

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORD MOTOR COMPANY,
Petitioner,

v.

AUTOCONNECT HOLDINGS LLC,
Patent Owner.

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

Case No.: IPR2026-00173

DECLARATION OF SCOTT ANDREWS

TABLE OF CONTENTS

List of Exhibits.....	3
I. Qualifications and Professional Experience.....	7
II. Relevant Legal Standards	17
A. General	17
B. Priority Dates for Claimed Subject Matter.....	18
C. Claim Construction Standard	19
D. Anticipation	20
E. Obviousness.....	21
III. Qualifications of One of Ordinary Skill in the Art.....	24
IV. U.S. Patent No. 9,173,100 to Ricci.....	26
A. Overview of the AutoConnect Patent Family	26
B. The '100 Patent File History	38
V. Claim Construction.....	46
VI. State of the Art.....	46
A. Vehicle Network Systems	47
B. Vehicle Network Security	52
VII. Overview of the Key Prior Art References Relied Upon.....	58
A. Vehicular Networks – Security, Vulnerabilities and Countermeasures, Master of Science Thesis in the program Networks and Distributed Systems (“Amirtahmasebi” Ex. 1019).....	58
B. US 2004/0185842 A1 (“Spaur” Ex. 1020).....	63
C. US 8,788,731 B2 (“Peirce” Ex. 1021)	66
D. Bosch Automotive Handbook 6th Edition (“Bosch” Ex. 1050)	69
VIII. Grounds for Challenge.....	70
A. Ground 1 – The Combination of Amirtahmasebi and Bosch teaches all of the limitations of claims 1-24.....	70
B. Ground 2 – The Combination of Spaur and Peirce Teaches all of the Limitations of Claims 1, 9, and 17.....	221
IX. Objective Indicia Does Not Support Patentability	289
X. Conclusion	289

List of Exhibits

Exhibit No.	Description
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	Complaint, <i>AutoConnect Holdings LLC v. Ford Motor Company</i> , Case No. 1:24-cv-01327-JCG (D. Del)
1008	U.S. Patent No. 9,173,100 with Additions to Specification Highlighted
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”)
1050	Bosch Handbook, (Automotive Handbook October 2004 6 th Edition) (“Bosch”)
1051	IEEE Dictionary, (IEEE 100 The Authoritative Dictionary of IEEE Standards Terms 2000 7 th Edition) (“IEEE Dictionary”)
1052	“Specification of The Bluetooth System” (June 30, 2010). Version 4.0 (Volumes 0-6) Available at https://www.bluetooth.com/specifications/specs/core-specification-4-0/ (Accessed June 27, 2025) (“Bluetooth Specification”)
1060	TCP/IP Tutorial and Technical Overview 6 th Ed. (International Business Machines Corporation – October 1998) (“IBM TCP/IP Tutorial”)
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 1st ACM international 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")
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 (“Digital Certificate Pool”)
1169	U.S. Patent No. 7,742,603 B2 to Tengler (“Security for Anonymous Vehicular Broadcast Messages”)

I, Scott Andrews, hereby declare as follows:

1. I am making this declaration at the request of Ford Motor Company in the matter of *inter partes* review of U.S. Patent No. 9,173,100 (“the ’100 Patent”) to Christopher Ricci. (Ex. 1001.)

2. Although I am being compensated at my usual and customary rate, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

3. This declaration is based on the information currently available to me. If additional information becomes available, I may continue my investigation and study, which may include a review of documents and information that may be produced, as well as testimony from depositions that have not yet been taken.

4. In preparation of this declaration, I have studied the exhibits as listed in the Exhibit List shown above in my report.

5. In forming the opinions expressed below, I have considered:

- a. The documents listed above as well as additional patents and documents referenced herein;
- b. The relevant legal standards, including the standard for obviousness provided in *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007), and any additional documents cited in the body of this declaration; and

- c. My knowledge and experience based upon my work and study in this area as described below.

I. Qualifications and Professional Experience

6. I have provided my full background in the curriculum vitae that is attached as Ex. 1004.

7. I have over 30 years of professional experience in the automotive and transportation industries, including intelligent transportation systems, vehicle electrical and electronics systems, vehicle information systems, and navigation systems.

8. I received an undergraduate Bachelor of Science degree in Electrical Engineering from the University of California, Irvine, in 1977. I received a Master's of Science degree in Electrical Engineering from Stanford University in 1982.

9. From 1977 to 1983, I held engineering positions at Ford Aerospace and Teledyne Microwave, working on, among other things, transmitter-receiver systems for guided missile systems and other related military electronics.

10. From 1983 to 1993, I worked at TRW, Inc. ("TRW") in the Space & Electronics Group, where I served as a project manager, a department manager, and as an assistant program manager on a variety of spacecraft communications systems projects. My last position at TRW Space & Electronics was as the manager of the MMIC Products Organization, which was directed toward monolithic microwave

integrated circuits. In that role, I developed TRW's commercial GaAs MMIC business. My responsibilities included development of a business strategy and business plan, and overall management of customer and research and development programs for my department. During my time in the MMIC Products Organization I also developed the first single chip 94 GHz radar, intended for use in automotive adaptive cruise control systems. While I was at TRW Space & Electronics, I received several awards for outstanding performance on Independent Research and Development projects.

11. In 1993, while still at TRW, I moved to the Automotive Electronics and Group and became the Director of Systems Engineering and Advanced Products. In this role, I was responsible for the overall management of TRW's advanced development programs in the automotive electronics space. These programs included, among other things, wireless remote keyless entry systems, vehicle tracking and location systems (e.g., roadside assistance and emergency response systems), emergency vehicle warning systems (e.g., transmitter-receiver systems that would provide a warning inside the user's vehicle when an active emergency vehicle was in the vicinity), automotive collision avoidance radar, and other types of vehicle information systems. I served in this role until 1996.

12. From 1996 to 2000, I worked at Toyota Motor Corporation as a Project General Manager in the R&D Management Division. My responsibilities included

conceptualizing and developing multimedia systems, along with new technology products and services for Toyota's future passenger vehicles. During my time at Toyota, I worked on developing adaptive cruise control systems that used radar and lidar sensors. For instance, I evaluated various sensors and subsystems in Europe and Japan specifically to support Toyota's development of adaptive cruise control and forward collision avoidance systems. In this role, I also worked closely with the Collision Avoidance Metrics Partnership (CAMP), a joint venture between Ford Motor Company and General Motors.

13. While at Toyota, I was responsible for a variety of research collaborations, including, for example, a collaboration with Dr. Paul Green at the University of Michigan Transportation Research Institute (UMTRI) wherein we studied the distraction created by different map displays for navigation systems, and identified various rules for the display of map information based on the speed of the vehicle. This included readability studies for how street names were displayed, and what level of map detail should be displayed as a function of vehicle speed.

