

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

FORD MOTOR COMPANY  
Ford,

v.

AUTOCONNECT HOLDINGS, LLC  
Patent Owner.

---

U.S. Patent No. 9,173,100 to Ricci

Case No.: IPR2026-00173

---

**PETITION FOR *INTER PARTES* REVIEW  
UNDER 35 U.S.C. § 311 *ET SEQ.* AND 37 C.F.R. § 42.100 *ET SEQ.*  
(U.S. PATENT NO. 9,173,100)**

## Table of Contents

List of Exhibits.....	iv
Mandatory Notices under 37 C.F.R. § 42.8.....	viii
Real Party-In-Interest - 37 C.F.R. § 42.8(b)(1).....	viii
Related Matters - 37 C.F.R. § 42.8(b)(2).....	viii
Lead and Back-Up Counsel - 37 C.F.R. § 42.8(b)(3).....	ix
Service Information - 37 C.F.R. § 42.8(b)(4).....	ix
Fees - 37 C.F.R. § 42.15(a).....	ix
I. Introduction.....	1
II. Grounds for Standing Requirements under 37 C.F.R. § 42.104.....	3
A. Grounds for Standing - 37 C.F.R. § 42.104(a).....	3
B. Challenged Claims - 37 C.F.R. § 42.104(b)(1).....	3
C. Prior Art Relied Upon.....	3
D. Grounds of Challenge – 37 C.F.R. § 42.104(b)(2).....	4
III. Person of Ordinary Skill in the Art (PHOSITA).....	5
IV. The '100 Patent.....	5
A. Priority Claim.....	5
B. Prosecution History.....	7
V. Claim Construction — 37 C.F.R. § 42.104(B)(3).....	7
A. Claims 1, 2, 5, 7, 8, 9, 10, 13, 15, 16, 17, 18, 21, 23, and 24: “and/or”.....	8
VI. The '100 Patent is not entitled to its earliest claimed priority date.....	8
VII. Prior Art Overview.....	11
A. Amirtahmasebi (EX1019).....	11
B. Spaur (EX1020).....	12
C. Peirce (EX1021).....	13
D. Bosch (EX1050).....	13
VIII. Unpatentability Grounds.....	14
A. Ground 1: Claims 1–24 are Obvious Over Amirtahmasebi and Bosch.....	14
1. Rationale to Combine.....	14
2. Independent Claim 1.....	15
a. Limitation 1[pre].....	15

b.	Limitation 1[a]	16
c.	Limitation 1[b]	18
d.	Limitation 1[c]	22
e.	Limitation 1[d]	25
f.	Limitation 1[e]	27
g.	Limitation 1[f]	30
3.	Dependent Claim 2	33
a.	Limitation 2[pre]	33
b.	Limitation 2[a]	36
c.	Limitation 2[b]	38
4.	Dependent Claim 3	39
a.	Limitation 3[pre]:	39
b.	Limitation 3[a]:	40
c.	Limitation 3[b]:	41
5.	Dependent Claim 4	42
a.	Limitation 4[pre]	42
b.	Limitation 4[a]	44
6.	Dependent Claim 5	44
a.	Limitation 5[pre]	44
b.	Limitation 5[a]	45
7.	Dependent Claim 6	47
a.	Limitation 6[pre]	47
b.	Limitation 6[a]	48
8.	Dependent Claim 7	50
9.	Dependent Claim 8	51
a.	Limitation 8[pre]	51
b.	Limitation 8[a]	53
c.	Limitation 8[b]	55
10.	Independent Claim 9 and 17	56
a.	Limitation 9[pre] and 17[pre]	56
b.	Limitations 9[a] and 17[a]	57
c.	Limitations 9[b] and 17[b]	57
d.	Limitations 9[c] and 17[c]	58
e.	Limitation 9[d] and 17[d]	58
f.	Limitations 9[e] and 17[e]	59
g.	Limitations 9[f] and 17[f]	59
11.	Dependent Claims 10 and 18	59
12.	Dependent Claims 11-16 and 19-24	59
a.	Claims 11 and 19	60

b.	Claims 12 and 20 .....	60
c.	Claims 13 and 21 .....	60
d.	Claims 14 and 22 .....	60
e.	Claims 15 and 23 .....	60
f.	Claims 16 and 24 .....	60
B.	Ground 2: Independent Claims 1, 9, and 17 are Obvious Over Spaur and Peirce .....	60
1.	Rationale to Combine .....	60
2.	Independent Claim 1 .....	62
a.	Limitation 1[pre].....	62
b.	Limitation 1[a] .....	62
c.	Limitation [1b].....	65
d.	Limitation [1c].....	68
e.	Limitation [1d].....	70
f.	Limitation [1e].....	72
g.	Limitation 1[f] .....	74
3.	Independent Claims 9 and 17.....	76
a.	Limitation 9[pre] and 17[pre] .....	76
b.	Limitations 9[a] and 17[a] .....	76
c.	Limitations [9b] and 17[b].....	77
d.	Limitations 9[c] and 17[c] .....	77
e.	Limitation 9[d] and 17[d] .....	77
f.	Limitations 9[e] and 17[e] .....	78
g.	Limitations 9[f] and 17[f].....	78
IX.	Conclusion .....	78
	Certificate of Service .....	79
	Certificate of Compliance Pursuant to 37 C.F.R. § 42.24 .....	80
	Appendix A - Listing of All Challenged Claims .....	1
	Appendix B - Comparison of Independent Claims.....	22
	Appendix C - Comparison of Dependent Claims .....	27

**List of Exhibits**

<b>Exhibit No.</b>	<b>Description</b>
1001	U.S. Patent No. 9,173,100 (“the ’100 Patent”)
1002	U.S. Patent No. 9,173,100 Certified File History (“the ’100 Patent File History”)
1003	Expert Declaration of Scott Andrews
1004	Scott Andrews Curriculum Vitae
1005	<i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-JCG (D. Del) (December 6, 2024) (“Complaint”)
1006	Plaintiff’s Opposition to Defendant’s Motion to Dismiss, <i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-CFC (D Del.) (February 28, 2025) (“Opposition”)
1007	<i>Intentionally left blank</i>
1008	U.S. Patent No. 9,173,100 with Additions to Specification Highlighted
1009	Summons, <i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-JCG (D. Del) (Dec. 10, 2024) (“Return of Service”)
1010-1018	<i>Intentionally left blank</i>
1019	Amirtahmasebi et al., “Vehicular Networks – Security, Vulnerabilities and Countermeasures, Master of Science Thesis in the program Networks and Distributed Systems,” and accompanying Librarian Declaration (“Amirtahmasebi”)
1020	U.S. Patent Application Pub. No. 2004/0185842 A1 to Spaur (“Spaur”)
1021	U.S. Patent No. 8,788,731 B2 to Peirce (“Peirce”)
1022-1049	<i>Intentionally left blank</i>
1050	Bosch Handbook, (Automotive Handbook October 2004 6 <sup>th</sup> Edition) (“Bosch”)
1051	IEEE Dictionary, (IEEE 100 The Authoritative Dictionary of IEEE Standards Terms 2000 7 <sup>th</sup> Edition) (“IEEE Dictionary”)
1052	“Specification of The Bluetooth System” (June 30, 2010). Version 4.0 (Volumes 0-6) Available at <a href="https://www.bluetooth.com/specifications/specs/core-specification-4-0/">https://www.bluetooth.com/specifications/specs/core-specification-4-0/</a> (Accessed June 27, 2025) (“Bluetooth Specification”)

1053-1059	<i>Intentionally left blank</i>
1060	TCP/IP Tutorial and Technical Overview 6 <sup>th</sup> Ed. (International Business Machines Corporation – October 1998) (“IBM TCP/IP Tutorial”)
1061-1081	<i>Intentionally left blank</i>
1082	M. Wolf, A. Weimerskirch, and C. Paar, “Security in Automotive Bus Systems,” in Workshop on Embedded IT-Security in Cars, Bochum, Germany, November 2004 (“Wolf”)
1083	P. Golle, D. Greene and J. Staddon, “Detecting and correcting malicious data in VANETs.” in Proceedings of the first ACM workshop on Vehicular ad hoc networks, (2004), ACM Press, pp 29–36. (“Golle”)
1084	T. Hoppe, S. Kiltz, and J. Dittmann. “Security threats to automotive CAN networks-Practical examples and selected short-term countermeasures.” Reliability Engineering & System Safety, Vol. 96, Issue 1, January 2011, pp. 11-25 (“Hoppe”)
1085	X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, “Security in vehicular ad hoc networks”, IEEE communications magazine. (Apr 30 2008), 46(4), pp.88-95. (“Lin”)
1086	M. Jusufovic and M. Nilsson. "Wireless Security in Road Vehicles-Improving Security in the SIGYN System." (2009). (“Jusufovic”)
1087	D. Nilsson, P. Phung, and U. Larson, “Vehicle ECU Classification Based on safety-Security Characteristics” In Proceedings of the 13th International Conference on Road Transport and Information Control (RTIC), 2008. (“Nilsson”)
1088	B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks,” in Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005. (“Parno”)
1089-1106	<i>Intentionally left blank</i>
1107	U.S. Patent and Trademark Office - U.S. 9,173,100 Maintenance Fee Payment Records
1108-1109	<i>Intentionally left blank</i>
1110	Flextronics “Flex celebrates 10 years of maintaining Ford’s prestigious Q1 quality certification in Guadalajara, Mexico” (Posted April 2, 2024) Available at <a href="https://flex.com/resources/10-years-of-maintaining-fords-q1-quality-certification">https://flex.com/resources/10-years-of-maintaining-fords-q1-quality-certification</a>

1111	<i>Intentionally left blank</i>
1112	Scheduling Order, <i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-JCG (D. Del) (“Scheduling Order”)
1113-1114	<i>Intentionally left blank</i>
1115	Defendant’s Motion to Dismiss, <i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-CFC (D Del.) Filed February 14, 2025 (“Motion to Dismiss”)
1116	<i>Intentionally left blank</i>
1117	Zetter, Mark “Ford and Flextronics automotive EMS, Venture Outsource” February 2010 (Available at <a href="https://ventureoutsource.com/contract-manufacturing/industry-pulse/ford-and-flextronics-automotive-ems">https://ventureoutsource.com/contract-manufacturing/industry-pulse/ford-and-flextronics-automotive-ems</a> , accessed November 18, 2025) (“Ford Flextronics EMS”)
1118	Schröter, Anke “Ford partners with Flextronics, evertiq.com”, February 12, 2010, (Available at <a href="https://evertiq.com/news/16197?">https://evertiq.com/news/16197?</a> , accessed November 18, 2025) (“Ford Flextronics 2010”)
1119	“Which Ford vehicles are compatible with Apple CarPlay?” (Available at <a href="https://www.ford.com/support/how-tos/sync/getting-started-with-sync/which-vehicles-are-compatible-with-apple-carplay/">https://www.ford.com/support/how-tos/sync/getting-started-with-sync/which-vehicles-are-compatible-with-apple-carplay/</a> Accessed November 18, 2025) (“Ford AppleCarPlay”)
1120	U.S. Patent and Trademark Office - U.S. 9,173,100 Assignment Abstract
1121-1150	<i>Intentionally left blank</i>
1151	File Wrapper of 61/560,509 (the “First Provisional”)
1152	File Wrapper of 61/637,164 (the “Second Provisional”)
1153	File Wrapper of 61/646,747 (the “Third Provisional”)
1154	File Wrapper of 61/653,275 (the “Fourth Provisional”)
1155	File Wrapper of 61/653,264 (the “Fifth Provisional”)
1156	File Wrapper of 61/653,563 (the “Sixth Provisional”)
1157	File Wrapper of 61/663,335 (the “Seventh Provisional”)
1158	File Wrapper of 61/672,483 (the “Eighth Provisional”)
1159	File Wrapper of 61/714,016 (the “Ninth Provisional”)
1160	File Wrapper of 61/715,699 (the “Tenth Provisional”)
1161	File Wrapper of U.S. Patent Publication No. 2013/0145482 (the “First Non-Provisional”)

1162	U.S. DOT Final Report, FHWA-JPO-17-483, “Development of DSRC Device and Communication System Performance Measures, Recommendations for DSRC OBE Performance and Security Requirements,” May 22, 2016. (“FHWA-JPO-17-483”)
1163	U.S. DOT, FHWA-JPO-12-061, “Communications Data Delivery System Analysis, Task 2 Report: High-Level Options for Secure Communications Data Delivery Systems,” June 21, 2012. (“FHWA-JPO-12-061”)
1164	U.S. DOT Final Draft, FHWA-JPO-18-686 “National Security Credential Management System (SCMS) Deployment Support, Potential SCMS Ownership and Governance Models,” June 22, 2018. (“FHWA-JPO-18-686”)
1165	U.S. DOT Final Report, FHWA-JPO-09-003, “Vehicle Infrastructure Integration Proof of Concept Executive Summary – Vehicle,” May 19, 2009. (“FHWA-JPO-09-003”)
1166	U.S. DOT Final Report, FHWA-JPO-09-043, “Vehicle Infrastructure Integration Proof of Concept Results and Findings Summary – Vehicle,” May 19, 2009. (“FHWA-JPO-09-043”)
1167	U.S. DOT Final Report, FHWA-JPO-09-017, “Vehicle Infrastructure Integration Proof of Concept Technical Description – Vehicle,” May 19, 2009. (“FHWA-JPO-09-017”)
1168	U.S. Patent No. 7,734,050 B2 to Tengler (“Tengler Digital Certificate Pool”)
1169	U.S. Patent No. 7,742,603 B2 to Tengler (“Tengler Security for Anonymous Vehicular Broadcast Messages”)

**Mandatory Notices under 37 C.F.R. § 42.8**

**Real Party-In-Interest - 37 C.F.R. § 42.8(b)(1)**

Ford certifies that Ford (“Petitioner”) is the real party-in-interest. No unnamed entity is funding, controlling, or directing this Petition or could control or direct this Petition or Ford’s participation.

**Related Matters - 37 C.F.R. § 42.8(b)(2)**

Petitioner identifies the following related judicial matter: *AutoConnect Holdings, LLC v. Ford Motor Company*, 1:24-cv-01327-JCG (D. Del) (pending) filed December 6, 2024. U.S. Patent No. 9,173,100 is being asserted in this proceeding, along with twelve other related patents: U.S. 9,020,491; U.S. 9,020,697; U.S. 9,082,239; U.S. 9,098,367; U.S. 9,116,786; U.S. 9,123,186; U.S. 9,140,560; U.S. 9,147,296; U.S. 9,147,297; U.S. 9,290,153; U.S. 10,862,764; and U.S. 11,163,931.

Petitioner filed IPR2025-01342 challenging U.S. 9,020,697, IPR2025-01383 challenging U.S. 9,290,153, IPR2025-01524 challenging U.S. 9,123,186, IPR2026-00002 challenging U.S. 9,147,296, IPR2026-00172 challenging U.S. 9,147,297, and IPR2026-00171 challenging U.S. 9,082,239.

Petitioner is also aware that U.S. Patent No. 9,173,100 is being asserted in *AutoConnect Holdings LLC v. General Motors LLC* 2-24-cv-00877 (EDTX) (pending) filed October 30, 2024.

**Lead and Back-Up Counsel - 37 C.F.R. § 42.8(b)(3)**

Petitioner identifies the following lead and back-up counsel:

<b>Lead Counsel</b>	<b>Back-Up Counsel</b>
Andrew B. Turner (Reg. No. 63,121) BROOKS KUSHMAN P.C. 150 W. Second St., Suite 400N Royal Oak, MI 48067-3846 Telephone (248) 358-4400 Facsimile (248) 358-3351 aturner@brookskushman.com	John P. Rondini (Reg. No. 64,949) John S. LeRoy (Reg. No. 48,158) Christopher C. Smith (Reg. No. 59,669) Francesca M. Cusumano (Reg. No. 81,149) BROOKS KUSHMAN P.C. 150 W. Second St., Suite 400N Royal Oak, MI 48067-3846 Telephone (248) 358-4400 Facsimile (248) 358-3351 jrondini@brookskushman.com jleroy@brookskushman.com csmith@brookskushman.com fcusumano@brookskushman.com

Pursuant to 37 C.F.R. § 42.10(b), an appropriate Power of Attorney is filed concurrently herewith.

**Service Information - 37 C.F.R. § 42.8(b)(4)**

Service information for lead and back-up counsel is provided in the designation of lead and back-up counsel above. Petitioner hereby consents to service by email at the following email address: FPGP0155IPR@brookskushman.com.

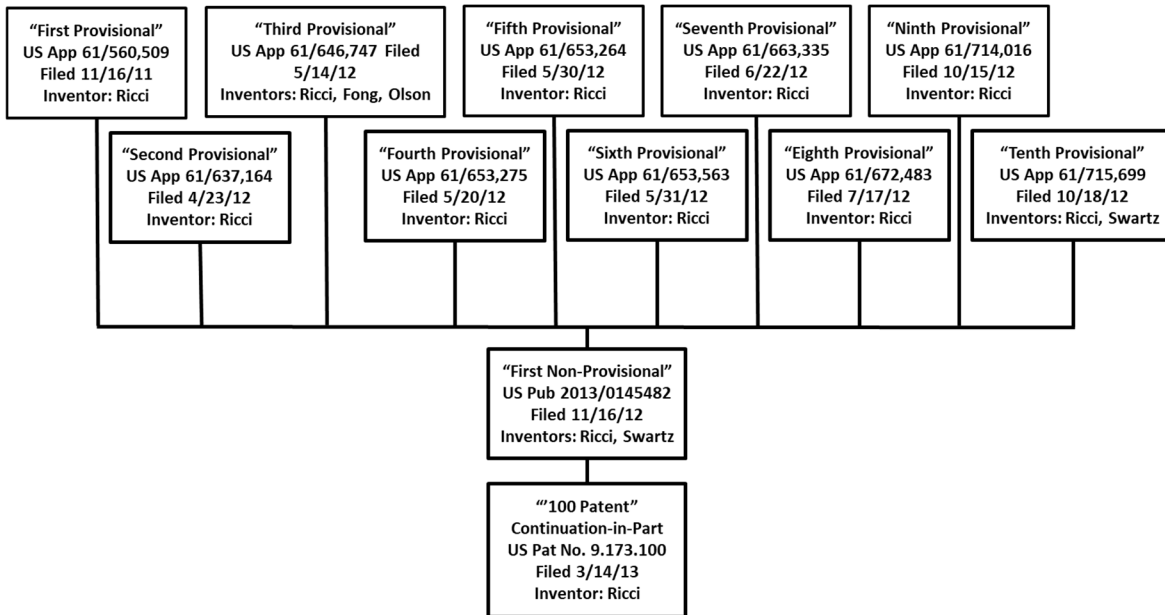
**Fees - 37 C.F.R. § 42.15(a)**

The filing fees associated with this Petition are being charged to Deposit Account 061510. The Board is authorized to charge any additional fees or credit any refunds pertaining to this Petition to Deposit Account 061510.

