Bus’ as ‘an example of a device inter-process communication channel used to send information between applications’”

³ *Id.*

(Pet. 66), the Petition fails to allege that Sathish's D-Bus is configured (or would be obviously configured) to "allow[] access to the bus only for software components identified by the access authorization information." *See* Pet. 66–67 (the Petition's analysis of Grounds 2B and 2C, failing to address this claim requirement). Ex. 2006, ¶49.

Accordingly, none of the Petition's Grounds 2A, 2B, and 2C cure the deficiency discussed above with respect to the Petition's Ground 1. And because Grounds 1, 2A, 2B, and 2C are the only grounds that challenge any independent claims, the Petition's remaining Grounds (which challenge only dependent claims) fail for at least the same reasons. Ex. 2006, ¶50.

VI. Conclusion

Because the Petition fails to set forth any plausible theory as to any challenged claim, the Petition does not establish a reasonable likelihood of prevailing and should be denied.

Date: July 1, 2026

Respectfully submitted,

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Fl.
Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

The undersigned hereby certifies that the above document was served on July 1, 2026, by filing this document through the Patent Trial and Appeal Case Tracking System (P-TACTS) as well as delivering a copy via electronic mail upon the following attorneys of record for Petitioner:

Anant K. Saraswat, Reg. No. 76,050
Gregory F. Corbett, pending admission *pro hac vice*
Turhan F. Sarwar, pending admission *pro hac vice*
George T. Scott, Reg. No. 62,859
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210-2206
ASaraswat-PTAB@wolfgreenfield.com
Gregory.Corbett@wolfgreenfield.com
TSarwar-PTAB@wolfgreenfield.com
GScott-PTAB@wolfgreenfield.com

Date: July 1, 2026
RUSS AUGUST & KABAT
12424 Wilshire Blvd., 12th Fl.
Los Angeles, CA 90025
Phone: (310) 826-7474

/James A. Milkey/
James A. Milkey
Reg. No. 79,503
Attorney for Patent Owner