14. In 1999, I founded Cogenia, Inc. to develop an enterprise-class data management software system. While at Cogenia, I developed and oversaw the company's business concept and strategic plan and led the executive team in the development of an enterprise data system for managing data between multiple user endpoints or devices. This included home and work computing environments, as

well as multiple mobile devices. In each case, key data useful to the user was prepositioned so that it could be easily accessed when and where the user needed it the most. Cogenia, Inc. ceased operations in December 2000.

15. I founded Cogenia Partners, LLC as an independent consultant in the intelligent vehicles and mobile systems industry in January 2001. My primary clients have been automotive manufacturers, various navigation and mobile device makers, and the U.S. Department of Transportation.

16. Between January 2001 and June 2003, I was engaged as a consultant to Toyota serving as a key member of the AMI-C technical team. At the conclusion of the AMI-C Release II specifications, I transitioned the AMI-C specifications to the International Organization for Standardization (or ISO) and the Open Services Gateway initiative (or OSGi) as part of the Connected Vehicle Trade Association, for which I currently serve as the Vice President of Technology.

17. My consulting experience includes serving between 2005 and 2010 as the Chief System Architect for the Vehicle Infrastructure Integration (“VII”) program. This was a cooperative research project sponsored by the Federal Highway Administration (“FHWA”) and a group of automakers who had formed the VII Consortium (or VIIC). In this role, I was responsible for developing the system architecture, defining requirements, and leading the development and testing of a system for communicating between the roadway and the car (V2I), and between cars

(V2V). This is the system described in greater detail by Amirtahmasebi. (Ex. 1019).

This work was also documented in a series of reports I authored for the US DOT.

(See Exs.1162¹-1167^{2,3,4,5,6}.) This program was the first major demonstration of vehicle area networks (VANETs) and included the development and initial

¹ FHWA-JPO-17-483, Ex. 1162 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on May 22, 2016.

² FHWA-JPO-12-061, Ex. 1163 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on June 21, 2012.

³ FHWA-JPO-18-686, Ex. 1164 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on June 22, 2018.

⁴ FHWA-JPO-09-003, Ex. 1165 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on May 19, 2009.

⁵ FHWA-JPO-09-043, Ex. 1166 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on May 19, 2009.

application of a radio network based on IEEE 802.11 together with messaging protocols (IEEE 1609.3) and security protocols (1609.2). (*See* Exs. 1162-1167.)

18. As is described in detail in the technical report FHWA-JPO-09-017 (Final Report: Vehicle Infrastructure Integration Proof of Concept Technical Description - Vehicle), the in-vehicle portion of the system that carried out all of the security processing, display, communications and applications functions was implemented using a EuroTech Dura Cor as shown below. (FHWA-JPO-09-017, Ex. 1167, p. 21.) This system also implemented a Vehicle Interface Service (VIS) that essentially created a firewall/gateway between the vehicle networks and the external components of the system to provide secure access to and from the vehicle networks. (FHWA-JPO-09-017, Ex. 1167, p. 47.)

⁶ FHWA-JPO-09-017, Ex. 1167 is a true and accurate copy of a report that I understand was published by the U.S. Department of Transportation on May 19, 2009.

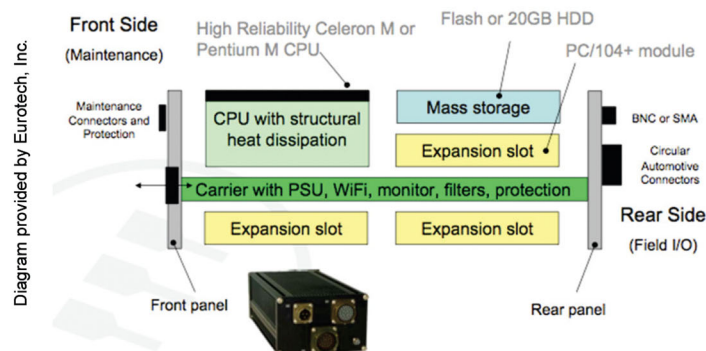


Figure 4-7 DuraCOR Unit Physical Architecture

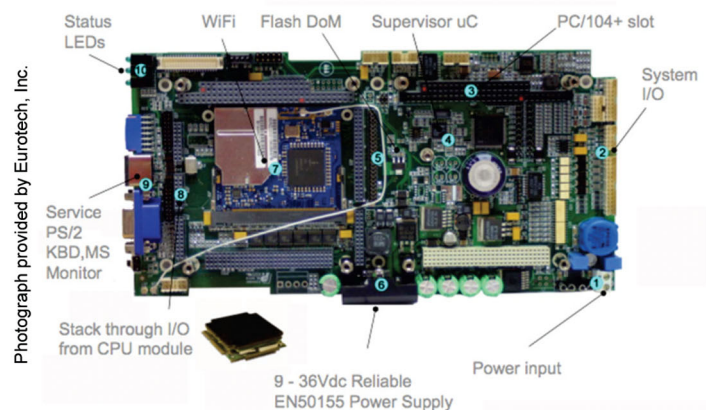


Figure 4-8 DuraCOR Unit Motherboard

Photograph of EuroTech DuraCOR Processing Unit Used to Implement In-Vehicle Functions (FHWA-JPO-09-017, Ex. 1167, p. 21)

19. As part of this work, I was also awarded two patents related to digital certificate management U.S. Patent No. 7,734,050, titled “Digital Certificate Pool,” (Ex. 1168) and U.S. Patent No. 7,742,603, titled “Security for Anonymous Vehicular Broadcast Messages” (Ex. 1169.)

20. My consulting experience also includes serving as technical consultant to the American Association of State Highway Transportation Officials (or AASHTO) for connected vehicle deployment analysis and strategy; technical consultant to Booz Allen for connected vehicle security credential communications

systems analysis, for the FHWA; and technical consultant to ARINC for the development of an advanced connected vehicle test facility for the FHWA Turner Fairbank Highway Research Center. I recently completed a project as co-principal investigator for Integrated Advanced Transportation System (a research program funded by FHWA).

21. I consult with the U.S. Department of Transportation, major carmakers, and suppliers on vehicle information systems, safety systems, communication systems, and vehicle network security systems. In the various positions mentioned above, I was responsible for the research and development of projects relating to numerous vehicle communications systems, vehicle information systems, user interface systems, sensory systems, control systems, and safety systems, and I also had the opportunity to collaborate with numerous researchers and suppliers to the auto industry. I am a member of the Institute of Electrical and Electronics Engineers (or IEEE), the IEEE Standards Association, the Society of Automotive Engineers (or SAE), the Institute of Navigation (or ION), and the International Council on Systems Engineering (or INCOSE).