## **I. Introduction**

Ford Motor Company (“Petitioner”) respectfully requests *inter partes* review of claims 1–24 of U.S. Patent No. 9,173,100 (“the ’100 Patent,” EX1001). Petitioner asserts the Challenged Claims are unpatentable for two reasons.

*First*, Petitioner contends that the ’100 Patent should not receive the October 16, 2011 priority date of the First Provisional. Instead, the ’100 Patent is a continuation-in-part (“CIP”) application containing new matter absent from prior related applications. Petitioner argues the claimed “*perimeter network*” limitation is supported only by the CIP’s new matter, so the ’100 Patent should be entitled to its March 14, 2013 filing date. Alternatively, if “*perimeter network*” is supported, Petitioner asserts each independent claim recites “isolation” limitations only disclosed in the October 15, 2012 “Ninth Provisional,” making that date the proper priority date.



### '100 Patent Family

*Second*, even if the Board concludes the Challenged Claims are entitled to the earliest alleged priority date, Petitioner disputes patentability in Ground 1 based on a July 2010 thesis addressing vehicle network security, vulnerabilities, and countermeasures (EX1019). Given this thesis was published by Chalmers University of Technology (Gottenburg, Sweden), it is unlikely to have been included in the Examiner’s search.

Lastly, strong arguments weigh against discretionary denial and favor institution. The district court lawsuit filed by AutoConnect (“Patent Owner” or “PO”) against Petitioner is in its early stages, with trial scheduled for October 2027—well after the projected final decision here. (EX1112, 29.) Although the ’100 Patent issued over ten years ago, PO also allowed it to lapse for more than three

years. (Ex. 1107). Petitioner also had settled expectations it would not be asserted since, among other reasons, the original PO supplies the accused product. (EX1110; EXS1117–1119), and the current PO made no use of the '100 Patent before contacting Petitioner in December 2023 (EX1002, 1137–1146; EX1005, 9).

## II. Grounds for Standing Requirements under 37 C.F.R. § 42.104

### A. Grounds for Standing - 37 C.F.R. § 42.104(a)

Petitioner certifies that the '100 Patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR.

### B. Challenged Claims - 37 C.F.R. § 42.104(b)(1)

Petitioner requests *inter partes* review for claims 1-24 of the '100 Patent and requests the PTAB find these claims as unpatentable.

### C. Prior Art Relied Upon

This Petition relies on the following prior art:

Exhibit	Reference	Date	Section <sup>1</sup>
EX1019	“Vehicular Networks – Security Vulnerabilities and Countermeasures” (“Amirtahmasebi”) <sup>2</sup>	<b>Published:</b> 7/8/2010	§102(b)

---

<sup>1</sup> Pre-AIA Sections §102/§103 apply.

<sup>2</sup> A declaration from Sara Holmberg is appended to EX1019 supporting that Amirtahmasebi is prior art under §102.

EX1020	U.S. 7,366,892 (“Spaur”)	<b>Issued:</b> 04/09/2008	§102(b)
EX1021	U.S. 8,788,731 (“Peirce”)	<b>Filed:</b> 7/30/2012 <b>Issued:</b> 7/22/2014	§102(e) <sup>3</sup>
EX1050	Bosch Automotive Handbook 6 <sup>th</sup> Edition (“Bosch”)	<b>Published:</b> October 2004	§102(b)

Amirtahmasebi, Peirce, and Bosch were neither cited nor relied upon during examination by the Patent Office during prosecution of the ’100 Patent. (EX1001, Cover.)

A related continuation of Spaur (i.e., U.S. Publication No. 2008/0148374) was cited by the PO on an Information Disclosure Statement dated October 18, 2013. (See EX1002, 151.) The Examiner did not apply the related Spaur publication number US 2008/0148374 during prosecution of the ’100 Patent.

**D. Grounds of Challenge – 37 C.F.R. § 42.104(b)(2)**

Ground	Basis <sup>4</sup>	References	Claims Challenged
1	§103	Amirtahmasebi and Bosch	1-24
2	§103	Spaur and Peirce	1, 9, and 17

<sup>3</sup> Peirce is prior art under §102(e) based on the 10/15/2012 filing date of the “Ninth Provisional” or alternatively the 03/14/2013 filing date of the ’100 Patent.

<sup>4</sup> Pre-AIA Sections 102 and 103 apply.

There is a reasonable likelihood that at least one Challenged Claim is unpatentable as explained herein. Petitioner requests review of the Challenged Claims, and judgment finding them unpatentable.

### **III. Person of Ordinary Skill in the Art (PHOSITA)**

A PHOSITA of the '100 Patent would have had, as of March 14, 2013<sup>5</sup>, a Bachelor's degree in Electrical/Mechanical Engineering, or an equivalent degree with at least two years of experience in communication systems, vehicle sensor systems, electronic user interface systems, or related technologies. Additional industry experience could make up for less education and vice versa. (EX1003, ¶¶52-55.) Petitioner's expert, Scott Andrews, qualifies as a PHOSITA for the '100 Patent. (EX1003, ¶¶1-28; *see also* EXs1004, 1052, 1060, 1082-1088.)

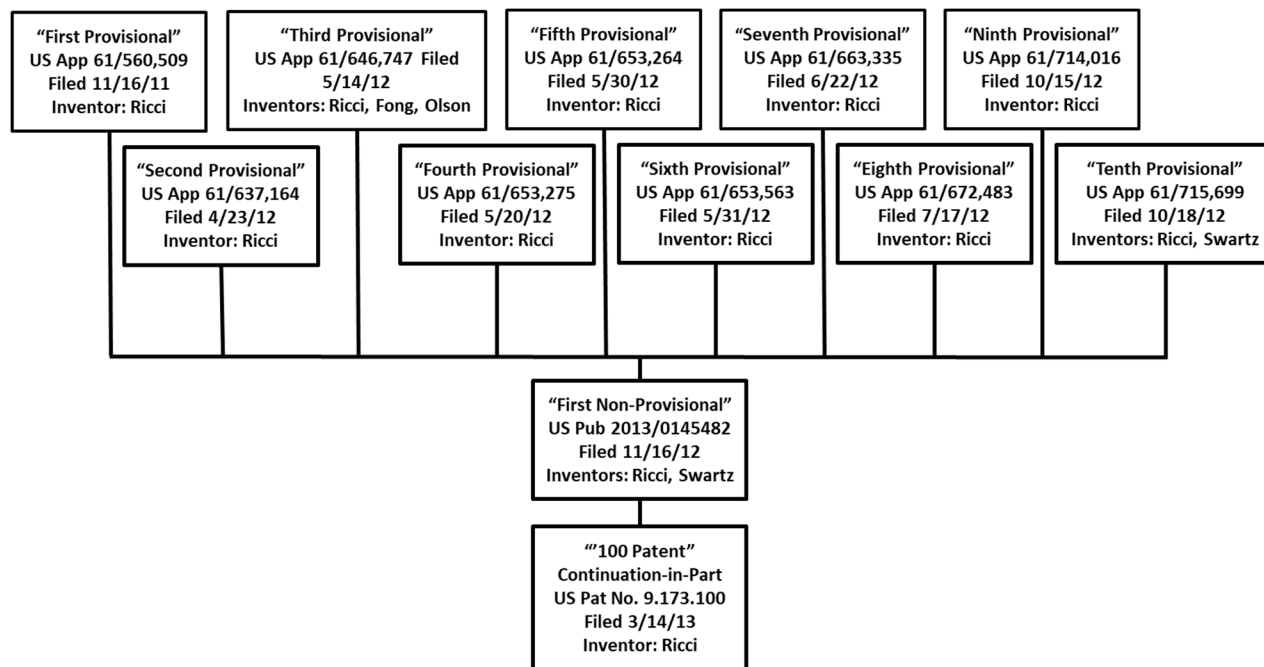
### **IV. The '100 Patent**

#### **A. Priority Claim**

The '100 Patent claims priority to ten separate provisional applications. (EX1003, ¶¶57-83; EX1001, Cover.)

---

<sup>5</sup> Regardless of any adjustment to the asserted priority date, the relevant date for a PHOSITA remains March 14, 2014.



The “First Non-Provisional” was filed on November 16, 2012. (EX1161, 1, 129.) The ’100 Patent was filed as a continuation-in-part (“CIP”) of the First Non-Provisional. (EX1002, 8-9). Critically, as filed, the ’100 Patent introduced substantial new material pertaining to a “*perimeter network*” and layered isolation measures—concepts not found in the First Non-Provisional nor in any of the Provisional Applications. (See EX1008<sup>6</sup>, 39:11-48.) None of the priority documents disclose or suggest the claimed “*perimeter network*” or the specific “*isolation*” mechanisms central to the challenged claims. Accordingly, the effective filing date

---

<sup>6</sup> EX1008 highlights the CIP additions and changes to the ’100 patent in comparison to the First Non-Provisional application.

for these claims is March 14, 2013, the date of the continuation-in-part, not any earlier provisional date. This underscores that the patentee sought to broaden the scope with new subject matter rather than merely continuing an existing invention. (EX1003, ¶¶84-86.)

### **B. Prosecution History**

During prosecution, PO filed multiple IDS forms citing hundreds of references during prosecution. (EX1002, 151-154, 340-342, 489-490, 676-679, 953, 992.)

In response to a rejection, PO amended the claims to include “isolation” limitations—like denying network access, redirection or blocking communications, and activating a second security mechanism. (EX1002, 655-673.) As explained below in the priority section, these “isolation” limitations—which resulted in a Notice of Allowance—are only supported by the Ninth Provisional. (EX1002, 925-934; EX1003, ¶¶88-100.)

### **V. Claim Construction — 37 C.F.R. § 42.104(B)(3)**

In an IPR proceeding, the claims are construed “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (*en banc*). Petitioner applies the plain and ordinary meaning of the Challenged Claims

to the asserted prior art references in support of all grounds herein.

Petitioner proposes the following claim constructions for the purposes of this Petition only.

**A. Claims 1, 2, 5, 7, 8, 9, 10, 13, 15, 16, 17, 18, 21, 23, and 24:  
“and/or”**

Petitioner interprets “and/or” as “or” in accordance with Patent Owner’s position for that term in the related litigation. (EX1006, 5-6.) Petitioner has argued certain claims are indefinite in district court. (EX1001, 6:37-44; EX1115, 15-16, 18.)

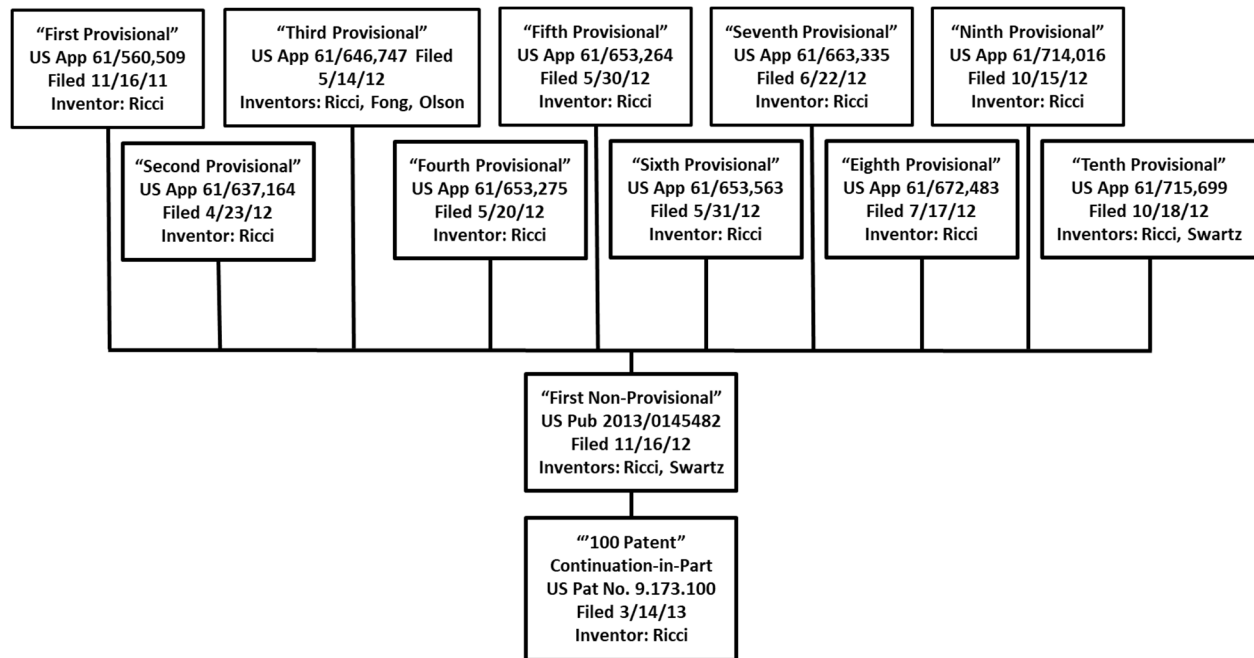
Since indefiniteness cannot be raised within an IPR petition, for purposes of addressing this term within the Challenged Claims the Petitioner adopts PO’s construction of “and/or” as meaning simply “or.” (EX1006, 6.)

**VI. The ’100 Patent is not entitled to its earliest claimed priority date**

No priority challenge was made during prosecution because the PTO does not make such findings absent interference or rejection requiring a determination of priority. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1305 (Fed. Cir. 2008); *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015). Ground 2 introduces intervening art that was filed in the interim period between the First Provisional application and the Ninth Provisional Application; since the Examiner made no priority determination, the burden shifts to PO. Under *PowerOasis* and *Dynamic Drinkware*, PO must show written

description support in earlier applications to rely on that date. PO cannot meet that burden.

As explained in § IV *supra*, the Challenged Claims cannot rely on the November 16, 2011 filing date of the First Provisional. First, as shown below, the '100 Patent is a CIP of the First Non-Provisional.



### '100 Patent Family

As filed, each independent claim requires *“a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components.”* (EX1001, 59:4-6, 61:3-6, 63:6-9.) As shown by the comparison between the specification of the '100 Patent and the First Non-Provisional, the concept and disclosure of a *“perimeter network”* was added to the specification of the '100 Patent. (EX1008, 39:11-15.) Therefore, under

*PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306-07 (Fed. Cir. 2008), new matter in a continuation-in-part cannot be used to retroactively support an earlier priority date. Because these features first appear in the '100 Patent, the claims cannot rely on any earlier filing. (EX1003, ¶¶101-106.) Thus, the earliest possible priority date for the challenged claims is March 14, 2013—the filing date of the application that introduced these disclosures. (EX1002, 1.)

Alternatively, because written description support for the “isolation” limitations (i.e., 1[d]-1[f] *infra*) appears only in the Ninth Provisional entitling the '100 Patent, at best, to its October 15, 2012 filing date. (See EX1001, claims 1, 9, 17; EX1002, 87-90; EX1159, 48-52, 99). As Petitioner’s expert explains, a PHOSITA would not have understood any of these early provisional applications to disclose the element requiring a determination of whether “*a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach.*” (EX1003, ¶¶102-105.)

The Ninth Provisional Application (filed October 15, 2012) is the first in the family to introduce any material related to isolation, but even that disclosure is limited. It includes Figure 24 and accompanying text describing middleware modules and data-stream management, yet it does not teach forming a “perimeter network”. (EX1159, 48-51, Fig. 24.)

Accordingly, to the extent PO argues it is entitled to a priority date prior to March 14, 2013, the inclusion of the “isolation” limitations to the Challenged Claims demonstrates the ’100 Patent is not entitled to a priority before the October 15, 2012 filing of the Ninth Provisional. (EX1003, ¶¶107-112.)

## **VII. Prior Art Overview**

### **A. Amirtahmasebi (EX1019)**

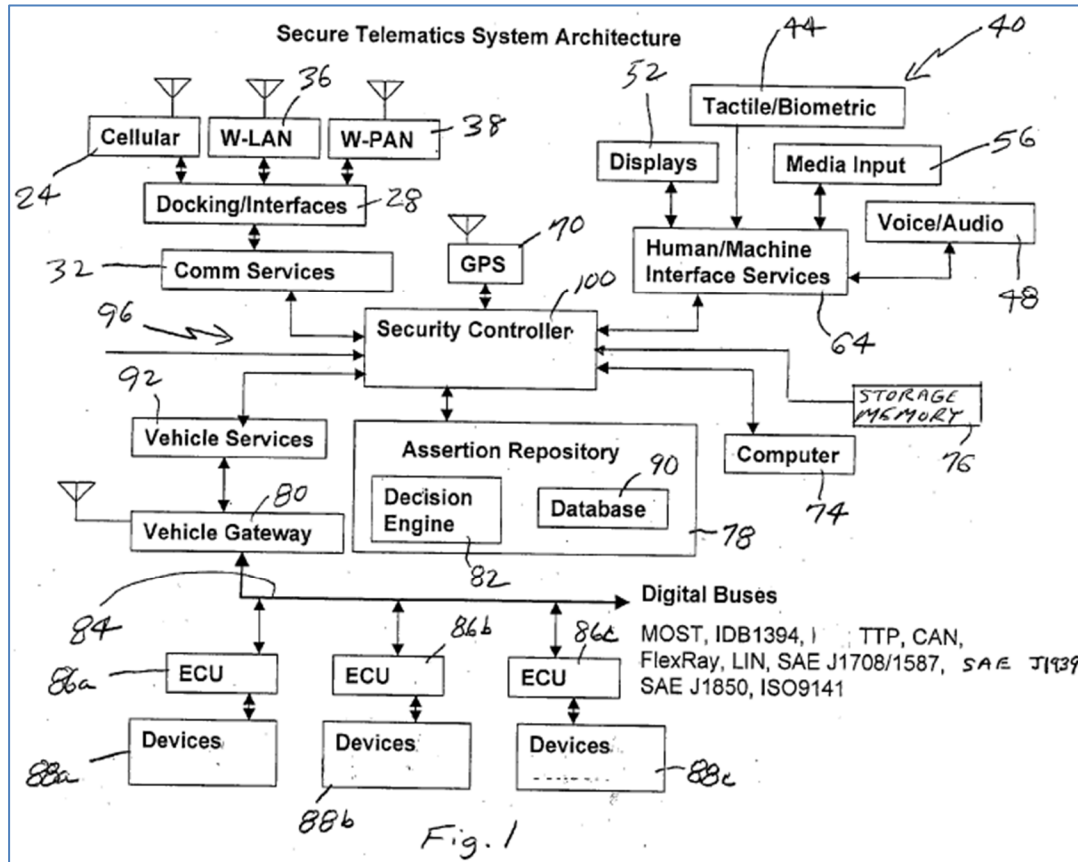
Amirtahmasebi is a thesis that provides an overview of vehicular network security, focusing on vulnerabilities and countermeasures for vehicle ad hoc networks (VANETs) and in-vehicle networks of electronic control units (ECUs,) sensors, and actuators (EX1019, 11). VANETs use On-Board Units (OBUs) and Road-Side Units (RSUs) for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. (EX1019, 13; Fig. 1.) A typical vehicle has 50–70 ECUs requiring multiple buses like LIN, CAN, MOST, and FlexRay, often segmented by gateways (EX1019, 24-25; Fig. 2). (EX1003, ¶¶140-146.)