22. I have authored numerous technical papers. My publications include papers on topics related to telematics, software and network architecture, and vehicle infrastructure, including integration of vehicle systems. I have attached to my curriculum vitae a list of all publications I have authored in the last 10 years.

23. Additionally, I am the named inventor of thirty U.S., Japanese and European patents, including patents related to controlling a mobile device based on contextual information from sensors. I have attached a complete list of my issued patents to my curriculum vitae.

24. I am familiar with the subject matter of this case, and consider myself an expert in, among other things, intelligent transportation systems, vehicle information and communications systems, and navigation systems.

25. I am familiar with the subject matter of this case, and consider myself an expert in, among other things, intelligent transportation systems, vehicle information and communications systems, and navigation systems.

26. I have previously prepared expert reports and testified in a number of cases concerning related systems.

27. I have previously prepared expert reports and testified in a number of cases concerning systems for vehicle networks, vehicle safety systems, vehicle network security, wireless communication, communication protocols, and hardware and software of electronic devices.

28. I am familiar with the subject matter of this case, and consider myself an expert in, among other things, intelligent transportation systems, vehicle information and communications systems, and navigation systems.

29. Intentionally left blank.

II. Relevant Legal Standards

A. General

30. I have been asked to provide opinions on the claims of the '100 Patent in light of the prior art.

31. It is my understanding that a claimed invention is unpatentable under 35 USC § 102 if a prior art reference teaches every element of the claim. Further, it is my understanding that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the alleged invention was made to a person having ordinary skill in the art to which the subject matter pertains. I also understand that an obviousness analysis takes into account factual inquiries including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

32. It is my understanding that the Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of the claimed subject matter. Some of these rationales include the following: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to obtain predictable results; a predictable use of prior art elements according to their established functions; applying a known technique to a known device to yield predictable

results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

B. Priority Dates for Claimed Subject Matter

33. I understand that in order to be considered “prior art,” patents or printed publications must predate the pertinent priority dates for the subject matter claimed in the ’100 Patent.

34. I have been informed that a patent is only entitled to a priority date based on an earlier filed application if the earlier filed application meets the requirements of pre-AIA 35 U.S.C. §112. Specifically, I have been informed that pre-AIA 35 U.S.C. § 112 ¶1 requires that the specification of a patent or patent application must “contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the [invention]” I understand that the requirements of this provision are commonly called the written description requirement and the enablement requirement.

35. I have been informed that compliance with both the written description requirement and enablement requirement must be determined as of the effective filing date of the application for which priority is sought.

36. I have been informed that to satisfy the written description requirement a patent's specification should reasonably convey to a person of skill in the art that the inventor had possession of the claimed invention as of the effective filing date of the application.

C. Claim Construction Standard

37. In order to properly evaluate these claims, I understand that the terms of the claims must first be construed.

38. I understand that in this proceeding, the claims are construed consistent with the specification and using the same construction as that used in litigation. I have been informed that the claims, after being construed in this manner, are then to be compared to the information in the prior art, which for this proceeding is limited to patents and printed publications. I also understand that, at the same time, absent some reason to the contrary, claim terms are typically given their ordinary and accustomed meaning as would be understood by one of ordinary skill in the art.

39. I understand that an apparatus claim limitation that includes functional language without reciting the structure limitations for performing the claimed function may be construed as a "means for" or "means plus" claim, even if the claim

limitation does not expressly use the term “means.” Such a claim limitation is interpreted to cover the structure disclosed in the specification for performing the claimed function and equivalents thereof.

D. Anticipation

40. I understand that the following standards govern the determination of whether a patent claim is “anticipated” by the prior art.

41. I understand that, for a patent to be “anticipated” by the prior art, each and every limitation of the claim must be found, expressly, implicitly or inherently, in a single prior art reference. I further understand that the requirement of strict identity between the claim and the reference is not met if a single element or limitation required by the claim is missing from the applied reference.

42. I understand that claim limitations that are not expressly described in a prior art reference may still be there if they are implicit or inherent to the thing or process being described in the prior art. I have been informed that to establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference and that it would be so recognized by persons of ordinary skill in the art. I have been informed that inherency cannot be established just because a certain thing may result from a given set of circumstances.

43. I understand that it is acceptable to consider evidence other than the information in a particular prior art document to determine if a feature is necessarily present in or inherently described by that reference.

E. Obviousness

44. I understand that for a single reference or a combination of references to render obvious a claimed invention, a person of ordinary skill in the art must have been able to arrive at the claimed invention by altering or combining the applied references.

45. I have been informed that a patent claim can be found unpatentable as obvious where the differences between the subject matter taught to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the relevant field. Specifically, I understand that the obviousness question involves a consideration of:

- a) the scope and content of the prior art;
- b) the differences between the prior art and the claims at issue;
- c) the knowledge of a person of ordinary skill in the pertinent art; and
- d) whatever objective factors indicating obviousness or non-obviousness may be present in any particular case – referred to as “secondary considerations.”

46. I have been informed that such secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unmet need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) the taking of licenses under the patent by others and (h) the patentee proceeded contrary to the accepted wisdom of the prior art. I understand that secondary considerations are relevant where there is a connection, or nexus, between the evidence and the claimed invention.

47. In addition, I understand that the obviousness inquiry should not be done in hindsight, but must be done using the perspective of a person of ordinary skill in the relevant art as of the effective filing date of the patent claim.

48. I understand that in order for a claimed invention to be considered obvious, there must be some rationale in the prior art, or the knowledge of a person of ordinary skill in the relevant art at the time of the invention, for combining cited references as proposed.

49. I understand that obviousness may also be shown by demonstrating that it would have been obvious to modify what is taught in a single piece of prior art to create the patented invention. I understand that obviousness may be shown by establishing that it would have been obvious at the time of the purported invention

to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of one of ordinary skill in the art, I have been informed the following are examples of approaches and rationales that may be considered:

- a) Combining prior art elements according to known methods to yield predictable results;
- b) Simple substitution of one known element for another to obtain predictable results;
- c) Use of a known technique to improve similar devices (methods, or products) in the same way;
- d) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- e) Applying a technique or approach that would have been “obvious to try” (i.e., choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- f) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or

g) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. I also understand that this suggestion or motivation may come from such sources as explicit statements in the prior art, or from the knowledge or common sense of one of ordinary skill in the art.

50. I understand that an invention that might be considered an obvious variation or modification of the prior art may be considered non-obvious if one or more prior art references discourages or lead away from the line of inquiry disclosed in the reference(s). I understand a reference does not “teach away” from an invention simply because the reference suggests that another embodiment of the invention is better or preferred. My understanding of the doctrine of teaching away requires a clear indication that the combination should not be attempted (e.g., because it would not work or explicit statement saying the combination should not be made).

51. Intentionally left blank.

III. Qualifications of One of Ordinary Skill in the Art

52. Based on my review of these materials, I believe that the relevant field for purposes of the '100 Patent includes vehicle network security systems and

isolating on board computational components in response to a security breach event is detected. (*See* the '100 Patent, Ex. 1001, Abstract.)

53. I have been asked to provide my opinion as to the level of skill of a person having ordinary skill in the art (“PHOSITA” or “ordinary artisan”) of the '100 Patent at the time of the claimed invention, which I have been instructed to assume is November 16, 2011. In determining the characteristics of a hypothetical person of ordinary skill in the art of the '100 Patent at the time of the claimed invention, I was told to consider several factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. I also placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time.

54. In my opinion, a PHOSITA of the '100 Patent at the time of its filing would have been a person having, as of November 16, 2011, a Bachelor's degree in Electrical Engineering, Communication Engineering, or an equivalent degree with at least two years of experience in wireless communication systems, vehicle electrical and electronic systems, vehicle networking systems, network security systems, or related technologies. Additional industry experience could make up for less education and vice versa. Such a person of ordinary skill in the art would have

been capable of understanding the '100 Patent and the prior art references discussed herein.

55. Based on my education, training, and professional experience in the field of the claimed invention, I am familiar with the level and abilities of a person of ordinary skill in the art at the time of the claimed invention. Additionally, I met at least these minimum qualifications to be a person having ordinary skill in the art at least as of November 16, 2011. Further, although my qualifications may exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the '100 Patent have been rendered from the perspective of a person having ordinary skill in the art at the time of the invention.

56. Intentionally left blank.

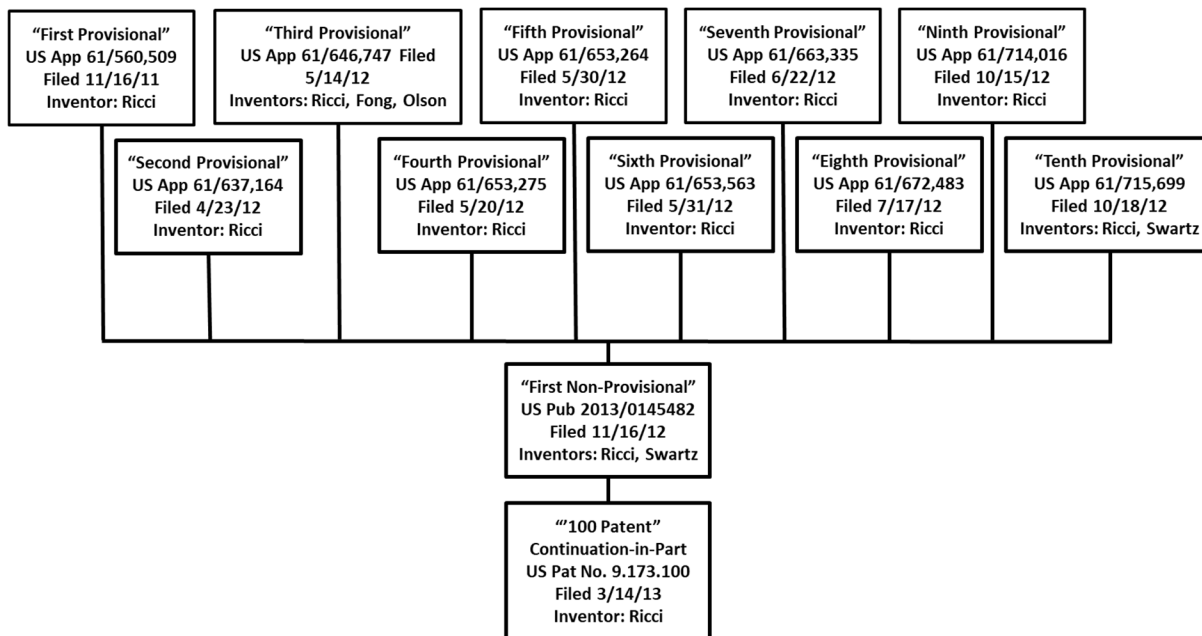
IV. U.S. Patent No. 9,173,100 to Ricci

A. Overview of the AutoConnect Patent Family

57. The AutoConnect family of related patents is illustrated below. I understand a first provisional Application No. 61/560,509 was filed on November 16, 2011 ("First Provisional"; Ex. 1151), a second provisional Application No. 61/637,164, was filed on April 23, 2012 ("Second Provisional"; Ex. 1152); a third provisional Application No. 61/663,335 was filed on June 22, 2012 ("Third Provisional"; Ex. 1153); a fourth provisional Application No. 61/646,747 was filed on May 14, 2012 ("Fourth Provisional"; Ex. 1154); a fifth provisional Application

No. 61/653,275 was filed on May 30, 2012 (“Fifth Provisional”; Ex. 1155); a sixth provisional Application No. 61/653,264 was filed on May 30, 2012 (“Sixth Provisional”; Ex. 1156); a seventh provisional Application No. 61/653,563 was filed on May 31, 2012 (“Seventh Provisional”; Ex. 1157); an eight provisional Application No. 61/672,483 was filed on July 17, 2012 (“Eighth Provisional”; Ex. 1158); a ninth provisional Application No. 61/714,016 was filed on October 15, 2012 (“Ninth Provisional”; Ex. 1159); and a tenth provisional Application No. 61/715,699 was filed on October 18, 2012 (“Tenth Provisional”; Ex. 1160).

58. It is my understanding that a non-provisional application No. 13/679,476 claiming the benefits of priority of all ten provisional applications was filed on November. 16, 2012, which later published as Publication No. 2013/0145482 (“First Non-Provisional”; Ex. 1161).



The '100 Patent Family

1. The “First Provisional” (Ex. 1151)

59. As shown in the above graphic, it is my understanding the AutoConnect Patent Family began with the November 16, 2011 filing of U.S. Provisional Patent Application No. 61/560,509 (“First Provisional”; Ex. 1151). (’100 Patent, Ex. 1001, Cover.)

60. The First Provisional, titled “COMPLETE VEHICLE ECOSYSTEM,” generally discloses the need for vehicle manufacturers to shift focus from merely adding features around a conveyance to building the vehicle environment around user comfort. (First Provisional, Ex. 1151, [0003]-[0005].) The disclosure describes an ecosystem designed to provide an “intuitive and immersive user experience” by integrating physical and mental comforts and operating seamlessly with current

electronic devices. (First Provisional, Ex. 1151, [0004].) The First Provisional generally discusses security and isolation capabilities, such as disabling features based on location or operator motion (*See* First Provisional, Ex. 1151, [0093]-[0099]), and the ability to selectively disassociate devices from the local network. (*See* First Provisional, Ex. 1151, [0120].)