Security risks stem from external wireless links compromising internal operations. Amirtahmasebi identifies attack vectors and urges robust security: tamper-resistant software via trusted computing, an integrated gatekeeper for monitoring inter-network and VANET traffic (EX1019, 40; Fig. 12), Intrusion Detection Systems (“IDS”) comparing traffic to malicious patterns (EX1019, 41), authentication with digital signatures and certificates (EX1019, 43-45), plus firewall

gateways and honeypots (EX1019, 45-47; EX1003, ¶¶147-151.)

### B. Spaur (EX1020)

Spaur discloses a telematics system with a central security controller (EX1020, Abstract, Fig. 1; EX1003, ¶152.)



EX1020, Fig. 1

The system includes multiple communication subsystems, including cellular telephones and wireless LAN interfaces (EX1020, [0009].) The security controller connects to various subsystems, including a wireless PAN 38 for wireless communication. A vehicle services module 92 communicates with a vehicle gateway 80, supports secure communications, and enables intra-vehicle Bluetooth PANs

(EX1020, [0035].) This allows wireless connection to user devices. The security controller encrypts to prevent “man-in-the-middle” attacks, as illustrated in Figure 3 (EX1020, Fig. 3; EX1003, ¶¶153-155.)

### **C. Peirce (EX1021)**

Peirce discloses “a message filtering system for a communications system in a vehicle” operating “via a vehicle bus.” (EX1021, Abstract.) It explains that transmit filters 210–213 and receive filters 218–221 are coupled to ECUs 214–217 with VSMs 38, 40, 42 (EX1021, 6:63-7:13, Fig. 2.) These filters follow a policy with executable instructions to validate message authenticity, including source ID, destination ID, and message ID, minimizing corrupt transmissions over bus 44 (EX1021, 7:28-54, 7:60-8:8.) Receive filters store known IDs and compare incoming messages, terminating mismatches before reaching VSM 42; transmit filters validate outgoing messages by comparing source IDs, blocking mismatches from bus 44 (EX1021, 8:45-9:3.) Peirce further teaches both filter types are physically or logically isolated from ECUs and protocol controller 265, mitigating corruption (EX1021, 9:29-35, Fig. 5; EX1003, ¶¶156-162.)

### **D. Bosch (EX1050)**

Bosch is a reference handbook that is “all about automotive engineering in a pocketbook.” (EX1050, Back Cover.) Bosch describes the common structure of an automotive electronic control unit (ECU) as of 2004, including a “[m]icroprocessor”

and “memory.” (EX1050, 94, 96.) Bosch “Microprocessor design seeks to avoid individualization in the face of large-scale integration.” (EX1050, 94; EX1003, ¶163.)

## **VIII. Unpatentability Grounds**

The references below render the claimed subject matter invalid under 35 U.S.C. §103 and Petitioner therefore has a reasonable likelihood of prevailing as to each of the following grounds of unpatentability. 35 U.S.C. § 314(a); 37 C.F.R. § 42.104(b)(4).

### **A. Ground 1: Claims 1–24 are Obvious Over Amirtahmasebi and Bosch**

#### **1. Rationale to Combine**

It would have been obvious to a PHOSITA to combine Amirtahmasebi’s security-focused vehicle-network architecture with Bosch’s well-established ECU and microprocessor architecture. Both references address complementary aspects of automotive control systems: Amirtahmasebi focuses on ECU-level security mechanisms, while Bosch provides foundational ECU hardware. (EX1019, 24-25; EX1050, 94-96, 1064-1065.) Amirtahmasebi describes ECUs by roles in network security—criticality classifications, distributed and centralized security modules, and mechanisms across CAN, LIN, MOST, and FlexRay networks. (EX1019, 20-22, 35-46; EX1003, ¶¶445-449.)

Bosch informs what was known in the art regarding ECUs use of microcomputers with CPU, program/data memory, and I/O interfaces. (EX1050, 94, 96, 1065.) Bosch further teaches Systems on a Chip (“SoCs”) for cost-sensitive automotive applications—the same ECUs contemplated by Amirtahmasebi. (EX1050, 94, 96.) A PHOSITA would have understood Amirtahmasebi’s security logic would be executable on Bosch’s architecture, reflecting routine engineering. Bosch teaches that microcomputers enable high integration and standardized ECU design. (EX1050, 94.) Combining these known elements to implement Amirtahmasebi’s security functions on Bosch’s ECU architecture would have been predictable and obvious. (EX1050, 94-96, 1064-1065; EX1003, ¶¶450-455.)

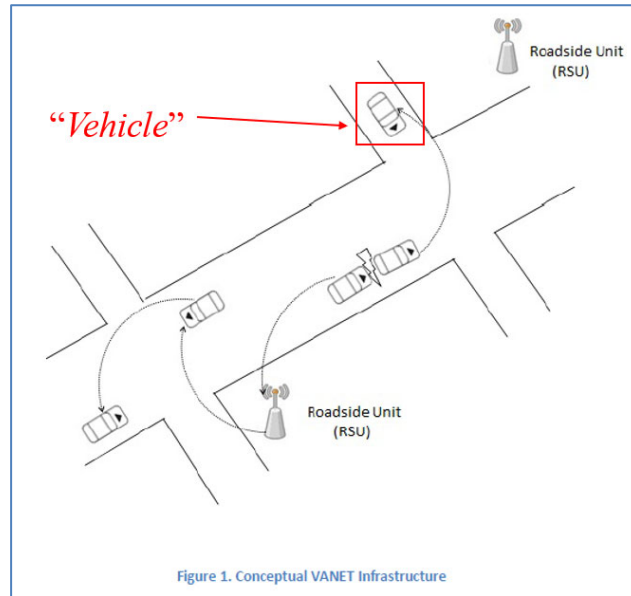
## **2. Independent Claim 1**

### **a. Limitation 1[pre]**

#### ***A vehicle, comprising:***

Amirtahmasebi is directed to the security of vehicular networks and describes the robustness of in-vehicle networks with respect to safety and security failures. (EX1019, 12, 47.) The reference explains that its purpose is to examine “security vulnerabilities in vehicular networks and their countermeasures, both in inter-vehicle (VANET) and in-vehicle networks, in order to secure the vehicular networks.” (EX1019, 7.) Figure 1 of Amirtahmasebi is expressly described as a “conceptual model” of a Vehicular Ad Hoc Network and reflects the reference’s focus on security

mechanisms implemented within “[a] vehicle.” (EX1019, 13, Fig. 1; EX1003, ¶¶165-168.)



**EX1019, Figure 1<sup>7</sup>**

**b. Limitation 1[a]**

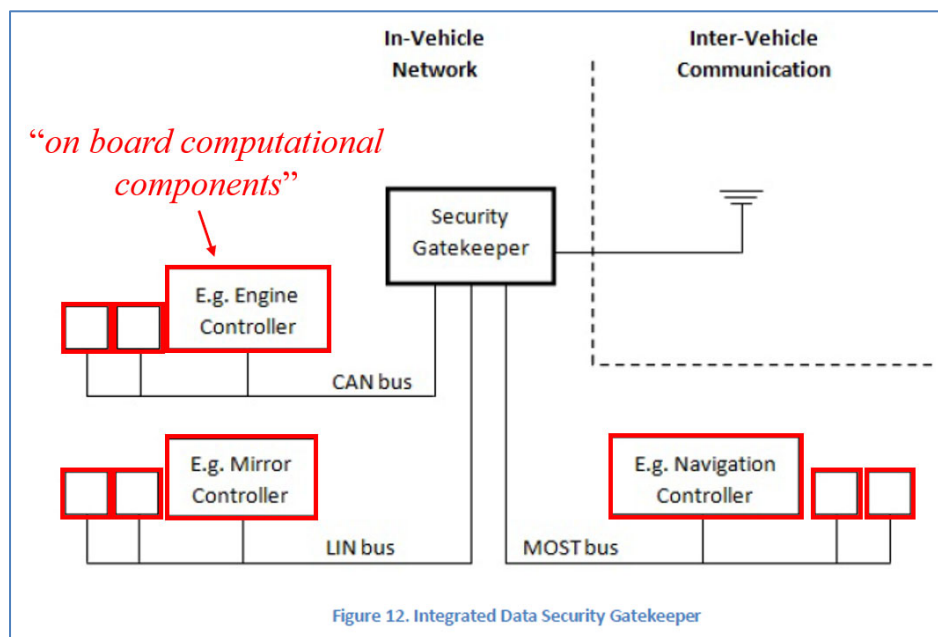
***a plurality of on board computational components;***

Amirtahmasebi describes that in-vehicle networks “are a combination of Electronic Control Units (ECU), sensors and actuators.” (EX1019, 11.) It further explains that modern vehicles include numerous ECUs distributed across the vehicle’s internal network architecture. (EX1019, 24.) Figure 2 and Figure 12 of Amirtahmasebi illustrates this arrangement by showing multiple ECUs throughout the network, represented by the white boxes within the depicted in-vehicle

---

<sup>7</sup> All annotations added by Petitioner, unless indicated otherwise.

communication structure. (EX1019, 24, 40, Fig. 2, Fig. 12; EX1003, ¶¶169-170.)



**EX1019, Figure 12**

A PHOSITA would have understood that these ECUs perform onboard computational tasks and are responsible for processing data essential to the operation of the vehicle. Amirtahmasebi organizes ECUs into the following categories depending on the criticality of their functions and the safety implications of their failure: powertrain ECUs; safety ECUs (e.g., airbag); comfort ECUs (e.g., temperature control); infotainment ECUs; and telematics ECUs. (EX1019, 24-25.) Amirtahmasebi emphasizes that “critical ECUs,” including powertrain ECUs, must be secured against cyberattacks, and discusses the need for “new gateway ECUs” incorporating increased computational resources to carry out their security functions. (EX1019, 55; EX1003, ¶¶171-172.)

In view of these disclosures, a PHOSITA would have understood Amirtahmasebi discloses ECUs which are “*a plurality of on board computational components.*” (EX1003, ¶¶173-175.)

**c. Limitation 1[b]**

*a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and*

Amirtahmasebi explains that vehicular networks “have several vulnerabilities and are exposed to different cyber attacks,” and because cyberattacks “can be a threat to the vehicle and its passengers” a “new infrastructure” is needed to protect in-vehicle networks from untrusted communications. (EX1019, 7.) A PHOSITA would have understood this disclosure as directing the creation of a security boundary around the vehicle’s internal ECUs to prevent infiltration by untrusted external sources. (EX1003, ¶176.)

Amirtahmasebi continues by disclosing “wireless gateways” connecting vehicles to other vehicles and roadside units. (EX1019, 13.) A PHOSITA would have understood “wireless gateways” as being external entry points through which untrusted data can reach in-vehicle systems. Amirtahmasebi also explains modern vehicles include multiple internal bus networks (e.g., LIN, MOST, CAN, FlexRay) each comprising ECUs that provide different functionality. (EX1019, 24-26; EX1003, ¶¶177-178.)

While these networks may have been “originally designed to work in isolation,” Amirtahmasebi teaches they are now connected to external networks to receive external communications (e.g., via Firmware Updates Over the Air “FOTA”). (EX1019, 28, 37-38.) These external communications have resulted in vehicle networks becoming susceptible to infiltration. (*Id.*) By connecting internal networks to external networks “without securing them,” attackers can perform unauthorized actions that may disable ECUs and cause safety-critical failures. (EX1019, 28.) Attacks may include sophisticated “vehicle viruses” embedded in code sent to the vehicle’s network through a FOTA process. (EX1019, 37-38.)

A PHOSITA would have therefore understood Amirtahmasebi teaches the formation of a logical “*perimeter network*” separating one or more internal vehicle ECUs from untrusted external communications. (EX1003, ¶¶180-182.) A PHOSITA would have understood Amirtahmasebi’s “*perimeter network*” may be formed to separate a specific ECU, i.e. the Navigation Controller, or multiple ECUs, sensors, or modules from communications with external sources as illustrated in Figure 12 below. (EX1003, ¶¶179-183.)

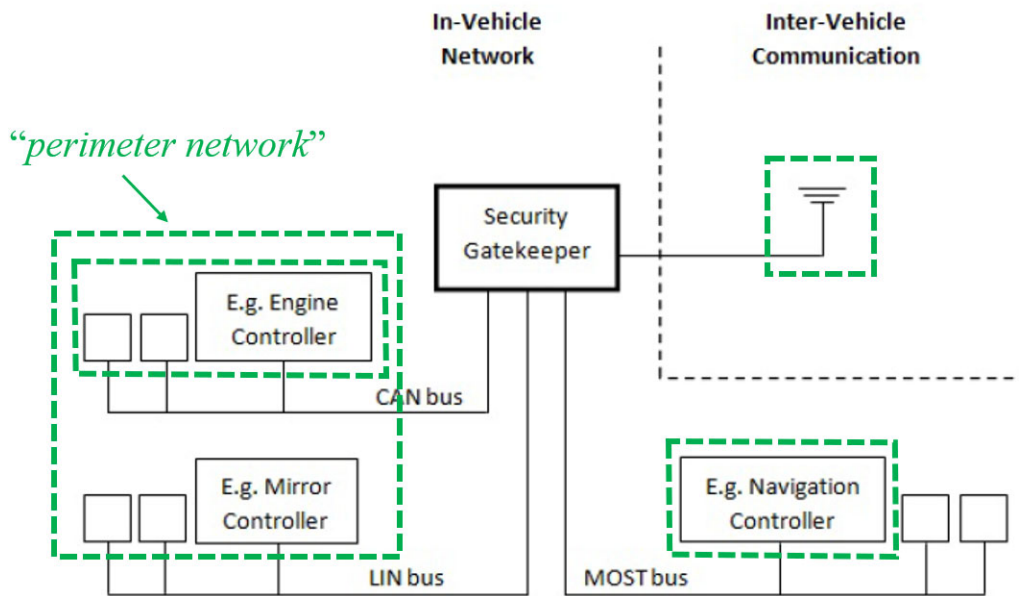


Figure 12. Integrated Data Security Gatekeeper

### EX1019, Figure 12

Amirtahmasebi teaches security methods and solutions that would allow the formation of such a logical “*perimeter network*” boundary to protect the ECUs residing within the vehicle.<sup>8</sup> (EX1019, 19-23, 39-50.) For instance, Amirtahmasebi teaches a “firewall mechanism within the network gateways” that would be used to

---

<sup>8</sup> Such security methods and solutions discussed by Amirtahmasebi include digital certificates issued by a Certificate Authority via Public Key Infrastructure (PKI). (EX1003, ¶¶188-191.) A PHOSITA would have understood such mechanisms individually or in combination would constitute a “*security mechanism*” implementing a “*security measure*” as required by this claim limitation. (EX1003, ¶¶192-193.)

enforce MAC- or signature-based authentication and subnet-specific authorization rules. (EX1019, 45-46.) Amirtahmasebi teaches the usage of a firewall mechanism would allow only messages from “valid and authentic ECUs” to pass through the firewall and be received by the internal bus networks. (EX1019, 45-46; EX1003, ¶¶198-201.)

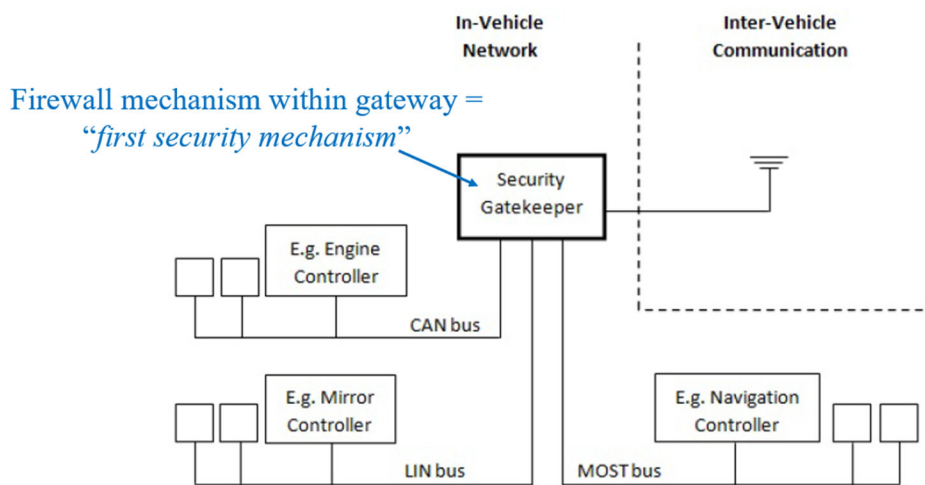


Figure 12. Integrated Data Security Gatekeeper

### EX1019, Figure 12

Amirtahmasebi further discloses an Intrusion Detection System or “IDS” can be added to the firewall mechanism-implemented gateway “to further enhance the communication and system security.” (EX1019, 46.) Amirtahmasebi discusses the IDS monitors, inspects, and analyzes messages and data exchanged within the vehicle to detect abnormalities indicative of malicious behavior. (EX1019, 41-42; EX1003, ¶¶194-197.)