2. The “Second Provisional” (Ex. 1152)

61. As shown in the above graphic, the AutoConnect Patent Family continues with the April 23, 2012 filing of U.S. Provisional Patent Application No. 61/637,164 (“Second Provisional”; Ex. 1152). (’100 Patent, Ex. 1001, Cover.)

62. The Second Provisional, titled “COMPLETE VEHICLE ECOSYSTEM,” generally discloses methods and systems for a complete vehicle ecosystem designed to “provide an intuitive and comfortable vehicular environment” by integrating new devices, methods, and systems with existing technology. (Second Provisional, Ex. 1152, Abstract, *see also* [0004].) The ecosystem covers a wide range of features, including customizable user interfaces (consoles, dashboards, heads-up displays), application stores, gesture recognition for control and safety, location-based services (parking/traffic), and systems for tracking, compliance, and remote vehicle control. The Second Provisional contains substantially similar disclosure to that of the First Provisional.

3. The “Third Provisional” (Ex. 1153)

63. As shown in the above graphic, the AutoConnect Patent Family continues with the May 14, 2012 filing of U.S. Provisional Patent Application No. 61/646,747 (“Third Provisional”; Ex. 1153). (’100 Patent, Ex. 1001, Cover.)

64. The Third Provisional, titled “BRANDING OF ELECTRICALLY PROPELLED VEHICLES VIA THE GENERATION OF SPECIFIC OPERATING SOUNDS,” generally discloses a system and method for controlling perceptible output (audio and/or visual) in a vehicle, particularly electric and hybrid vehicles, to generate synthetic sounds for branding purposes and to enhance safety by warning non-occupants (like pedestrians) of the vehicle's presence, motion, and operating status. (*See* Third Provisional, Ex. 1153, 8-10.)

4. The “Fourth Provisional” (Ex. 1154)

65. As shown in the above graphic, the AutoConnect Patent Family continues with the May 20, 2012 filing of U.S. Provisional Patent Application No. 61/653,275 (“Fourth Provisional”; Ex. 1154). (’100 Patent, Ex. 1001, Cover.)

66. The Fourth Provisional, titled “VEHICLE APPLICATION STORE FOR CONSOLE,” generally discloses a method and system for integrating an application store within a vehicle's on-board console or display, providing occupants with access to a plurality of free or paid applications. (*See* Fourth Provisional, Ex. 1154, pp. 7-8, 17.)

5. The “Fifth Provisional” (Ex. 1155)

67. As shown in the above graphic, the AutoConnect Patent Family continues with the May 30, 2012 filing of U.S. Provisional Patent Application No. 61/653,264 (“Fifth Provisional”; Ex. 1155). (’100 Patent, Ex. 1001, Cover.)

68. The Fifth Provisional, titled “CONTROL OF DEVICE FEATURES BASED ON VEHICLE STATE,” generally discloses a feature control system that governs access to one or more features of a communication device (e.g., a smartphone) based on the vehicle's state and the physical location of the device or user within the vehicle. (*See* Fifth Provisional, Ex. 1155, Abstract.)

6. The “Sixth Provisional” (Ex. 1156)

69. As shown in the above graphic, the AutoConnect Patent Family continues with the May 31, 2012 filing of U.S. Provisional Patent Application No. 61/653,563 (“Sixth Provisional”; Ex. 1156). (’100 Patent, Ex. 1001, Cover.)

70. The Sixth Provisional, titled “COMPLETE VEHICLE ECOSYSTEM,” generally discloses methods and systems designed to provide an intuitive and comfortable vehicular environment by integrating existing technology with new devices, methods, and systems to create a comprehensive ecosystem. (*See* Sixth Provisional, Ex. 1156, Abstract.)

7. The “Seventh Provisional” (Ex. 1157)

71. As shown in the above graphic, the AutoConnect Patent Family continues with the June 22, 2012 filing of U.S. Provisional Patent Application No. 61/663,335 (“Seventh Provisional”; Ex. 1157). (’100 Patent, Ex. 1001, Cover.)

72. The Seventh Provisional, titled “COMPLETE VEHICLE ECOSYSTEM,” has a substantially similar disclosure to that of the Second Provisional (Ex. 1152), with the addition of reference to “The Attachments” Exhibits A through C appended to the specification. (Seventh Provisional, Ex. 1157, [0153]-[0157]; *see also* 57-103.)

73. Exhibits A-C describe the FlexA3 architecture, discussing the components and mechanisms available for implementing vehicle security, particularly by introducing dedicated hardware (Firewall Blade) and specialized software (malware detection/elimination capabilities) (Seventh Provisional, Ex. 1157, 57-103.)

8. The “Eighth Provisional” (Ex. 1158)

74. As shown in the above graphic, the AutoConnect Patent Family continues with the July 17, 2012 filing of U.S. Provisional Patent Application No. 61/672,483 (“Eighth Provisional”; Ex. 1158). (’100 Patent, Ex. 1001, Cover.)

75. The Eighth Provisional, titled “VEHICLE CLIMATE CONTROL,” describes “an automated climate control system for a vehicle that considers factors”

and/or “the internal temperature of the vehicle passenger compartment”. (Eighth Provisional, Ex. 1158, [0004].)

9. The “Ninth Provisional” (Ex. 1159)

76. As shown in the above graphic, the AutoConnect Patent Family continues with the October 15, 2012 filing of U.S. Provisional Patent Application No. 61/714,016 (“Ninth Provisional”; Ex. 1159). (’100 Patent, Ex. 1001, Cover.)

77. The Ninth Provisional, titled “VEHICLE MIDDLEWARE,” generally describes a comprehensive vehicle middleware system intended to improve “data stream management and integration,” enhance “vehicle safety, data security, and/or data processing,” and enable “remote authorized third party” access to vehicle functions. (Ninth Provisional, Ex. 1159, 3.) The core architecture is built around one or more processing modules located at various points within the vehicle, which are configured to connect and interface with the various buses in the vehicle and implement a “middleware point of control.” (Ninth Provisional, Ex. 1159, 10-11.)