A PHOSITA would therefore have understood that Amirtahmasebi’s firewall

mechanism, alone or together with the IDS, is the “*first security mechanism*” that enforces “*security measure[s]*” (i.e., MAC- or signature-based authentication and subnet-specific authorization rules) to form a logical boundary or “*perimeter network*” separating internal ECUs (“*the plurality of on-board computational components*”) from external or untrusted communications. A PHOSITA would have understood this firewall mechanism protects “*the plurality of on board computational components*” (i.e., the ECUs and related devices on the in-vehicle networks) by ensuring that only authorized traffic is allowed into or across the internal communication domain. (EX1003, ¶¶199-203.)

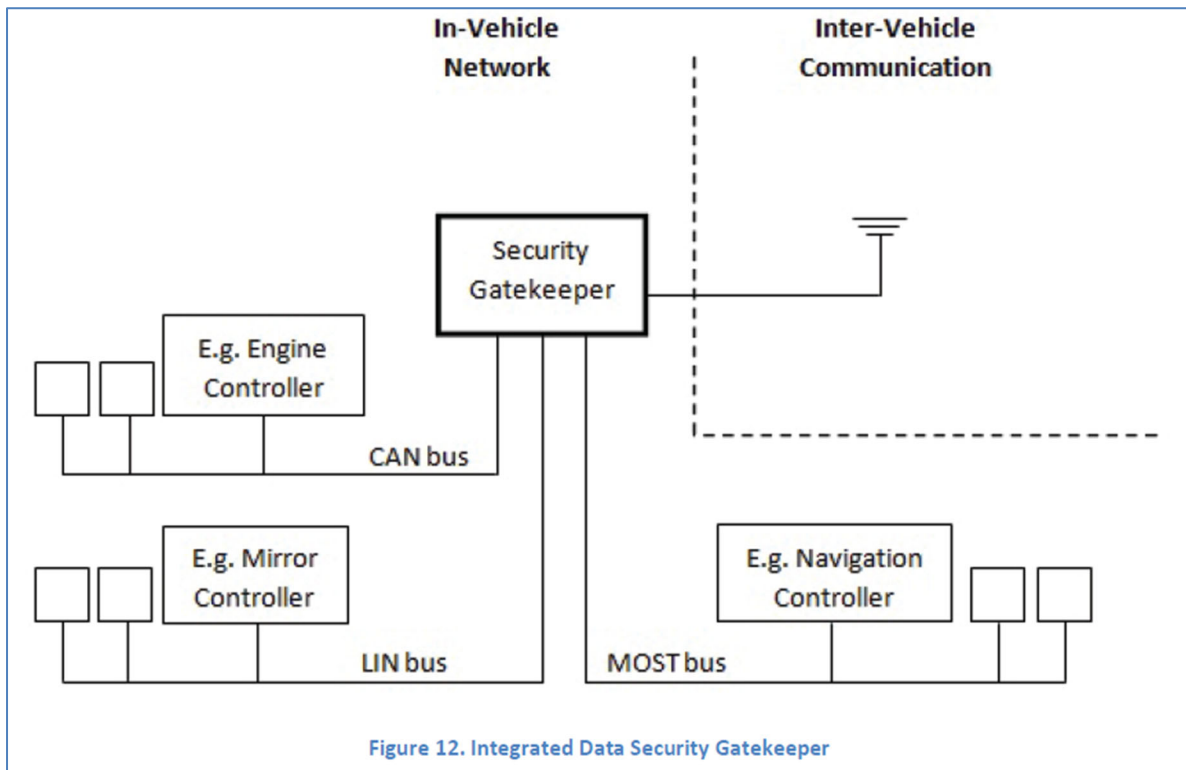
**d. Limitation 1[c]**

***a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,***

Amirtahmasebi discloses the internal vehicular networks (e.g., CAN, LIN, and MOST) may be “connected by gateways in order to be able to communicate with each other as well.” (EX1019, 24.) Amirtahmasebi teaches these gateways, or “integrated gatekeepers,” operate as intermediary ECUs between each internal network. (EX1019, 24, 40; EX1003, ¶¶204-205.)

Amirtahmasebi further illustrates the gateway/gatekeeper positioned between external “inter-vehicle communication” and the internal bus networks. (EX1019, 40, Fig. 12.) A PHOSITA would have understood these gatekeepers as forming the

above discussed security boundary around the ECUs of the in-vehicle networks (i.e. a “*perimeter network*”). (EX1003, ¶205.)



**EX1019, Figure 12**

Amirtahmasebi characterizes these gatekeepers as part of its “embedded information security” and “software security” mechanisms. (EX1019, 40-41.)

Amirtahmasebi explains the “firewall mechanism” discussed above may be designed “within network gateways.” (EX1019, 45.) When implemented within the gateway ECUs, the “firewall mechanism” would then be configured to use “message authentication codes (MAC) or digital signatures” to authenticate and authorize messages sent between ECUs. (EX1019, 45-46.) In cases where no MACs or digital signatures are used between ECUs, “the rules of firewalls can be defined

individually, based on each vehicular subnet authorizations,” so that “only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.” (EX1019, 46; EX1003, ¶¶206-210.)

The firewall within the network gateways can also regulate cross-network message flow in order to protect more critical networks; for example:

Restricting the access level of different types of networks to other parts of the bus system can be another approach to defining firewall rules...ECUs of less important networks such as LIN or MOST should not be able to send messages into higher safety relevant and more critical bus systems such as CAN or FlexRay.

(EX1019, 46.)

A PHOSITA would have understood that these firewall and message-inspection functions are implemented as software routines executing on the gateway ECU’s microprocessor. (EX1003, ¶¶211-212.)

Bosch confirms that automotive ECUs employ microprocessor-based microcomputers: the microprocessor is the CPU that processes inputs, executes program instructions, and outputs control signals. (EX1050, 94-96, 1065.) A PHOSITA would have understood the “*microprocessor*” disclosed by the Bosch Handbook would functionally operate and be structurally the same as the “gateways” or “security gatekeepers” ECUs disclosed by Amirtahmasebi. (EX1003, ¶213.)

Therefore, a PHOSITA would have understood that the firewall and IDS logic run on that microprocessor. (EX1003, ¶212.)

Amirtahmasebi explains that attackers may inject “malicious code” into an ECU, causing it to send malformed or invalid frames. (EX1019, 33.) As discussed above, the firewall mechanism and IDS on the gateway detect these anomalies by validating MACs or signatures and comparing message characteristics to expected patterns. A PHOSITA would have understood the gateway/gatekeeper of Amirtahmasebi to be a “*microprocessor-executed network controller*” with logic that inspects, manages, and filters traffic to detect malicious behavior (i.e., “*an instance of a breach of the security measure.*”) (EX1003, ¶¶214-215.)

**e. Limitation 1[d]**

***(ii) determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and***

Amirtahmasebi expressly recognizes that “[v]ehicle networks must be designed in such a way that once one ECU’s security has been compromised, other parts of the network must be able to work fine and not let the compromised ECU disrupt the whole vehicle network.” (EX1019, 39.) A PHOSITA would have understood Amirtahmasebi as teaching the system will evaluate whether a

compromised ECU can be isolated from ECUs that remain unaffected. (EX1003, ¶¶216-219.)

Amirtahmasebi explains that the gateway “firewall mechanism” performs access-control determinations that a PHOSITA would have understood decides whether an ECU can be isolated. (EX1003, ¶221.) Amirtahmasebi teaches that “[r]estricting the access level of different types of networks to other parts of the bus system can be another approach to defining firewall rules” and provides the example that ECUs from lower-criticality networks such as LIN or MOST “should not be able to send messages into higher safety relevant and more critical bus systems such as CAN or FlexRay.” (EX1019, 46.) Amirtahmasebi further notes that “only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.” (EX1019, 46.) A PHOSITA would have understood that Amirtahmasebi’s gateway (“*microprocessor executable network controller*”) having a firewall mechanism determines whether a potentially compromised ECU—identified by failing firewall authentication or authorization—can interact with the remainder of the network, and thus whether it can “*be isolated*” from unaffected ECUs. (EX1003, ¶¶220-221.)

Amirtahmasebi also describes the IDS taking actions can “detect[] communication misbehavior, based on its type, [and] the IDS can take appropriate countermeasures ranging from raising simple intrusion warning messages to even

deactivating the misbehaving ECU.” (EX1019, 46.) A PHOSITA would have understood that “deactivating” an ECU prevents it from transmitting further messages on the shared bus and thus prevents it from interacting with any other ECU. In bus-based systems, where each ECU receives every frame sent by any other ECU, an ECU that is unable to transmit or respond is effectively “isolated.” (EX1003, ¶222.)

A PHOSITA would have recognized that an IDS must determine whether the detected misbehavior warrants isolation before taking that action. The “appropriate countermeasure” taken by the IDS can range from triggering a warning message for minor anomalies, while more severe or malicious patterns may trigger deactivation. (EX1019, 46.) Thus, Amirtahmasebi’s gateway (“*microprocessor executable network controller*”) having the firewall mechanism IDS functionality would evaluate whether the affected ECU “*can*” and should “*be isolated*” from the unaffected ECUs—i.e., whether isolating it is an appropriate and feasible countermeasure. (EX1003, ¶¶222-224.)

**f. Limitation 1[e]**

***(iii) when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of***

***(a) isolate the at least one on board computational component not affected by or potentially affected by***

*the instance of a breach of a security measure from the computational component affected by the instance of a breach of a security measure and*

*(b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,*

This limitation requires that, when a computational component is affected by a security breach, the system performs at least one of two isolation options: (a) isolating the unaffected components from the compromised component, or (b) isolating the compromised component from the unaffected components. The phrase “at least one of” makes clear that the claim does not require both actions—performing either option satisfies the limitation.

As discussed in connection with limitation 1[d], once the security system determines the compromised ECU can be isolated, Amirtahmasebi discloses mechanisms for how to perform that isolation. Amirtahmasebi explains, for instance, the “firewall mechanism” would be designed such that “only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.” (EX1019, 46.)

A PHOSITA would have understood that when an ECU fails authentication or authorization—because it is misbehaving, compromised, or transmitting messages inconsistent with the established security policy—the firewall mechanism

of the gateway prevents that ECU's messages from entering or traversing the in-vehicle network. A PHOSITA would therefore have recognized that Amirtahmasebi teaches the gateway ("*microprocessor executable network controller*") having firewall functionality "*isolates*" the affected ECU ("*the computational component affected by the instance of a breach of a security measure*") from the unaffected ECUs ("*at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure*") on the in-vehicle network by blocking the invalid ECU's messages at the gateway. (EX1019, 46; EX1003, ¶225.)

Isolation is also taught by Amirtahmasebi through the IDS functionality of the gateway. Amirtahmasebi states that, "[i]n case of detected communication misbehavior, based on its type, the IDS can take appropriate countermeasures ranging from raising simple intrusion warning messages to even deactivating the misbehaving ECU." (EX1019, 46.) A PHOSITA would have understood that deactivation of the misbehaving ECU prevents it from transmitting messages on the shared bus and from participating in inter-ECU communication. In the context of a broadcast bus system (such as CAN), preventing an ECU from sending frames means effectively removing that ECU from the networked system. Thus, a PHOSITA would therefore have recognized that Amirtahmasebi teaches the gateway ("*microprocessor executable network controller*") having IDS functionality

“isolates” the affected ECU (“*the computational component affected by the instance of a breach of a security measure*”) from the unaffected ECUs (“*at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure*”) on the in-vehicle network by blocking the deactivating it. (EX1019, 46; EX1003, ¶225-226.)

A PHOSITA would have understood “isolating” the affected ECU also isolates the unaffected ECUs from the compromised component because bus-based in-vehicle networks allow any ECU’s transmission to be received by all other ECUs, blocking or deactivating the misbehaving ECU protects the healthy ECUs from receiving or being influenced by malicious or corrupted messages. A PHOSITA would therefore also have understood the gateway having a firewall mechanism (which prevents the compromised ECU from sending unauthorized messages) and an IDS (which deactivates the misbehaving ECU entirely) separately or together operate to provide “isolating” the unaffected ECU (“*at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure*”) from the affected ECUs (“*the computational component affected by the instance of a breach of a security measure*”). (EX1003, ¶227.)

**g. Limitation 1[f]**

***wherein the isolation is one or more of:***

*(1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure,*

*(2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a **firewall and/or gateway** to enforce a security measure,*

*(3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and*

*(4) activating a second security mechanism in response to the instance of a breach of a security measure.*

Limitation 1[f] recites the isolation must only be “one or more of” four specified isolation options: (1) denying vehicular wireless network access to the affected ECU; (2) directing its communications to a firewall/gateway for enforcement of a security measure; (3) blocking its communications; and (4) activating a second security mechanism. Amirtahmasebi teaches at least option (3), and a PHOSITA would also have understood the disclosed firewall and IDS mechanisms of the gateway satisfy options (1) and (2). (EX1003, ¶228.)

As discussed above, Amirtahmasebi explains the firewall mechanism within the gateway may review MAC or digital signatures of communications as “authentication and authorization” of ECUs. (EX1019, 45-46.) Amirtahmasebi further discusses requiring ECUs to “register themselves” at the Gateway ECU “inside the network in order to be able to send and communicate with other network

nodes,” and failure to register would result in the ECU’s messages be “discarded by the rest of the network.” (EX1019, 45.) Amirtahmasebi further states “only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.” (EX1019, 46; EX1003, ¶229.)

A PHOSITA would have understood that when a gateway “discards” a non-authenticated ECU’s messages, those messages never reach the vehicle network, and the affected ECU cannot receive legitimate responses because it is barred from participating as an authenticated node. A PHOSITA would have understood this constitutes “*isolation*” as “*blocking communications to and from*” the compromised ECU (“*the computational component affected by the instance of a breach of a security measure*”), satisfying option (3) of this limitation. (EX1003, ¶¶230-232.)

Amirtahmasebi also explains the IDS gateway functionality can take increasingly severe countermeasures when it detects malicious behavior, “ranging from raising simple intrusion warning messages to even deactivating the misbehaving ECU.” (EX1019, 46.) A PHOSITA would have recognized that deactivation of the ECU prevents it from transmitting onto or participating in the shared communication bus and thereby blocks all communications to and from the compromised ECU—constituting “*isolation*” as “*blocking communications to and from*” the compromised ECU (“*the computational component affected by the instance of a breach of a security measure*”), satisfying option (3) of this limitation.

(EX1003, ¶232.)

Because a deactivated ECU cannot meaningfully place messages on the bus or receive them, a PHOSITA would have understood this also constitutes “*isolation*” as “*denying vehicular wireless network access*” to the compromised ECU (“*the computational component affected by the instance of a breach of a security measure*”) satisfying option (1) of this limitation. (EX1003, ¶232.)

Amirtahmasebi’s firewall mechanism gateway functionality also satisfies option (2), because directing messages to a gateway firewall for authentication and authorization—before they may be introduced to the network—precisely matches the claim limitation language of “*isolation*” as “*directing communications to and from the computational component...to a firewall and/or gateway to enforce a security measure.*” (EX1019, 45-46; EX1003, ¶230.) A PHOSITA would have understood that every communication involving the compromised ECU is routed to the gateway for enforcement of firewall rules, satisfying this alternative as well. (EX1003, ¶230.)

### 3. Dependent Claim 2

#### a. Limitation 2 ``` [pre] ```

*The vehicle of claim 1, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow,*

***heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource,***

Amirtahmasebi discloses multiple classes of cyberattacks against in-vehicle networks that correspond directly to the enumerated “*security breach instance[s]*.” Amirtahmasebi describes both logical and physical attack vectors, including malware, viruses, spoofing, impersonation, and denial-of-service attacks. (EX1019, 30-38.) A PHOSITA would have understood each of these disclosed attacks as falling squarely within the types of breach instances recited in the dependent claims. (EX1003, ¶234.)

For example, Amirtahmasebi explains that attackers may exploit ECU software-update functionality by “injecting malicious code” resulting in the ECU sending “malformed or invalid frames with wrong intervals on the bus which will confuse other ECUs within the vehicle.” (EX1019, 33.) A PHOSITA would have recognized this as classic “*malware*”—malicious software that compromises a system and causes unauthorized or harmful behavior. (EX1003, ¶¶235-236.)

Amirtahmasebi discloses complex blended attacks, referring to “a combination of these attacks” forming a “vehicle virus” which “can be built into a piece of code and be sent to the vehicle’s network through a FOTA process.” (EX1019, 37-38.) A PHOSITA would have understood that malicious code

spreading, escalating, and causing harm to the vehicle's electronic systems is “a virus,” another explicitly claimed security breach instance. (EX1003, ¶237.) The “building blocks” of this virus—“Read,” “Spoof,” “Drop,” “Modify,” “Flood,” “Steal,” and “Replay”—are described in Figures 4–10. (EX1019, 30-32, Figs. 4–10; EX1003, ¶238.)

Amirtahmasebi also discloses both “logical denial of service” attacks such as “repeatedly sending faulty messages or excessively running a particular program” and “physical denial-of-service” attacks via “signal jamming, data deletion, or communication deactivation” (EX1019, 34, 37.) A PHOSITA would have understood these disclosures as describing “*denial-of-service attacks*,” another enumerated breach instance. (EX1003, ¶¶240-242.)

Amirtahmasebi further describes spoofing attacks, stating: “[s]poof: Due to lack of authentication, the attacker can inject messages targeted to the victim ECU(s) into the network...” (EX1019, 30.) A PHOSITA would have understood this disclosure describes “*spoofing*” another enumerated breach instance. (EX1003, ¶¶243-244.)

Additionally, Amirtahmasebi discusses “impersonation and masquerading attacks,” where “the attacker tries to hide his identity and pretend to be a legitimate node by applying data modification or injection attacks” thereby “abusing other's identities.” (EX1019, 34.) A PHOSITA would have viewed this as a form of

“*identity theft (or MAC-spoofing)*,” another enumerated breach instance. (EX1003, ¶¶245-246.)

Because claim 2 requires only that the “security breach instance is *one or more of*” these types, Amirtahmasebi’s disclosure of multiple instances satisfies this limitation. (EX1003, ¶247.)

**b. Limitation 2[a]**

*wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and*

Limitation 1[c] explains that Amirtahmasebi discloses a gateway ECU operating as a central point of security enforcement protecting the internal vehicle networks. As discussed above, Amirtahmasebi’s gateway would be understood as including a “*microprocessor executable network controller*” for receiving and processing security-related information originating from multiple sources within the system. (EX1003, ¶248.)

First, Amirtahmasebi teaches a firewall mechanism within network gateways that performs authentication and authorization of messages. (EX1019, 45-46.) Amirtahmasebi explains “ECUs must register themselves inside the network in order to be able to send and communicate with other network nodes, and if not, their messages will be discarded by the rest of the network. Gateway ECUs will be in

charge of other ECUs' signature verification and authentication.” (EX1019, 45.)

Amirtahmasebi explains “only messages from valid and authentic ECUs will be able to pass through the firewall rules.” (EX1019, 46.) A PHOSITA would have understood that when the firewall detects a failed authentication or invalid signature, the firewall produces or triggers a security-related alert that the gateway's network controller receives and acts upon. (EX1003, ¶¶249-250.) Amirtahmasebi therefore teaches receiving “*a warning signal*” from both “*a gateway*” and “*a firewall*.”

Second, Amirtahmasebi discloses “a honeypot can be used for gathering attacker's information” serving as a tool for “prevention and early detection of malicious attacks based on studying the attackers' malicious and unauthorized behavior.” (EX1019, 46.) A PHOSITA would have understood that Amirtahmasebi's “*honeypot*,” upon detecting malicious access attempts or behavioral signatures, produces detection output in the form of “*a warning signal*” that would be sent to and processed by the gateway's network controller. (EX1003, ¶¶251-252.)

Third, Amirtahmasebi describes an Intrusion Detection System (IDS) capable of detecting “obvious misuse of Message-IDs,” and that “by adding some IDS functionality to the ECUs, these attacks can be identified and mitigated by the ECUs themselves.” (EX1019, 41.) Amirtahmasebi describes the IDS compares messages against predefined patterns and examines low-level characteristics such as “voltage

amplitudes...clock edges, propagation delays, [and] signal attenuation” to “identify unauthenticated devices which will try to inject messages on the CAN network.” (EX1019, 41.) A PHOSITA would have understood that such ECUs of Amirtahmasebi qualify as “*network nodes impacted by the security breach instance*,” and that when these ECUs detect malicious behavior, they transmit “*a warning signal*” to the network controller for further action. (EX1003, ¶¶253-259.)

Fourth, a POSA would have understood a “*network probe*” to be hardware or software that monitors network traffic for security-related anomalies, which is performed by the IDS detection modules disclosed in Amirtahmasebi and discussed in limitation 1[b]. (EX1003, ¶257.) Thus, a PHOSITA would have understood the gateway IDS in Amirtahmasebi operates as a “*network probe*” capable of sending “*a warning signal*” associated with a security breach to the network controller within the gateway ECU. (EX1003, ¶258.)

**c. Limitation 2[b]**

*wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.*

As discussed above in connection with limitation 1[b], Amirtahmasebi specifically describes a “firewall mechanism within the network gateways” that authenticates and authorizes messages passing between ECUs. (EX1019, 45-46.) Amirtahmasebi teaches that the gateway firewall may apply “message authentication codes (MAC) or digital signatures” to validate inter-ECU communications. (*Id.*) Amirtahmasebi further discloses that when MACs or digital signatures are not used, the gateway may instead enforce subnet-specific authorization rules—i.e., firewall rules defined at a per-subnetwork level. (*Id.*) In both cases, the result is the same: “only messages from valid and authentic ECUs will be able to pass through the firewall rules and thus be transmitted on the in-vehicle bus system.” (EX1019, 45-46; EX1003, ¶260.)

A PHOSITA would have understood that Amirtahmasebi’s firewall mechanism within the gateway is “*a first security mechanism*” that functions therefore “*isolating the vehicular network by a firewall and/or gateway*” as required by this limitation. (EX1003, ¶264.)

#### **4. Dependent Claim 3**

##### **a. Limitation 3[pre]:**

*The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational component,*

Amirtahmasebi repeatedly explains that security breaches may occur within the vehicle’s own embedded electronic systems—specifically, its Electronic Control Units (ECUs). (EX1019, 33.) Amirtahmasebi teaches attackers may inject malicious code into an ECU of the vehicle by exploiting its software-update functionality. (EX1019, 33.) Such malicious code “will be downloaded to the ECU and will result in sending malformed or invalid frames with wrong intervals on the bus which will confuse other ECUs within the vehicle.” (EX1019, 33.) Amirtahmasebi further emphasizes that vehicle networks must be designed to tolerate the compromise of one of these ECUs, explaining that “once one ECU’s security has been compromised, other parts of the network must be able to work fine and not let the compromised ECU disrupt the whole vehicle network.” (EX1019, 39.) A PHOSITA would have recognized that this disclosure explicitly identifies “*the computational component affected by the security breach instance*” as an ECU located physically within the vehicle, and therefore “*an on board computational component.*” (EX1003, ¶¶266-268.)

**b. Limitation 3[a]:**

***wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and***

Amirtahmasebi classifies ECUs into five categories based on safety criticality.

Powertrain ECUs and vehicle safety ECUs are described as “safety-critical,” because failure of these units poses risks to vehicle safety. (EX1019, 24-25.) By contrast, comfort ECUs, infotainment ECUs, and telematics ECUs are expressly identified as non-safety-related because their failure does not endanger the vehicle or passengers. (EX1019, 24-25.) A PHOSITA would have understood Amirtahmasebi’s disclosure of vehicle systems having “*critical devices*” in the referenced safety-critical ECU units in addition to “*non-critical devices*” in the referenced non-safety-related ECU units, all of which are in the vehicle and thus comprise the “*plurality of on-board computational components.*” (EX1003, ¶¶269-272.)

**c. Limitation 3[b]:**

***wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.***

As explained above in limitation [1b], Amirtahmasebi discloses that a vehicle contains multiple in-vehicle subnetworks—such as CAN, LIN, MOST, and FlexRay—that the ECUs residing those networks are isolated by the logical “*perimeter network*”. A PHOSITA would have understood this “*perimeter network*” functions to separate internal ECUs from untrusted external communications, thereby protecting various ECUs within those subnetworks, including the critical

and non-critical devices discussed in limitation [3a], which are the “*on-board computational components*” referenced in this limitation. (EX1003, ¶273.)

Amirtahmasebi further teaches distributed and semi-central security architectures in which ECUs possess “autonomous security functionality,” including ECU-level intrusion detection. (EX1019, 41, 49.) Because these detections and countermeasures occur within a shared bus—e.g., on the CAN network—a PHOSITA would have understood that both the compromised ECU (the “*computational component affected by the security breach instance*”) and the unaffected ECU(s) it communicates with (“*the at least one on board computational component*”) reside within the same perimeter-protected in-vehicle network. (EX1003, ¶¶274-276.)

## 5. Dependent Claim 4

### a. Limitation 4[pre]

***The vehicle of claim 2, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and***

As described above in limitation 1[b], Amirtahmasebi teaches that the “*perimeter network*” is formed by the security mechanism that separates and therefore protects ECUs within in-vehicle subnetworks from untrusted external communications. (EX1019, 24, 28, 32, Fig. 12.) A PHOSITA would have

understood these protected subnetworks contain ECUs that serve as the vehicle's "*on-board computational components*." (EX1003, ¶¶176-202, 280-281.)

Amirtahmasebi also discloses that malicious behavior may originate from ECUs or devices outside the protected subnetwork. For example, the reference teaches that security rules may prevent ECUs on "less important networks such as LIN or MOST" from sending messages into "more critical bus systems such as CAN or FlexRay." (EX1019, 46.) A PHOSITA would have understood that when firewall rules block a LIN- or MOST-based ECU from communicating with ECUs on a protected CAN network, the misbehaving ECU is "*outside the perimeter network*" that contains the protected CAN-based ECUs. (EX1003, ¶¶282-285.)

Similarly, Amirtahmasebi describes attacks originating from external computing systems, including vehicle-virus attacks delivered through FOTA updates or VANET interfaces. (EX1019, 32, 37-38.) A PHOSITA would have understood these external systems lie outside the security boundary protecting the in-vehicle networks. (EX1019, 32, 37-38.)

Thus, whether the source of the breach is (1) an ECU on a different, restricted subnetwork or (2) an external system sending malicious software or messages, a PHOSITA would have understood that Amirtahmasebi discloses a "*computational component affected by the security breach instance*" that is "*outside the perimeter network*" contains the protected on-board ECU(s) (at least one of "*plurality of on*

*board computational components*”). (EX1003, ¶¶286-288.)

**b. Limitation 4[a]**

*wherein the at least one board computational component is **one or more of** an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.*

Amirtahmasebi discloses ECUs on the vehicle are classified by functional role and safety criticality, including powertrain ECUs and vehicle safety ECUs (both safety-critical), as well as comfort, infotainment, and telematics ECUs (non-safety-critical). (EX1019, 24-25.) As discussed above, a PHOSITA would have understood these ECUs are computational components. A PHOSITA would have understood that safety-critical ECUs such as the powertrain ECU are “*critical system controllers*,” while comfort/infotainment/telematics ECUs correspond to “*non-critical system controllers*”. (EX1003, ¶¶290-291.)

**6. Dependent Claim 5**

**a. Limitation 5[pre]**

*The vehicle of claim 1 wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing*

***the at least one on board computational component and***

The claim language in these limitations is materially identical to that of limitation 4[pre], and a PHOSITA would have understood the analysis to be the same. As explained in connection with limitation 4[pre], Amirtahmasebi teaches that a logical “*a perimeter network*” may be established to protecting selected ECUs within the vehicle from communications from external sources or from ECUs within the vehicle that may have been compromised. A PHOSITA would have also understood a misbehaving ECU on a subnetwork or an external computing device delivering malicious code (e.g. via a FOTA-based vehicle virus) resides “*outside*” that protected perimeter. (EX1003, ¶¶292-293.)

**b. Limitation 5[a]**

***wherein the microprocessor executable network controller analyzes the security breach instance by **one or more** of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.***

As discussed above in limitation [2a], Amirtahmasebi describes an IDS that analyzes network behavior by comparing message activity against predefined patterns and known indicators of malicious activity. Amirtahmasebi explains that the IDS “compar[es] incoming/outgoing messages with predefined patterns,” and that these patterns—such as message-frequency profiles and low-level

communication characteristics—must be “defined as malicious behavior.” (EX1019, 41.) Amirtahmasebi further states that “IDS systems must compare its existing data with some reference data in order to be able to perform intrusion detection” confirming that behavior is evaluated relative to historical or baseline behavior. (EX1019, 41; EX1003, ¶294.)

Amirtahmasebi also discloses both (1) rule-based detection—where “predefined actions, behaviors and combinations are stored in a signature/rule database and network traffic will be compared with the values in the database”—and (2) anomaly-based detection, where the system identifies deviations from “normal actions” defined in advance. (EX1019, 42.) A PHOSITA would have understood these disclosures as comparisons to templates characteristic of differing types of attacks, and as applying rules to determine whether the observed behavior is malicious. (EX1003, ¶295.)

A PHOSITA would have understood that Amirtahmasebi’s gateway “*microprocessor executable network controller*” analyzes a security-breach instance because the disclosed IDS reviews message behavior over time—i.e., “*reviewing historical behavior*”—and compares current traffic to established baselines. A PHOSITA would have understood the gateway IDS then evaluates that behavior against templates of known malicious actions (rule-based detection) and predefined normal behavior (anomaly-based detection) (“*comparing the behavior to templates*

*characteristic of differing types of attacks*”), to determine whether the activity indicates an attack. (EX1003, ¶¶296-298.)

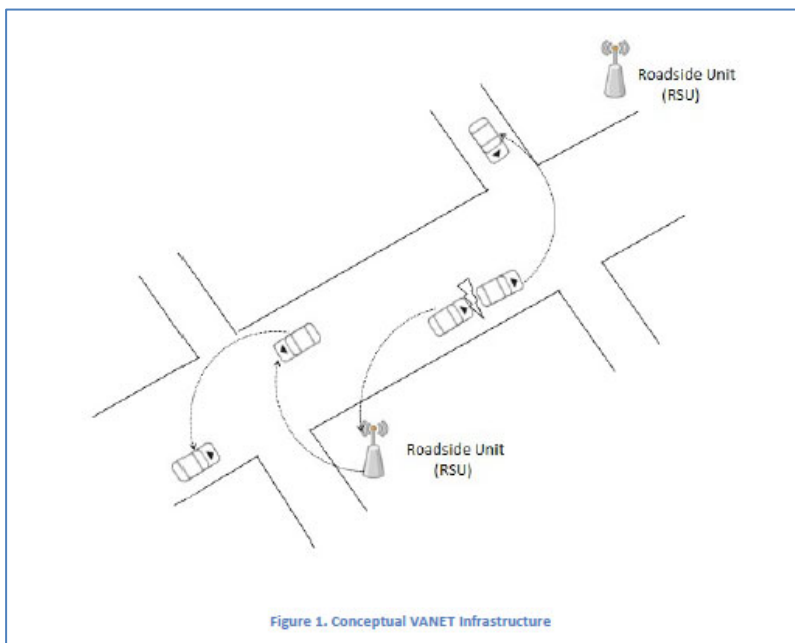
**7. Dependent Claim 6**

**a. Limitation 6[pre]**

*The vehicle of claim 1, wherein the computational component affected by the security breach instance is an external computational device and*

Amirtahmasebi expressly teaches “logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication,” and that an “external attacker... can exploit the available wireless communication interface used for VANET applications.” (EX1019, 32; EX1003, ¶¶300-302.)

Amirtahmasebi also teaches a vehicle may be targeted by “external attackers such as a road-side attacker using his laptop computer to launch an attack scenario.” (EX1019, 21.) Amirtahmasebi explains such attacks may include transmission of “Bogus Information” that inject false messages into the vehicle’s network by “outsiders.” (EX1019, 15; EX1003, ¶¶303-304.)



**EX1019, Figure 1**

As discussed above, Amirtahmasebi discloses an “integrated gatekeeper” that is “used as a connection boundary between inner and outer vehicle networks.” (EX1019, 40, Fig. 12.) Amirtahmasebi explains that “[f]rom the attackers’ point of view, the communication channel seems the best entry point... [because external attackers] can perform their attacks and damages remotely.” (EX1019, 33.)

A PHOSITA would have understood Amirtahmasebi’s “*external device*”—such as a remote laptop or other off-vehicle node—is a “*computational component affected by the security breach instance*” as it initiates a security breach or attack scenario directed at the vehicle’s internal ECUs. (EX1003, ¶¶305-306.)

**b. Limitation 6[a]**

*wherein the at least one on board computational component not affected by the security breach instance*

***is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.***

A PHOSITA would have understood this limitation to mean the vehicle's wireless communication path would refuse access to the external device launching the attack, thereby preventing any of its transmissions from reaching the in-vehicle network and isolating the on-board components. (EX1003, ¶307.)

Amirtahmasebi explains digital signatures and certificates would be used to exclude external attackers so that “external nodes will not be able to send messages within the corresponding domain.” (EX1019, 21.) Amirtahmasebi further explains the vehicle's gatekeeper/gateway would “identify and remove the malicious behaving or defective nodes by revoking their certificates.” (*Id.*)

A PHOSITA would have understood that Amirtahmasebi's certificate-based access control and gatekeeper functionality teach isolation of on-board components, because the gateway evaluates whether the “*external computational component*” possesses a valid certificate—i.e., it “*denies vehicular wireless network access*” to unauthorized devices—and enforces that determination by blocking or revoking access for malicious or untrusted external nodes. A PHOSITA would have further understood that this denial of wireless access prevents any transmissions from the external computational device from reaching the in-vehicle network, thereby

“isolating” the unaffected on-board computational components from the security-breach instance. (EX1003, ¶¶308-311.)

## 8. Dependent Claim 7

*The vehicle of claim 1, wherein **at least one of the following is true about the isolation:***

**[a]** *communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway **and/or** firewall are redirected through and filtered by the gateway **and/or** firewall and*

**[b]** *communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.*

Claim 7 recites that “at least one of the following” options be “true.” During prosecution, this claim was evaluated as option (a) and (b) as shown above. (EX1002, 631-632.) During prosecution, PO removed the indication of (a) and (b). (EX1002, 658-660.) Petitioner evaluates this claim as broken up above showing two options: a and b, and as explained below Amirtahmasebi discloses limitation [b].

Amirtahmasebi discloses “a firewall mechanism” implemented “within [the] network gateway[.]” ECU. (EX1019, 45.) Amirtahmasebi teaches “only messages from valid and authentic ECUs” are permitted to traverse the gateway and be

transmitted on the in-vehicle bus; invalid or unauthenticated messages are discarded. (EX1019, 46.) This firewall also prevents ECUs from lower-security networks (e.g., LIN or MOST) from sending messages into higher-criticality networks such as CAN or FlexRay. (*Id.*) A PHOSITA would have understood that because the firewall gateway in Amirtahmasebi prevents messages from unauthenticated or invalid ECUs from traversing the network boundary, the gateway “blocks”—either entirely or partially—communications between a compromised ECU (“*the computational component affected by the security breach instance*”) and a “*not affected*” ECU operating on the vehicular wireless network (such as a navigation ECU). (EX1003, ¶¶315-321.)

## 9. Dependent Claim 8

### a. Limitation 8[pre]

***The vehicle of claim 1, wherein the at least one computational component is inside of a perimeter network of the vehicle, wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,***

As discussed with regards to limitation 1[a], Amirtahmasebi discloses vehicles having “a combination of Electronic Control Units (ECU).” (EX1019, 11.) As described above in limitation 1[b], Amirtahmasebi teaches that a perimeter network is formed by the security mechanism protecting in-vehicle subnetworks

such as CAN, LIN, MOST, and FlexRay. (EX1019, 24, 28, 32; Fig. 12.) A PHOSITA would have understood these subnetworks include the ECUs that make up the vehicle's on-board computational components. (EX1003, ¶¶176-202, 326.)