78. The Ninth Provisional includes discussion regarding Figure 24, below:

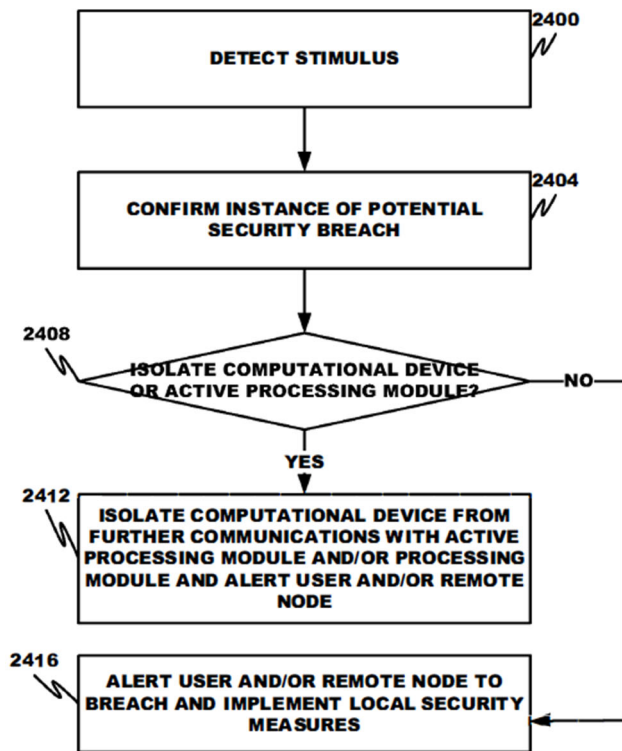


FIG. 24

Ninth Provisional, Ex. 1159, Figure 24

79. The Ninth Provisional discloses the following narrative description and discussion corresponding to Figure 24:

Operation of Network Controller 1528

Fig. 24 depicts another operation of the network controller 1528. As noted,
20 security for cyber attacks is important for an Internet-enabled vehicle. Drivers are
accessing data from Internet service providers via smart phone, tablet computer, and/or
on board or embedded technologies as well as utilizing hands-free communication
technology to send and receive phone calls and text messages. Automotive
manufacturers are sending and receiving data based on electronic sensor readings and
25 event data recording. Due to the potentially dire consequences of a security breach on on
board processing module operation, rigorous security measures should be deployed.
While the vehicular network can employ passive techniques, such as configuration of
access restrictions in access points (such as encryption, checks on MAC addresses,
disabling ESSID broadcasting, isolation of the vehicular network by the firewall and
30 gateway, hiding the SSID (Service Set Identifier), MAC ID filtering (allowing access

from know, pre-approved MAC addresses, 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 (in one or more
of 2, 3, and/or application layer), and RF shielding substantially surrounding the interior
5 of the vehicle (to attenuate signals and prevent wireless signals from propagating outside
the vehicle), active techniques may also be employed. Communications with external
computational devices 1532 can be channeled through the gateway/firewall 1512.

One active technique is depicted in Fig. 24.

In step 2400, the network controller 1528 detects a stimulus, such as an instance
10 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. The stimulus may be a warning signal received by the network controller 1528
15 from the gateway/firewall 1512, a honeypot (which is a decoy network-assistant resource
to provide network surveillance and early-warning tool, a network node, mapping a
template corresponding to a specific attack type to received signals, a network probe, and
the like.

In step 2404, the network controller 1528 attempts to confirm the instance of
20 potential security breach. This can be done by reviewing historical behavior, such as
shown by communication logs (containing signal description (e.g., type, source,
destination, protocol, and payload type) and signal receipt timestamps) not only for the
current node but also for other nodes and comparing the behavior to templates
characteristic of differing types of attacks and/or applying rules to the historical behavior.
25 The security breach details, signal description (e.g., type, source, destination, protocol,
and payload type) and signal receipt timestamps, are recorded in memory 220 and
firewall settings, including whitelists and blacklists, are updated.

In decision diamond 2408, the network controller 1528 determines whether or not
the computational devices impacted or potentially impacted by the security breach can be
30 isolated from other vehicular network components or whether the active processing

module can be isolated from other non-critical computational components. For an external computational device 1532, such as a tablet computer, smart phone, laptop computer, personal digital assistant, and the like, isolation is possible simply by denying vehicular wireless network access or access, by a component of the vehicular wireless network, to the external computational device 1532. For components in the vehicular wireless network, communications to and from the affected components, which normally do not pass through the gateway/firewall, can be redirected through and filtered by the gateway/firewall or, depending on the criticality of the affected component(s), such communications can be blocked. For the active processing module 124, non-critical communications to and from other non-critical computational components, which normally do not pass through the gateway/firewall, can be redirected through and filtered by the gateway/firewall before being provided to the active processing module or, depending on the criticality of the communication(s), such communications can be blocked. Critical communications, or communications with critical components, typically cannot be delayed by firewall processing. In one variation, a critical communication security mechanism is activated when a security breach is detected. The security mechanism can include, for example, one or more of encrypting access restrictions in critical components and the active processing module (such as encryption, checks on MAC addresses, disabling ESSID broadcasting, hiding the SSID (Service Set Identifier), MAC ID filtering (allowing access from known, pre-approved MAC addresses, 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, and end-to-end encryption (in one or more of 2, 3, and/or application layer). When isolation is possible, the network controller 1528, in step 2412, isolates the affected computational device(s) from further communications with or filters communications with the active processing module 124 or the active processing module from further communications with the affected computational component(s) and alerts the user and/or a remote node 1500 of the security breach and details regarding it. When isolation is not possible, the network controller 1528 alerts the user and/or a remote node 1500 of the security breach and details regarding it. The critical security mechanism may be activated to protect the critical components and active processing module.

Ninth Provisional, Ex. 1159, 48-51

10. The “Tenth Provisional” (Ex. 1160)

80. As shown in the above graphic, the AutoConnect Patent Family continues with the October 18, 2012 filing of U.S. Provisional Patent Application No. 61/715,699 (“Tenth Provisional”; Ex. 1160). (’100 Patent, Ex. 1001, Cover.)

81. The Tenth Provisional, titled “VEHICLE MIDDLEWARE,” generally describes a vehicle middleware system utilizing modular processing units to integrate and manage communications across diverse vehicle buses (CAN, LIN, Ethernet) for improved data stream management and interoperability. (*See* Tenth Provisional, Ex. 1160, Abstract; *see also* Tenth Provisional, Ex. 1160, 16.)

82. The Tenth Provisional is largely identical to the Ninth Provisional, with the exception of the addition of Figure 29 in the Tenth Provisional, and an accompanying description of the “Presence Reporting Module 2056”. (*See* Tenth Provisional, Ex. 1160, 26, 73-79.)

83. The Tenth Provisional has an identical Figure 24 to the Ninth Provisional, and an identical description of Figure 24, as shown above. (*See* Tenth Provisional, Ex. 1160, 52-54.)

11. The “First Non-Provisional” (Ex. 1161)

84. As shown in the above graphic, the AutoConnect Patent Family continues with the November 16, 2012 filing of U.S. Non-Provisional Patent Application No. 13/682,362, published as U.S. Patent Application Publication No. 2013/0145482 (“First Non-Provisional”; Ex. 1161). (’100 Patent, Ex. 1001, Cover.)

85. The First Non-Provisional titled “VEHICLE MIDDLEWARE,” purports to claim priority to the First through Tenth Provisional Applications. (Ex. 1161; 1-7.) The disclosure of the First Non-Provisional is substantially identical to

the disclosure of the Tenth Provisional (and therefore the Ninth Provisional) in general, including identical Figure 24 and accompanying description in the specification. (*See* First Non-Provisional, Ex. 1161, pp. 61-63, 119.)