Amirtahmasebi discloses ECUs on the vehicle are classified by functional role and safety criticality, including powertrain ECUs and vehicle safety ECUs (both safety-critical), as well as comfort, infotainment, and telematics ECUs (non-safety-critical). (EX1019, 24-25.) Amirtahmasebi emphasizes security risks from external wireless links and proposes robust architectures, including an integrated gatekeeper, firewall, and IDS, to protect internal networks and ensure critical ECUs remain unaffected by breaches. (EX1019, 40-41, Fig. 12). As discussed for claim 1, a PHOSITA would have understood these ECUs would be separated from external sources by a logical "*perimeter network*" and once separated, the ECUs would be the "*at least one computational component is inside of a perimeter network of the vehicle.*" (EX1003, ¶¶327-328.)

Amirtahmasebi explains that "ECU firmware must be possible to update in order to have maximum performance and fix occasional software bugs" (EX1019, 27.) Amirtahmasebi further discloses that "[v]ehicles can connect to the manufacturer's web portal and download the software to their respective ECUs," which is accomplished using "Firmware Over the Air (FOTA)" wireless connections where the ECU is "reflash[ed]" and new firmware is "installed" (EX1019, 28.)

Amirtahmasebi also recognizes that this FOTA process introduces security vulnerabilities because it can be exploited so that malicious code (e.g., a virus) can be wirelessly sent and injected into an ECU that is connected to the vehicular wireless network by a gateway. (EX1019, 33, 47.) A PHOSITA would have therefore understood that an ECU capable of receiving such a FOTA update—such as a Powertrain ECU—would be indirectly “*in a vehicular wireless network*” by virtue of its connection to a gateway designed to receive FOTA requests intended for that ECU. (EX1003, ¶¶328-331.)

**b. Limitation 8[a]**

*wherein the computational component affected by the security breach instance is a node on the vehicular wireless network and physically **and/or** logically positioned outside of but interiorly **and/or** internally to the perimeter network, and*

Again, Petitioner construes “*and/or*” for purposes of this petition as being “*or*.” Amirtahmasebi teaches that a firewall mechanism “within the gateway” (i.e., gatekeeper) operates as the node between external communications and the vehicle’s internal networks, monitoring and controlling message flow to prevent malicious traffic. (EX1019, 40, Fig. 12; EX1003, ¶334.)

Amirtahmasebi teaches that a firewall mechanism, implemented as a “data gatekeeper” within a network gateway, inspects and manages information exchanged between inner and outer vehicle networks to ensure integrity and

confidentiality. (EX1019, 40, 45, Fig. 12.) This gatekeeper controls message flow to block malicious communications, while IDS can detect misbehavior and take countermeasures, including disabling a compromised ECU (“*computational component affected by the security breach instance*”). (EX1019, 42.) Amirtahmasebi further explains that logical attacks may be launched internally or remotely via wireless interfaces, making the communication channel “the best entry point” for attackers (EX1019, 32-33.) Such attacks target computational components—including ECUs, telematics modules, and external devices connected via Bluetooth or Wi-Fi—that operate as “*node[s] on the vehicular wireless network.*” (EX1019, 21, 40–41, Fig. 12; EX1003, ¶¶334-339.)

Petitioner notes the claim language and the ’100 Patent fail to provide a clear explanation of how a component could simultaneously be inside and outside the recited “*perimeter network.*” For purposes of this petition, a PHOSITA would have understood this limitation to describe a dynamic condition: an ECU initially resides within the perimeter network when unaffected, but upon detection of a security breach, the logical perimeter network is reconfigured to isolate the compromised ECU. During this transition, the ECU moves from an internal position to an external position relative to the logical “*perimeter network.*” A PHOSITA would have therefore understood this limitation to be satisfied by an ECU that is logically repositioned from an internal to an external position when “*affected by a security*

*breach.*” (EX1019, 15, 32-33, Fig. 12; EX1003, ¶341.)

**c. Limitation 8[b]**

*wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions in the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.*

Petitioner construes “*and/or*” for purposes of this petition as being “*or*.”

Amirtahmasebi discloses that the vehicle implements encryption for communications exchanged between ECUs within the bus system, explaining that the system “encrypt[s] the transmitted information between ECUs” using combinations of symmetric and asymmetric encryption to secure internal messages. (EX1019, 45.) A PHOSITA would have understood this encryption amounts to end-to-end encryption of ECU-to-ECU communications on the internal bus. (EX1003, ¶345.)

A PHOSITA would have understood that applying encryption directly to ECU traffic discloses enabling a “*critical communication security mechanism*” as recited in Limitation 8[b]. A PHOSITA would further have understood encrypting internal bus communications prevents a compromised computational component—such as

the component affected by the security-breach instance—from accessing, interpreting, or interfering with protected ECU data. This cryptographic protection therefore isolates the compromised component from other nodes of the bus. (EX1003, ¶346.)

Thus, a PHOSITA would have understood Amirtahmasebi teaches each requirement of Limitation 8[b]: “*isolation is effected*” and achieved through use of a security mechanism of encryption of information transmitted between the ECUs (“*a critical communication security mechanism*” as “*end-to-end encryption*”). (EX1003, ¶347.)

#### **10. Independent Claim 9 and 17**

As shown in the Comparison Chart of the Independent Claims (Appendix B), the limitations recited by claims 9 and 17 are nearly indistinguishable from the limitations recited by claim 1. To the extent a limitation is different, Petitioner addresses it below. For all similar limitations, Claims 9 and 17 are unpatentable for the same reasons expressed with regard to claim 1.

##### **a. Limitation 9[pre] and 17[pre]**

For claim 9, Amirtahmasebi clearly describes security-enhancing procedures that a PHOSITA would have recognized as methods performed by a vehicle’s onboard systems. (EX1003, ¶¶354-357, EX1019, 20-21, 41.)

*See* claim 1[pre]. (EX1003, ¶¶166-168, 401-402.)

**b. Limitations 9[a] and 17[a]**

Limitation 9[a] is a method claim which begins by reciting “*in a vehicle comprising*” which is shown by 1[pre].

For the remainder of limitations 9[a]/17[a], *see* 1[a]. (EX1003, ¶¶169-175, 358-360, 403.)

**c. Limitations 9[b] and 17[b]**

Limitation 17[b] additionally recites “*a non-transient, tangible computer readable medium comprising...*” (See Appx. B.) Amirtahmasebi teaches each ECU is controlled by firmware responsible for communication and task execution, and that “sensitive and valuable information must be securely stored.” (EX1019, 24, 51.) Bosch teaches a PHOSITA that an ECU is a microcomputer consisting of a microprocessor. Bosch also teaches the “microprocessor contains the controller ... which ensures implementation of the commands stored in the program memory.” (EX1050, 94-96.) A PHOSITA would have understood an ECU is a non-transient, tangible microcomputer including readable program memory (“*readable medium*”). A PHOSITA would have understood the functions disclosed by Amirtahmasebi reside in “*non-transient, tangible computer-readable media*” (e.g., flash memory, EEPROM) embedded in each ECU. These media store firmware, cryptographic keys, certificates, IDS patterns, and secure-storage data—i.e., the first security mechanism is implemented using persistent memory. (*Id.*; EX1003, ¶¶404-407.)

*See* 1[b]. (EX1003, ¶¶176-202, 361-362, 408-409.)

**d. Limitations 9[c] and 17[c]**

Limitation 17[c] additionally recites “*on board a selected vehicle that, when executed....*” Amirtahmasebi teaches each ECU is controlled by firmware responsible for communication and task execution, and that “sensitive and valuable information must be securely stored.” (EX1019, 24, 51.) Bosch confirms that a “microprocessor represents the integration of a computer's central processing unit on a single chip” and that a “controller ensures implementation of the commands stored in the program memory.” (EX1050, 94-96.) This confirms to a PHOSITA that the controller would operate to “*execute*” the stored software programs like those disclosed by Amirtahmasebi. (EX1003, ¶¶410-412.)

*See* 1[c]. (EX1003, ¶¶204-215, 363-364, 413.)

**e. Limitation 9[d] and 17[d]**

Limitation 9[d] uses slightly different wording, than claim 1, but this would not have changed a PHOSITA’s understanding of the function. In each case, the controller must evaluate whether the compromised ECU can be separated from unaffected ECUs, exactly as Amirtahmasebi teaches through firewall-based filtering and IDS-based deactivation logic.

*See* 1[d]. (EX1003, ¶¶216-224, 365-366, 414-415.)

**f. Limitations 9[e] and 17[e]**

Limitation 9[e] recites a “*microprocessor executable network controller.*” Amirtahmasebi teaches an ECU that is controlled by firmware responsible for communication and task execution, and that “sensitive and valuable information must be securely stored.” (EX1019, 24, 51.) Bosch confirms that a “microprocessor represents the integration of a computer's central processing unit on a single chip” and that a “controller ensures implementation of the commands stored in the program memory.” (EX1050, 94-96.) This confirms to a PHOSITA that Amirtahmasebi’s ECU is a microprocessor controller that operates to execute stored software programs.

*See* 1[e]. (EX1003, ¶¶225-227, 367-369, 416-417.)

**g. Limitations 9[f] and 17[f]**

*See* 1[f]. (EX1003, ¶¶228-232, 370-372, 418-420; EX1019, 45-46.)

**11. Dependent Claims 10 and 18**

As shown in the Comparison Chart of the Dependent Claims (Appendix C), the limitations recited by claims 10 and 18 are identical to claim 2. Claims 10 and 18 are unpatentable for the same reasons expressed with regard to claim 2. (EX1003, ¶¶234-264, 374-377, 422-425.)

**12. Dependent Claims 11-16 and 19-24**

As shown in the Comparison Chart of the Dependent Claims (Appendix C),

the limitations recited by claims 11-16 and 19-24 are nearly identical to the limitations of claims 3-8. Petitioner therefore relies on its analysis from claims 3-8 as indicated below.

**a. Claims 11 and 19**

*See* claim 3. (*See* EX1003, ¶¶265-276, 378-382, 426-429.)

**b. Claims 12 and 20**

*See* claim 4. (*See* EX1003, ¶¶277-291, 383-385, 430-432.)

**c. Claims 13 and 21**

*See* claim 5. (*See* EX1003, ¶¶292-298, 386-388, 433-435.)

**d. Claims 14 and 22**

*See* claim 6. (*See* EX1003, ¶¶299-311, 389-394, 436-438.)

**e. Claims 15 and 23**

*See* claim 7. (*See* EX1003, ¶¶315-321, 395-396, 439-440.)

**f. Claims 16 and 24**

*See* claim 8. (*See* EX1003, ¶¶326-347, 397-400, 441-444.)

**B. Ground 2: Independent Claims 1, 9, and 17 are Obvious Over Spaur and Peirce**

**1. Rationale to Combine**

It would have been obvious to a PHOSITA to combine Spaur’s vehicle network system with Peirce’s filtering system to improve safety and security. Spaur expressly states its description is not limiting and allows “variations and

modifications commensurate with the above teachings[.]” (EX1020, [0233].) Both references address vehicle network security. (EX1020, Abstract, [0001]; EX1021, Abstract, 1:5-7.) Spaur discloses a centralized security controller that “ensur[es] secure access to and control[s] [the] use of resources in the vehicle.” (EX1020, Abstract, [0010], [0042], [0048], [0051]-[0052]; EX1003, ¶¶546-549.)

Peirce discloses transmit and receive filters that block corrupt or unauthorized messages before they reach the bus, preventing compromised ECUs or VSMS from affecting other components. (EX1021, Abstract; 7:60-8:8, 8:43-9:3.) These filters may be “physically and/or logically isolated from the ECU,” enabling independent operation even if the ECU is compromised. (EX1021, 9:29-35.) Positioned externally in the communication path, they stop improper traffic before it reaches bus 44. (EX1003, ¶¶550-559.) A PHOSITA would have been motivated to integrate Peirce’s ECU-independent filters into Spaur’s security controller to add isolation capabilities, yielding predictable results—enhanced security through detection and isolation of compromised components. (EX1003, ¶560.) Peirce teaches filters implemented as separate hardware blocks, such as ASICs, and software logic for validating message contents and terminating unauthorized transmissions. (EX1021, 7:40-43, 8:41-9:3, 9:8-12, 9:29-35, 10:47-51.)

Combining these known elements would have been straightforward and within the skill of the art. A PHOSITA would have combined Spaur and Peirce

because both address the same problem—securing in-vehicle communications—and Peirce provides a known, predictable technique for enhancing systems like Spaur’s centralized controller. The combination simply applies each reference according to its established function and yields the expected result: improved detection, filtering, and isolation of improper messages. Neither reference teaches away, and Spaur expressly invites modifications, giving a PHOSITA a reasonable expectation of success in implementing this straightforward improvement. (EX1003, ¶¶561-563.)

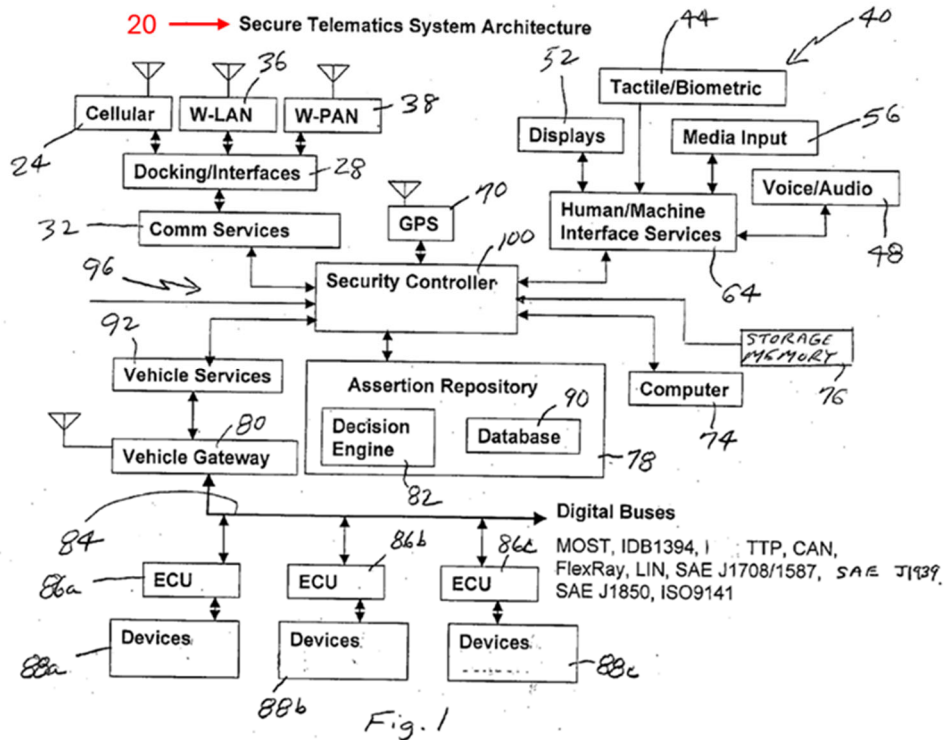
**2. Independent Claim 1**

**a. Limitation 1[pre]**

Spaur discloses that “[i]n accordance with the present invention, system and method are provided for utilizing resources, including proprietary resources in a vehicle.” (EX1020, [0006]; EX1003, ¶¶456-458.)

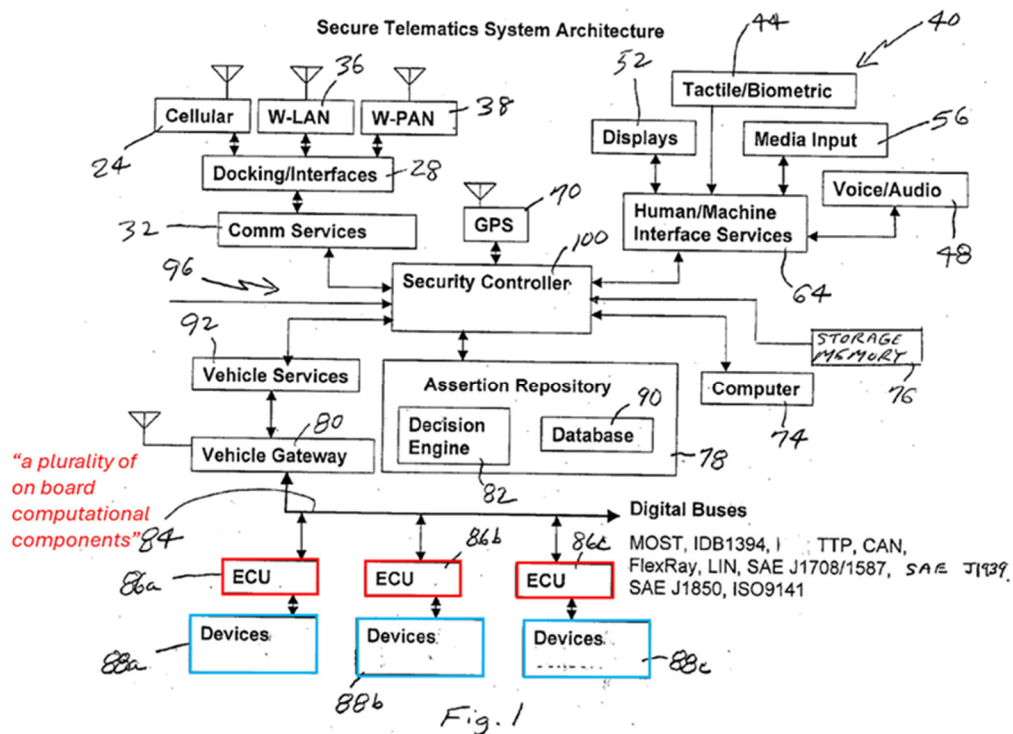
**b. Limitation 1[a]**

Spaur discloses a “telematics secure system 20” that includes multiple subsystems and apparatuses “for providing communications to and from the vehicle.” (EX1020, [0027]; EX1003, ¶459.)



EX1020, Figure 1

Spaur discloses that additional resources are found in the vehicle, including “one or more vehicle buses 84” that communicate with various ECUs 86. (EX1020, [0034].) Spaur further discloses that “[e]ach ECU 86 interfaces one or more of the digital buses 84 with a particular vehicle device 88” and that the vehicle device 88 (annotated in blue below) can include “an engine monitor, an engine temperature sensor, a pressure sensor, an inflator system for activating air bags and/or vehicular tension-producing devices (e.g., for tensioning seat belts).” (EX1020, [0034]; EX1003, ¶¶460-461.)



EX1020, Figure 1

A PHOSITA would have understood that Spaur’s disclosure of the ECUs 86 implementing subsystems (e.g., body control, engine control, telematics control), indicates that the ECUs act as “on board computational components” because each of these subsystems requires active processing, software execution, and real-time decision making. (EX1020, [0034].) Spaur further explains that the ECUs 86 interface with vehicle devices 88 (e.g., engine monitor, temperature sensor) indicating that the ECUs 86 receive and interpret data from vehicle devices 88. (EX1020, [0034].) A PHOSITA would have also recognized that many of the vehicle devices 88 themselves generate or condition sensor data, and therefore perform

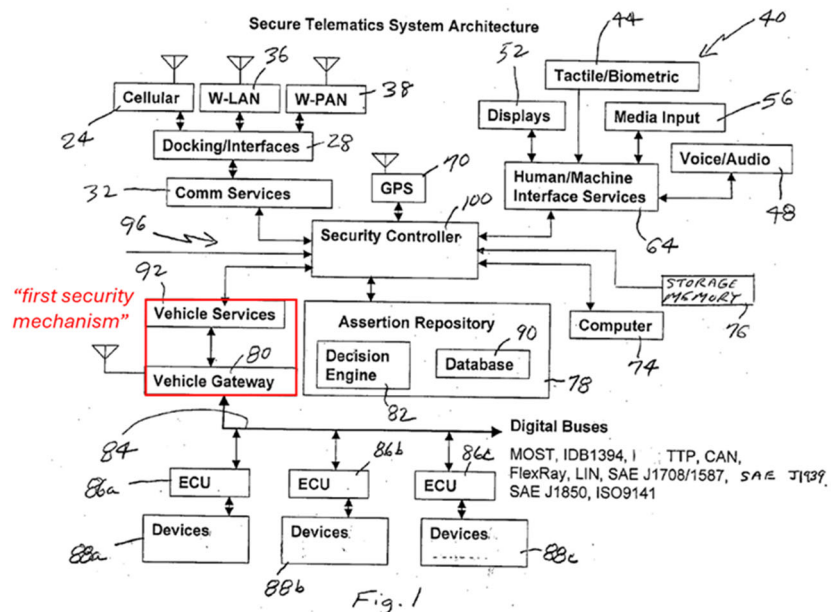
embedded processing functions, and may likewise qualify as “*on board computational components.*” (EX1020, [0034]; EX 1003, ¶¶462-464.)

**c. Limitation [1b]**

Spaur discloses that a “vehicle gateway 80 conventionally communicates with one or more vehicle buses 84 [e.g., MOST, CAN, FlexRay, LIN] to which one or more vehicle devices 88 are connected or communicate with using electronic control units (ECUs) 86.” (EX1020, [0034].) Spaur explains that the gateway 80 “controls access to and use of the vehicle buses 84” and can receive wireless inputs that supply control signals to vehicle devices 88. (EX1020, [0034].) Spaur further discloses that the vehicle gateway 80 is “[i]n communication...[with] a vehicle services module 92” and that “communications relative to the vehicle gateway 80 pass through the vehicle services module 92” to control access to the “vehicle buses 84 and vehicle devices 88.” (EX1020, [0035].) Spaur explains that the vehicle services module 92 “support[s] secure communications,” “arbitrat[es] vehicle bus access,” “monitor[s] and log[s] usage,” “enforce[es] rules,” and “manag[es] tools related to providing security, such as access keys or certificates approving access.” (EX1020, [0035]; EX1003, ¶465.)

A PHOSITA would have understood that because communications to the vehicle buses 84 and devices 88 pass through both the services module 92 and the gateway 80 – where access control, secure communication, rule enforcement, and

certificate management occur – these components collectively enforce the “*security measure[s]*” governing in-vehicle communications and operate together as the “*first security mechanism.*”<sup>9</sup> (EX1003, ¶¶466-475.)



EX1020, Figure 1

A PHOSITA would have further understood that the vehicle gateway 80 and the vehicle services module 92 (“*first security mechanism*”) creates a security boundary (“*perimeter network*”) to protect the internal vehicle network from

<sup>9</sup> A PHOSITA would have understood the communication services module 32 or the HMI services module 64 of Spaur individually or in combination would constitute a “*security mechanism*” implementing a “*security measure*” as required by this claim limitation. (EX1003, ¶¶471-476, 478.)

external, untrusted communications. Spaur teaches that external inputs – including wireless commands – are received through the vehicle gateway 80 and vehicle services module 92 before being introduced onto the internal vehicle buses 84 or delivered to the ECUs 86/vehicle devices 88. (EX1020, [0034]-[0035].) By having external communication paths terminate at this boundary, Spaur effectively teaches a logical perimeter protecting the internal ECUs 86 or vehicle devices 88 from unauthorized or malformed traffic (i.e., communication). (EX1003, ¶¶476-477.)

A PHOSITA would have understood that Spaur’s architecture can alternatively be viewed as forming the “*perimeter network*” around the external or peripheral communication sources themselves, because the vehicle gateway 80 and vehicle services module 92 act as a containment boundary that authenticates, evaluates, and filters the external inputs before they reach the internal network. (EX1020, [0034]-[0035].) These security functions—access control, rule enforcement, protocol validation, and traffic mediation—form a “*perimeter*” that isolates the external devices from the trusted in-vehicle network. (EX1003, ¶478.)

A PHOSITA would have further understood that the “*perimeter network*” can also be established around individual ECUs 86, because communication to any ECUs 86 first passes through the gateway 80 and services module 92, where secure-communication checks and authentication occur, thereby forming a boundary for each ECU 86 dependent on the messages entering through its associated bus.

(EX1020, [0034]-[0035]; EX1003, ¶¶479-480.)

**d. Limitation [1c]**

Spaur discloses that the telematics secure system 20 interfaces with “a common bus 96” linked to “a security controller 100,” which operates as a communication hub or switch. (EX1020, [0036].) Spaur discloses that the security controller “control[s] usage of resources,” performs “security authentication,” “facilitates secure channel establishment,” “provides bus and bandwidth arbitration,” and “monitor[s] traffic to ensure communications conform to required security profiles. (EX1020, [0010].) Spaur further states that the security controller 100 “monitors common bus 96 activity and vehicle bus 84 activity...to ensure that the security conditions established during confirmation or authentication continue to be met,” and may “dynamically discontinue the secure channel connection” if they fail. (EX1020, [0042]; EX1003, 481-483, 485-486.)

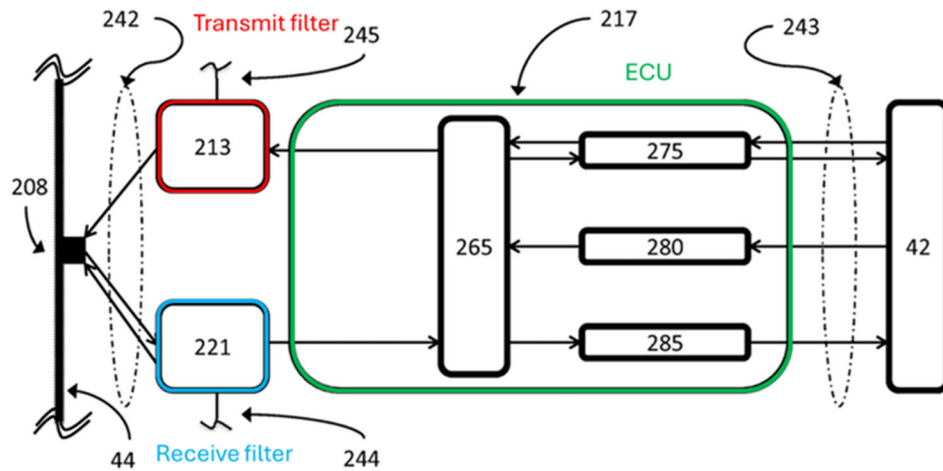
A PHOSITA would have understood that Spaur’s disclosure indicates that the security controller 100 executes software instructions to evaluate and enforce security conditions (“*detect an instance of a breach of the security measure*”). Additionally, Spaur states that “the security controller 100 can be implemented as a single chip,” indicating that it is a processor-based integrated circuit with a processor core, memory, and executable logic—i.e., a “*microprocessor-executable network controller.*” (EX1020, [0039]; EX1003, ¶484.)

Spaur further discloses that the security controller 100 implements security-enforcing firewall functions that protect vehicle resources from “invalid, unwanted, or malformed requests.” (EX1020, [0048].) Spaur states that external applications must be “certified” before accessing vehicle services, and the security controller 100 performs authentication and key exchange, limiting access for non-certified applications. (EX1020, [0048]; EX1003, ¶487.)

A PHOSITA would have understood that the security controller 100’s (“*network controller*”) identification and rejection of invalid, malformed, or non-certified requests reflects detection of communications that violate required security conditions—i.e., “*detect[ing] an instance of a breach of the security measure.*”

In addition to Spaur’s disclosure, and as explained in the Rationale to Combine section, the combination of Spaur’s security controller 100 and Peirce’s filter-policy logic provide a system that also “*detect[s] an instance of a breach of the security measure.*” (EX1003, ¶¶488, 546-563.)

Peirce discloses a filtering system with multiple transmit filters (210-213) and receive filters (218-221), each coupled to an ECU 86. (EX1021, 6:63-7:5.)



**Figure 5**

**EX1021, Figure 5**

These filters operate under a “filter policy” including executable instructions for “validating or verifying the authenticity of the message contents,” such as source ID, destination ID, and message ID. (EX1021, 7:38-51.) Peirce states that this policy “minimize[s] or eliminate[s] the transmission of corrupt messages”—including those generated by “a malicious third party (e.g., a hacker)” —to prevent improper or harmful vehicle behavior. (EX1021, 7:60-8:8.) A PHOSITA would have understood that the filters evaluate messages and identify those that violate the filter policy before allowing them on the bus, thereby “*detect[ing] an instance of a breach of the security measure.*” (EX1003, ¶¶489-493.)

**e. Limitation [1d]**

In addition to the ECUs 86 and the vehicle devices 88 (“*on board*

*computational components*”), Spaur teaches other components that receive, process, and analyze data, including “computers 74” (e.g., PDAs, laptops, or other intelligent processing units). (EX1020, [0031].) Spaur further discloses an assertion repository 78 with a policy decision engine 82 that “decide[s] which information of a plurality of stored information is to be released to a particular request.” (EX1020, [0033].) A PHOSITA would have understood that these components also constitute “*computational components*,” because they receive, process, and analyze data. (EX1003, ¶¶494-496.)

As explained above in limitation [1c], the combination of Spaur and Peirce teaches a mechanism for detecting when a particular resource, ECU, or communication channel no longer satisfies the required security conditions or violates a filter policy. (EX1003, ¶¶481-493, 497.) Spaur discloses that the security controller 100 continuously monitors “common bus 96 activity and vehicle bus 84 activity...to ensure that the security conditions...continue to be met,” where monitored resources include “vehicle buses, vehicle devices, interfaces, subsystems” (e.g., computers 74, assertion repository 78), storage memory, applications, and communication hardware/software. (EX1020, [0007], [0031]-[0032], [0042].) When these conditions fail, the security controller 100 “dynamically discontinue[s] the secure [communication] channel connection.” (EX1020, [0042].) A PHOSITA would have understood that by linking secure channel termination to a failure of a

required security condition, Spaur's disclosure indicates that the security controller 100 evaluates the state of individual resources and determines whether that specific bus, ECU, or communication path has deviated from authorized behavior, warranting isolation through termination of its secure channel ("*determine whether [an affected] computational component...can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure*"). (EX1003, ¶¶498-499.)

Spaur further states that the security controller 100 authenticates resources, mediates traffic, and provides bus and bandwidth arbitration. (EX1020, [0010].) These functions require the security controller 100 to decide whether a particular ECU or resource should be permitted to communicate and, conversely, when communication should be halted due to unauthorized or abnormal activity. Thus, Spaur teaches that the security controller 100 "*determine[s] whether a computational component affected by the instance of a breach...can be isolated*" from unaffected components. (EX1003, ¶¶500-501.)

**f. Limitation [1e]**

As discussed in limitations [1c] and [1d], Spaur discloses that the security controller 100 evaluates the state of individual resources—such as specific buses, ECUs, or communication paths—and determines when they deviate from authorized behavior, warranting isolation via termination of their secure channels. (EX1020,

[0007], [0010], [0031]-[0032], [0042].) Spaur further confirms the controller's isolation function by contrasting the Figure 1 and Figure 2 embodiments. In Figure 2, because the security controller 100-1 is no longer positioned as a switch or hub, "its ability to isolate segments of the common bus 96-1 does not exist," which reinforces that the Figure 1 architecture enables isolation of compromised segments. (EX1020, [0049], Figs. 1-2; EX1003, ¶¶481-502.)

Peirce further teaches isolation by terminating unauthorized communications. For example, Peirce discloses that the receive filter 221 "compare[s] the message ID of an incoming message with the known message IDs...to validate" matching messages and terminating those that do not match so they "never reach[] the VSM 42." (EX1021, 8:47-55.) Peirce provides a parallel mechanism for outgoing messages, stating that the transmit filter 213 validates source IDs and terminates non-matching messages before they reach the bus. (EX1021, 8:62-9:3.) A PHOSITA would have understood that terminating transmissions at the filter isolates the affected component from the rest of the network by preventing the corrupt or unauthorized message from propagating. (EX1003, ¶¶503-505.)

As stated in the Rationale to Combine section, the combined system of Spaur and Peirce provides coordinated monitoring and termination of unauthorized communication channels, thereby physically and logically isolating corrupted ECUs or other resources from unaffected on-board computational components. (EX1003,

¶¶506-507, 546-563.)

**g. Limitation 1[f]**

Petitioner interprets “*firewall and/or gateway*”<sup>10</sup> as “or” in accordance with Patent Owner’s position for that term in the related litigation. (EX1006, 6.) Again, Petitioner construes “*and/or*” for purposes of this petition as meaning “*or*.”

Limitation 1[f] recites the isolation must only be “one or more of” four specified isolation options: (1) denying vehicular wireless network access to the affected ECU; (2) directing its communications to a firewall/gateway for enforcement of a security measure; (3) blocking its communications; and (4) activating a second security mechanism. The combination of Spaur and Peirce teaches at least options (1) and (3), because by “*blocking communications to and from the computational component affected by the instance of the breach of a security measure*”, the systems is also “*denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure.*”

Spaur discloses that the security controller 100 monitors “[a]ll traffic between or among entities and/or resources” and monitors bus activity to ensure security conditions “continue to be met,” terminating the secure communication channel

---

<sup>10</sup> Petitioner makes the same interpretation with regards to Claim 9 and 17.

when they are not. (EX1020, [0010], [0042], *see also* [0034]-[0035].) Since communications flow through the security controller 100, a PHOSITA would have understood that terminating a component's secure channel prevents it from sending or receiving further messages—i.e., “*denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure*” or “*blocking communications to and from the computational component affected by the breach.*” Spaur further discloses that the vehicle gateway 80 and vehicle services module 92 control bus access, “enforce rules,” support “secure communications,” “arbitrate bus access,” and “manages access keys and certificates.” (EX1020, [0010], [0034]-[0035].) The security controller 100 – acting together with the vehicle gateway 80 and vehicle services module 92 - cuts off an affected component's ability to communicate across the vehicle buses when a required security condition is not met, thereby enforcing the same blocking function. (EX1020, [0042]; EX1003, ¶¶508-512.)

Peirce likewise discloses filter policies in both transmit and receive filters that block unauthorized or suspicious traffic based on message characteristics, preventing disallowed ECUs or nodes from placing messages onto—or receiving messages from—the network. (EX1021, 10:4-23.) A PHOSITA would have understood that these filter-based blocking mechanisms provide the selective communication blocking required by limitation [1f], and that when combined with

the security controller 100 disclosed in Spaur that provides secure-channel termination and certificate-based access control, the integrated system provides multiple mechanisms for blocking, denying, or preventing communications by components involved in a security breach. (EX1003, ¶¶513-515.)

### **3. Independent Claims 9 and 17**

As shown in the Comparison Chart of the Independent Claims (Appendix B), the limitations recited by claims 9 and 17 are nearly indistinguishable from the limitations recited by claim 1. To the extent a limitation is different, Petitioner addresses it below. For all similar limitations, claims 9 and 17 are unpatentable for the same reasons expressed with regard to claim 1.

#### **a. Limitation 9[pre] and 17[pre]**

Claim 9 recites the same limitations as claim 1 in method form, and Spaur teaches “system and method... for utilizing resources, including proprietary resources in a vehicle” (EX1020, [0006]; EX1003, ¶¶517-518).

*See* 1[pre]. (EX1003, ¶¶457-458, 519, 532.)

#### **b. Limitations 9[a] and 17[a]**

Limitation 9[a] is a method claim which begins by reciting “in a vehicle comprising.” This portion of limitation 9[a] is the same, and therefore satisfied for the same reasons discussed by limitation 1[pre].

*See* 1[a]. (EX1003, ¶¶459-464, 520-521, 533.)

**c. Limitations [9b] and 17[b]**

Limitation [17b] additionally recites “*a non-transient, tangible computer readable medium comprising.*” Spaur teaches that a storage memory 76 “can contain proprietary data and/or program code” and may include “hard disks and/or removable memory, such as CD-ROMs.” (EX1020, [0031].) Because hard disks and CD-ROMs are well understood to be non-transitory storage media (EX1050, 94–95; EX1051, 152), a PHOSITA would have understood Spaur to teach “*a non-transient, tangible computer-readable medium*” that stores the program code implementing the security-enforcing functions of the vehicle gateway 80 and vehicle services module 92 (“*first security mechanism*”). (EX1003, ¶¶534-537.)

*See* 1[b]. (EX1003, ¶¶465-480, 522, 538.)

**d. Limitations 9[c] and 17[c]**

Limitation 17[c] additionally recites “*on board a selected vehicle that, when executed.*” Spaur’s processor-based security controller 100 and Peirce’s filter-policy logic are expressly implemented within the vehicle’s on-board network architecture, and their executable instructions detect and respond to security-condition failures when executed on the selected vehicle.