86. The First Non-Provisional, however, adds Figure 30 and its accompanying description, which is not present in any of the First through Tenth Provisionals. Figure 30 shows a social networking module 2070. (*See* First Non-Provisional, Ex. 1161, 83-89, 125.)

87. Intentionally left blank.

B. The '100 Patent File History

88. It is my understanding U.S. Patent Application No. 13/828,960 was filed on March 14, 2013 with twenty four (24) claims, including independent claims 1, 9, and 17. ('100 Patent File History, Ex. 1002, 5, 101-106.)

89. It is my understanding that: (1) on October 18, 2013, the Patentee filed an Information Disclosure Statement listing over 100 references. ('100 Patent File History, Ex. 1002, 151-154); on July 3, 2014, the Patentee filed another Information Disclosure Statement listing over 50 references. ('100 Patent File History, Ex. 1002, 1161); and on October 20 2014, the Patentee filed another Information Disclosure Statement listing over 30 references. ('100 Patent File History, Ex. 1002, 489-490.)

90. It is my understanding that on January 5, 2015, the Examiner issued the first Office Action rejecting all claims 1-24 as being obvious under 35 U.S.C. § 103

over Maher (US 2013/0212659) in view of Gelvin (US 7,891,004). ('100 Patent File History, Ex. 1002, 621-634.)

91. It is my understanding that on April 6, 2015, the Patentee filed a Response including amendments to all claims 1-24. ('100 Patent File History, Ex. 1002, 655-673.) Among other things, claim 1 was amended to recite “*wherein the isolation is one or more of (1) denying vehicular wireless network access to the computational component affected by the security breach instance, (2) directing communications to and from the computational component affected by the 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 security breach instance, and (4) activating a second security mechanism in response to the security breach instance.*” ('100 Patent File History, Ex. 1002, 658.) The Patentee also submitted arguments that the above features are not taught or suggested by Maher and Gelvin. ('100 Patent File History, Ex. 1002, 669-670.)

92. It is my understanding that on April 14, 2015, the Patentee filed another Information Disclosure Statement listing over 70 references. ('100 Patent File History, Ex. 1002, 676-679.)

93. It is my understanding that on June 5, 2015, the Examiner issued a Notice of Allowance with an Examiner’s Amendment correcting a typographical error in claim 1. The Examiner indicated “No reason for allowance is needed as the

record is clear in light of this instant Examiner's Amendment and applicant's arguments and amendment filed on 04/06/2015.” (’100 Patent File History, Ex. 1002, 925-934.)

94. It is my understanding that on June 3, 2015, and September 4, 2015, the Patentee filed additional Information Disclosure Statement collectively submitting over 10 references. (’100 Patent File History, Ex. 1002, 953, 992.)

95. On September 8, 2015, the Patentee filed an Amendment After Allowance Pursuant to 37 C.F.R. § 1.312 which included amendments to independent claims 1, 9 and 17 to include an “instance of a breach of the security measure,” and arguments that the claim amendments were intended to “clarify any potential ambiguity”⁷ and did not require an additional search. (’100 Patent File History, Ex. 1002, 1076-1087.)

96. It is my understanding that on September 10, 2015, the Examiner issued a Notice of Non-Compliant Information Disclosure Statement indicating the Information Disclosure Statement filed on September 4, 2015 was not compliant with 37 C.F.R. § 1.97(d) because the Information Disclosure Statement lacked a

⁷ Unless indicated to the contrary, all emphasis in the quoted excerpts has been added.

statement as specified in 37 C.F.R. § 1.97(e). ('100 Patent File History, Ex. 1002, 1095.)

97. It is my understanding that on September 25, 2015, the Examiner issued a Response to Amendment under Rule 312 indicating that the amendment filed on September 8, 2015 was entered. ('100 Patent File History, Ex. 1002, 1099-1100.)

98. It is my understanding that on October 27, 2015, the application issued as the '100 Patent to Flextronics AP, LLC. ('100 Patent, Ex. 1001, Cover.)

99. It is my understanding that on January 18, 2016, the Patentee filed a Request for Certificate of Correction to correct a typographical error in claim 24. ('100 Patent File History, Ex. 1002, 1106-1107.)

100. It is my understanding that on March 29, 2016, the Examiner issued the Certificate of Correction correcting the typographical error in claim 24 ('100 Patent File History, Ex. 1002, 1110.)

1. Priority of the '100 Patent

101. I understand the '100 Patent was filed as a Continuation-in-Part ("CIP") of the First Non-Provisional Application, and through that application it purported to claim priority to the First through Tenth Provisional Applications. ('100 Patent File History, Ex. 1002, 9-10.) I therefore evaluated whether each earlier application provides sufficient written description support for the claims of the '100 Patent.

a. The First, Second, Third, Fourth, Fifth, Sixth,

Seventh, and Eighth Provisionals

102. It is my opinion that none of the First through Eighth Provisionals (Exs. 1151-1158) explicitly disclose the core conditional logic required by the independent claims of the '100 Patent—specifically, conditional logic claimed to differentiate the internal security status of on-board computational components and then protectively isolate components based on that determination.

103. In particular, the First through Eighth Provisionals fail to disclose the critical limitation of claim 1[d], element (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.*” This conditional determination is a central feature of the claimed invention and is not supported by the disclosures in the First through Eighth Provisionals

104. Because these earlier applications do not disclose the required conditional decision, they also necessarily fail to disclose the corresponding conditional actions recited in claim 1[e] element (iii): “*when the computational component affected by the instance of a breach . . . can be isolated . . . 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 . . . from the computational component affected by the instance of a breach . . . and (b) isolate the computational*

component affected by the instance of a breach . . . from the at least one on board computational component not affected by or potentially affected by the instance of a breach . . . [.]” These action steps logically depend on the conditional determination in (ii), and thus also lack written description support.

105. Accordingly, in my opinion, the First through Eighth Provisionals do not provide sufficient written description for the subject matter eventually claimed in the ’100 Patent.

106. Therefore, the ’100 Patent cannot claim priority to any of the First through Eighth Provisionals.

b. The Ninth and Tenth Provisionals and The First Non-Provisional

107. As discussed above, the Ninth and Tenth Provisionals and the First Non-Provisional each contain the same version of Figure 24 and the same accompanying description. (See sections IV.A.9-11.)

108. Because the ’100 Patent was filed as a CIP of the First Non-Provisional, I reviewed the specification filed with the ’100 Patent and compared it directly to the specification of the First Non-Provisional.