*See* 1[c]. (EX1003, ¶¶481-493, 523-524, 539-540.)

**e. Limitation 9[d] and 17[d]**

*See* 1[d]. (EX1003, ¶¶494-501, 525-526, 541.)

**f. Limitations 9[e] and 17[e]**

Limitation 9[e] recites a “microprocessor executable network controller.” Spaur discloses that the security controller 100 executes software instructions to evaluate and enforce security conditions and “can be implemented as a single chip,” indicating that it is a processor-based integrated circuit with a processor core, memory, and executable logic—i.e., a “*microprocessor-executable network controller.*” (EX1020, [0039].)

*See* 1[e]. (EX1003, ¶¶502-507, 527-528, 542-543.)

**g. Limitations 9[f] and 17[f]**

*See* 1[f]. (EX1003, ¶¶508-515, 529-530, 544-545.)

**IX. Conclusion**

For the foregoing reasons, the Board should grant institution.

Respectfully submitted,

Dated: December 8, 2025

/ Andrew B. Turner /  
Andrew B. Turner (Reg. No. 63,121)  
John P. Rondini (Reg. No. 64,949)  
John S. LeRoy (Reg. No. 48,158)  
Christopher C. Smith (Reg. No. 59,669)  
Francesca Cusumano (Reg. No. 81,149)  
**Brooks Kushman P.C.**  
150 W. Second St., Suite 400N  
Royal Oak, MI 48067-3846  
(248) 358-4400

*Attorneys for Ford*

**Certificate of Service**

The undersigned hereby certifies that the foregoing **PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. § 311 *ET SEQ.* AND 37 C.F.R. § 42.100 *ET SEQ.* (U.S. PATENT NO. 9,173,100)**, including all exhibits and supporting evidence, was served by overnight courier in its entirety on **December 9, 2025**, upon the following correspondence address as shown for the '100 Patent:

<p><b>192827 - Avantech Law, LLP</b> 80 S 8th St, Suite 900 Minneapolis, MN 55402 UNITED STATES</p>
---

Respectfully submitted,

Dated: December 8, 2025

/ Andrew B. Turner /  
Andrew B. Turner (Reg. No. 63,121)  
John P. Rondini (Reg. No. 64,949)  
John S. LeRoy (Reg. No. 48,158)  
Christopher C. Smith (Reg. No. 59,669)  
Francesca Cusumano (Reg. No. 81,149)  
**Brooks Kushman P.C.**  
150 W. Second St., Suite 400N  
Royal Oak, MI 48067-3846  
(248) 358-4400

*Attorneys for Ford*

**Certificate of Compliance Pursuant to 37 C.F.R. § 42.24**

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper contains 13,800 words, excluding the parts of the paper exempted by §42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of § 42.6(a)(iii)&(iv).

Respectfully submitted,

Dated: December 8, 2025

/ Andrew B. Turner /  
Andrew B. Turner (Reg. No. 63,121)  
John P. Rondini (Reg. No. 64,949)  
John S. LeRoy (Reg. No. 48,158)  
Christopher C. Smith (Reg. No. 59,669)  
Francesca Cusumano (Reg. No. 81,149)  
**Brooks Kushman P.C.**  
150 W. Second St., Suite 400N  
Royal Oak, MI 48067-3846  
(248) 358-4400

*Attorneys for Ford*

### Appendix A - Listing of All Challenged Claims

<b>1[pre]</b>	A vehicle, comprising:
<b>[1a]</b>	a plurality of on board computational components;
<b>[1b]</b>	a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and
<b>[1c]</b>	a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,
<b>[1d]</b>	(ii) determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and
<b>[1e]</b>	(iii) when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of (a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a

	<p>security measure from the computational component affected by the instance of a breach of a security measure and (b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,</p>
<b>[1f]</b>	<p>wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure.</p>
<b>2[pre]</b>	<p>The vehicle of claim 1, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle</p>

	attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,
<b>[2a]</b>	wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and
<b>[2b]</b>	wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.
<b>3[pre]</b>	The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational

	component,
<b>[3a]</b>	wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and
<b>[3b]</b>	wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.
<b>4[pre]</b>	The vehicle of claim 2, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and
<b>[4a]</b>	wherein the at least one board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a

	remote control module, a computational module selector, an expansion module, an application, and a plug-in module.
<b>5[pre]</b>	The vehicle of claim 1, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and
<b>[5a]</b>	wherein the microprocessor executable network controller analyzes the security breach instance by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.
<b>6[pre]</b>	The vehicle of claim 1, wherein the computational component affected by the security breach instance is an external computational device and
<b>[6a]</b>	wherein the at least one on board computational component not affected by the security breach instance is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational

	component.
<b>[7]</b>	The vehicle of claim 1, wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.
<b>8<pre>[pre]</pre></b>	The vehicle of claim 1, wherein the at least one computational component is inside of a perimeter network of the vehicle, wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,
<b>[8a]</b>	wherein the computational component affected by the security breach instance is a node on the vehicular wireless network and physically

	and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and
<b>[8b]</b>	wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions in the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.
<b>9 [pre]</b>	A method, comprising:
<b>[9a]</b>	in a vehicle comprising a plurality of on board computational components,
<b>[9b]</b>	a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and
<b>[9c]</b>	a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach

	instance;
<b>[9d]</b>	in response, the microprocessor executable network controller determining whether a computational component affected by the possible security breach instance can be isolated from at least one on board computational component not affected by or potentially affected by the possible security breach instance; and
<b>[9e]</b>	when the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance, the microprocessor executable network controller at least one of (a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance from the computational component affected by the possible security breach instance and (b) isolating the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance,

<b>[9f]</b>	wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the possible security breach instance, (2) directing communications to and from the computational component affected by the possible security breach instance to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the possible security breach instance, and (4) activating a second security mechanism in response to the possible security breach instance.
<b>10[pre]</b>	The method of claim 9, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,
<b>[10a]</b>	wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance,

	and a network probe, and
<b>[10b]</b>	wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.
<b>11[pre]</b>	The method of claim 10, wherein the computational component affected by the security breach instance is an on board computational component,
<b>[11a]</b>	wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and
<b>[11b]</b>	wherein the computational component affected by the security breach instance and the at least one on board computational component are

	both within a perimeter network of the vehicle.
<b>12[pre]</b>	The method of claim 10, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and
<b>[12a]</b>	wherein the at least one board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.
<b>13[pre]</b>	The method of claim 9, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and

<b>[13a]</b>	wherein the microprocessor executable network controller detects a possible security breach instance by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.
<b>14[pre]</b>	The method of claim 9, wherein the computational component affected by the security breach instance is an external computational device and
<b>[14a]</b>	wherein the at least one on board computational component not affected by the security breach instance isolation is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.
<b>[15]</b>	The method of claim 9, wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not

	<p>normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.</p>
<b>16[pre]</b>	<p>The method of claim 9, wherein the at least one computational component is inside of a perimeter network of the vehicle, wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,</p>
<b>[16a]</b>	<p>wherein the computational component affected by the security breach instance is a node on the vehicular wireless network and physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and</p>
<b>[16b]</b>	<p>wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions in the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the</p>

	SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.
<b>17[pre]</b>	In a vehicle comprising
<b>[17a]</b>	a plurality of on board computational components,
<b>[17b]</b>	a non-transient, tangible computer readable medium comprising a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components and
<b>[17c]</b>	a microprocessor executable network controller on board a selected vehicle that, when executed, detects an instance of a breach of the security measure,
<b>[17d]</b>	determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security

	measure, and,
<b>[17e]</b>	when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and at least one of isolates the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure from the computational component affected by the instance of a breach of the security measure isolates the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure,
<b>[17f]</b>	wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of the security measure, (2) directing communications to and from the computational component affected by the instance of a breach of the security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications

	<p>to and from the computational component affected by the instance of a breach of the security measure, and (4) activating a second security mechanism in response to the instance of a breach of the security measure.</p>
<b>18[pre]</b>	<p>The computer readable medium of claim 17, wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource and</p>
<b>[18a]</b>	<p>wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and</p>
<b>[18b]</b>	<p>wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID</p>

	(Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.
<b>19[pre]</b>	The computer readable medium of claim 18, wherein the computational component affected by the security breach instance is an on board computational component,
<b>[19a]</b>	wherein the at least one on board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and
<b>[19b]</b>	wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.
<b>20[pre]</b>	The computer readable medium of claim 18, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least

	one on board computational component and
<b>[20a]</b>	wherein the at least one on board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.
<b>21[pre]</b>	The computer readable medium of claim 17, wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and
<b>[21a]</b>	wherein the microprocessor executable network controller detects a possible security breach instance by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a

	further security breach instance.
<b>22[pre]</b>	The computer readable medium of claim 17, wherein the computational component affected by the security breach instance is an external computational device and
<b>[22a]</b>	wherein the at least one on board computational component not affected by the security breach instance is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.
<b>[23]</b>	The computer readable medium of claim 17, wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component

	affected by the security breach instance are blocked in whole or part.
<b>24[pre]</b>	The computer readable medium of claim 17, wherein the at least one computational component is inside of a perimeter network of the vehicle, wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,
<b>[24a]</b>	wherein the computational component affected by the security breach instance is a node on the vehicular wireless network and physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and
<b>[24b]</b>	wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.



**Appendix B - Comparison of Independent Claims**

	<b>Claim 1</b>		<b>Claim 9</b>		<b>Claim 17</b>
	1[pre] A vehicle, comprising:		9[pre] A method, comprising:		17[pre] In a vehicle comprising
[1a]	a plurality of on board computational components;	[9a]	in a vehicle comprising  a plurality of on board computational components,	[17a]	a plurality of on board computational components,
[1b]	a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and	[9b]	a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components, and	[17b]	a non-transient, tangible computer readable medium comprising  a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components and
[1c]	a microprocessor executable network controller	[9c]	a microprocessor executable network controller,	[17c]	a microprocessor executable network controller

	operable to  (i) detect an instance of a breach of the security measure,		the microprocessor executable network controller  identifying a possible security breach instance;		on board a selected vehicle that, when executed,  detects an instance of a breach of the security measure,
[1d]	(ii) determine whether a computational component affected by the instance of a breach of the security measure  can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and	[9d]	in response, the microprocessor executable network controller  determining whether a computational component affected by the possible security breach instance  can be isolated from at least one on board computational component not affected by or potentially affected by the possible security breach instance; and	[17d]	determines whether a computational component affected by the instance of a breach of the security measure  can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and,

<p>[1e]</p>	<p>(iii) when the computational component affected by the instance of a breach of the security measure</p> <p>can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure,</p> <p>at least one of</p> <p>(a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure</p>	<p>[9e]</p> <p>when the computational component affected by the possible security breach instance</p> <p>can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance,</p> <p>the microprocessor executable network controller</p> <p>at least one of</p> <p>(a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance</p>	<p>[17e]</p> <p>when the computational component affected by the instance of a breach of the security measure</p> <p>can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and</p> <p>at least one of</p> <p>isolates the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure</p>
-------------	---	--	---

	<p>from the computational component affected by the instance of a breach of a security measure and</p> <p>(b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,</p>		<p>from the computational component affected by the possible security breach instance and</p> <p>(b) isolating the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance,</p>		<p>from the computational component affected by the instance of a breach of the security measure</p> <p>isolates the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure,</p>
[1f]	<p>wherein the isolation is one or more of:</p> <p>(1) denying vehicular wireless network access to the computational component affected by the instance of a</p>	[9f]	<p>wherein the isolation is one or more of:</p> <p>(1) denying vehicular wireless network access to the computational component affected by the possible security breach instance,</p>	[17f]	<p>wherein the isolation is one or more of:</p> <p>(1) denying vehicular wireless network access to the computational component affected by the instance of a breach</p>

<p>breach of a security measure,</p> <p>(2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure,</p> <p>(3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and</p> <p>(4) activating a second security mechanism in response to the instance of a breach of a security measure.</p>	<p>(2) directing communications to and from the computational component affected by the possible security breach instance to a firewall and/or gateway to enforce a security measure,</p> <p>(3) blocking communications to and from the computational component affected by the possible security breach instance, and</p> <p>(4) activating a second security mechanism in response to the possible security breach instance.</p>	<p>of the security measure,</p> <p>(2) directing communications to and from the computational component affected by the instance of a breach of the security measure to a firewall and/or gateway to enforce a security measure,</p> <p>(3) blocking communications to and from the computational component affected by the instance of a breach of the security measure, and</p> <p>(4) activating a second security mechanism in response to the instance of a breach of the security measure.</p>
---	---	--

**Appendix C - Comparison of Dependent Claims**

<p><b>Depends from Ind.</b></p> <p><b>Claim 1</b></p>	<p><b>Depends from Ind.</b></p> <p><b>Claim 9</b></p>	<p><b>Depends from Ind.</b></p> <p><b>Claim 17</b></p>
<p>2[pre] The vehicle of claim 1, wherein the security breach instance is one or more of</p> <p>an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,</p>	<p>10[pre] The method of claim 9, wherein the security breach instance is one or more of</p> <p>an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,</p>	<p>18[pre] The computer readable medium of claim 17, wherein the security breach instance is one or more of</p> <p>an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource and</p>
<p>[2a] wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach</p>	<p>[10a] wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach</p>	<p>[18a] wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach</p>

instance, and a network probe, and	instance, and a network probe, and	instance, and a network probe, and
<p>[2b] wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.</p>	<p>[10b] wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.</p>	<p>[18b] wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.</p>
<p>3[pre] The vehicle of claim 2,</p> <p>wherein the computational component affected by</p>	<p>11[pre] The method of claim 10,</p> <p>wherein the computational component affected by</p>	<p>19[pre] The computer readable medium of claim 18,</p> <p>wherein the computational component affected by</p>

the security breach instance is an on board computational component,	the security breach instance is an on board computational component,	the security breach instance is an on board computational component,
[3a] wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and	[11a] wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and	[19a] wherein the at least one on board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and
[3b] wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.	[11b] wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.	[19b] wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.
4[pre] The vehicle of claim 2,  wherein the computational component affected by the security breach instance is outside of a perimeter network of the	12[pre] The method of claim 10,  wherein the computational component affected by the security breach instance is outside of a perimeter network of the	20[pre] The computer readable medium of claim 18,  wherein the computational component affected by the security breach instance is outside of a perimeter network of the

<p>vehicle containing the at least one on board computational component and</p>	<p>vehicle containing the at least one on board computational component and</p>	<p>vehicle containing the at least one on board computational component and</p>
<p>[4a] wherein the at least one board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.</p>	<p>[12a] wherein the at least one board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.</p>	<p>[20a] wherein the at least one on board computational component is one or more of an on board sensor, a media controller, a gateway, a firewall, a processing module, a network controller, an input/output system, a display controller, an audio controller, an arbitration module, a health check module, a critical system controller, a non-critical system controller, an on board sensor monitor, a displayed object movement module, a diagnostic module, a media filter, a network selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.</p>
<p>5[pre] The vehicle of claim 1,</p>	<p>13[pre] The method of claim 9,</p>	<p>21[pre] The computer readable medium of claim 17,</p>

<p>wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and</p>	<p>wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and</p>	<p>wherein the computational component affected by the security breach instance is outside of a perimeter network of the vehicle containing the at least one on board computational component and</p>
<p>[5a] wherein the microprocessor executable network controller analyzes the security breach instance</p> <p>by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.</p>	<p>[13a] wherein the microprocessor executable network controller detects a possible security breach instance</p> <p>by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.</p>	<p>[21a] wherein the microprocessor executable network controller detects a possible security breach instance</p> <p>by one or more of reviewing historical behavior and comparing the behavior to templates characteristic of differing types of attacks and/or applying rules to the historical behavior and updating firewall settings to protect against a further security breach instance.</p>
<p>6[pre] The vehicle of claim 1,</p> <p>wherein the computational component affected by</p>	<p>14[pre] The method of claim 9,</p> <p>wherein the computational component affected by</p>	<p>22[pre] The computer readable medium of claim 17,</p> <p>wherein the computational component affected by</p>

<p>the security breach instance is an external computational device and</p>	<p>the security breach instance is an external computational device and</p>	<p>the security breach instance is an external computational device and</p>
<p>[6a] wherein the at least one on board computational component not affected by the security breach instance is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.</p>	<p>[14a] wherein the at least one on board computational component not affected by the security breach instance isolation is isolated from the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.</p>	<p>[22a] wherein the at least one on board computational component not affected by the security breach instance is isolated form the external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.</p>
<p>7[pre] The vehicle of claim 1, wherein at least one of the following is true about the isolation:  communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not</p>	<p>15[pre] The method of claim 9, wherein at least one of the following is true about the isolation:  communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not</p>	<p>23[pre] The computer readable medium of claim 17, wherein at least one of the following is true about the isolation:  communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not</p>

<p>normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.</p>	<p>normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.</p>	<p>normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.</p>
<p>8[pre] The vehicle of claim 1,</p> <p>wherein the at least one computational component is inside of a perimeter network of the vehicle,</p> <p>wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,</p>	<p>16[pre] The method of claim 9,</p> <p>wherein the at least one computational component is inside of a perimeter network of the vehicle,</p> <p>wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,</p>	<p>24[pre] The computer readable medium of claim 17,</p> <p>wherein the at least one computational component is inside of a perimeter network of the vehicle,</p> <p>wherein the at least one on board computational component in a vehicular wireless network not affected by the security breach instance is a critical component,</p>
<p>[8a] wherein the computational component affected by</p>	<p>[16a] wherein the computational component affected by</p>	<p>[24a] wherein the computational component affected by</p>

<p>the security breach instance is a node on the vehicular wireless network and physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and</p>	<p>the security breach instance is a node on the vehicular wireless network and physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and</p>	<p>the security breach instance is a node on the vehicular wireless network and physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network, and</p>
<p>[8b] wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions in the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.</p>	<p>[16b] wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions in the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.</p>	<p>[24b] wherein isolation is effected by enabling a critical communication security mechanism that is one or more of encryption of access restrictions the at least one on board computational component in a vehicular wireless network, disabling ESSID broadcasting, hiding the SSID, performing MAC ID filtering, performing static IP addressing, implementing IEEE 802.11, 802.11i, and/or 802.1x security, using wired equivalent privacy encryption, using one or more of TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.</p>