109. The specification filed with the ’100 Patent contains substantial new disclosure regarding Figure 24—material that does not appear in any of the First through Tenth Provisionals or in the First Non-Provisional. These additions are

reproduced and highlighted in the file history (100 Patent File History, Ex. 1002, 71-72). As I understand it, these new portions were introduced for the first time in the '100 Patent itself.

In decision diamond 2408, the network controller 1528 determines whether or not the computational devices impacted or potentially impacted by the security breach event can be isolated from other vehicular network components or whether the active processing module

20 can be isolated from other non-critical computational components. This can depend, for example, on whether the affected computational component is physically and/or logically within or internal and/or external to a Dimilitarized Zone ("DMZ") or perimeter network. As will be appreciated, a DMZ is a physical or logical subnetwork, within the vehicular wireless network, that contains and exposes the network's external-facing services to a larger

25 untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to the vehicular wireless network; that is, an external attacker only has access to equipment in the DMZ, rather than any other part of the network. The DMZ typically includes services, such as Web servers, mail servers, FTP servers, and voice mail servers. For an external computational device 1532 (outside the DMZ), such as a tablet computer,

30 smart phone, laptop computer, personal digital assistant, and the like, and/or device within the DMZ isolation is possible simply by denying vehicular wireless network access or access, by a component of the vehicular wireless network, to the external computational device 1532. For components in the vehicular wireless network, communications to and from the affected components, which normally do not pass through the gateway/firewall, can be redirected through and filtered by the gateway/firewall or, depending on the criticality of the

5 affected component(s), such communications can be blocked. For the active processing module 124, non-critical communications to and from other non-critical computational components, which normally do not pass through the gateway/firewall, can be redirected through and filtered by the gateway/firewall before being provided to the active processing module or, depending on the criticality of the communication(s), such communications can

10 be blocked. Critical communications, or communications with critical components, typically cannot be delayed by firewall processing. In one variation, a critical communication security mechanism is activated for the components physically and/or logically within the vehicular wireless network and internal to the DMZ when a security breach event is detected. The security mechanism can include, for example, one or more of encrypting access restrictions

15 in critical components and the active processing module (such as encryption, checks on MAC addresses, disabling ESSID broadcasting, hiding the SSID (Service Set Identifier), MAC ID filtering (allowing access from known pre-approved MAC addresses, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, and end-to-end encryption

20 (in one or more of 2, 3, and/or application layer(s))).

'100 Patent File History, Ex. 1002, 71-72

110. Most importantly, the '100 Patent is the first application to introduce and describe “a perimeter network” and a “DMZ” in the context of the isolation determinations associated with Figure 24. ('100 Patent File History, Ex. 1002, 70-71.) These concepts do not appear in the Ninth or Tenth Provisionals (Exs. 1159, 1160), nor in the First Non-Provisional (Ex. 1161), but are present in the claims of the '100 Patent ('100 Patent, Ex. 1001, claims).

111. Thus, in my opinion, the earliest possible priority date that the '100 Patent could be entitled to is the date of the Ninth and Tenth Provisional filings, October 15, 2012 and October 18, 2012, respectively. (Exs. 1159, 1160.)

112. However, because the key added subject matter—including the DMZ/perimeter network concepts and expanded logic around conditional isolation—is disclosed only in the '100 Patent specification itself, it is my understanding that the '100 Patent is more likely entitled only to its own filing date, March 14, 2013. (Ex. 1001, Cover; Ex. 1002.)

2. Delayed Payment of Maintenance Fee

113. It is my understanding that on August 3, 2022, the new Patent Owner (AutoConnect Holdings LLC) filed a Petition to Accept Unintentionally Delayed Payment of Maintenance Fee in an Expired Patent with an Affidavit stating the missed payment was “unintentional.” ('100 Patent File History, Ex. 1002, 1137-1146.)

114. It is my understanding that on March 7, 2023, the United States Patent Trademark Office (“USPTO”) issued a Petition Decision which dismissed the Petition on the ground that the Petition was filed more than 2 years after the patent expired. (’100 Patent File History, Ex. 1002, 1155-1159.)

115. It is my understanding that on the same day March 7, 2023, the new Patent Owner filed a Renewed Petition with two affidavits. (’100 Patent File History, Ex. 1002, 1161-1172.)

116. On April 5, 2023, the USPTO issued a second Petition Decision which granted the Renewed Petition. (’100 Patent File History, Ex. 1002, 1175-1177.)

117. It is my understanding that Amirtahmasebi (Ex. 1019), Spaur (Ex. 1020), and Peirce (Ex. 1021) were not considered during examination and are not cited on the ’100 Patent (’100 Patent, Ex. 1001, at 1-4.)

V. Claim Construction

118. In order to properly evaluate these claims, I understand that the terms of the claims must first be construed. I also understand that, at the same time, absent some reason to the contrary, claim terms are typically given their ordinary and accustomed meaning as would be understood by one of ordinary skill in the art.

VI. State of the Art

A. Vehicle Network Systems

119. Modern vehicles rely on a highly distributed network of controllers (e.g., electronic control units (ECUs)) “that are increasingly networked together by various bus communications systems” and collectively perform a wide range of operational functions. (Wolf, Ex. 1082, p. 1⁸.) Vehicle communication networks “have access to several crucial components of the vehicle, like breaks, airbags, and the engine control.” (Wolf, Ex. 1082, p. 1.) As vehicles become increasingly software-defined and feature-rich, the number, complexity, and interdependence of these ECUs has grown significantly, yielding increased security risks and making in-vehicle network design and security foundational to automotive system designs.

120. To allow these ECUs to communicate, vehicles incorporate a variety of in-vehicle networks (e.g., CAN, LIN, FlexRay, MOST, Bluetooth), each chosen for its suitability to particular types of data exchange. (Wolf, Ex. 1082, p. 2.) One of the most commonly used communication protocols is the Controller Area Network (CAN) bus, which “is an event-triggered controller network for serial communication[s]” used for “real-time in-car communication between controllers, networking for example the antilock breaking [sic] system (ABS) or the engine

⁸ Wolf, Ex. 1082 is a true and accurate copy of a research paper that I understand was published in November 2004.

management system.” (Wolf, Ex. 1082, pp. 2-3.) Messages transmitted on a CAN bus can be broadcasted to all connected nodes using a priority identifier; however, all receiving nodes decide individually if the message should be processed. (Wolf, Ex. 1082, p. 3.) This arbitration mechanism ensures that high-priority messages take precedence on the network, making the protocol particularly well suited for critical vehicle operations. However, CAN is limited in bandwidth, which restricts its use for high-volume or multimedia data and motivates the continued reliance on other networks for data-rich communication needs. (Wolf, Ex. 1082, p. 3.)

121. In addition to CAN, other bus systems are incorporated to support other vehicle functions. For example, the Local Interconnect Network (LIN) provides a low-cost, low-speed alternative for non-safety-critical components, such as automatic door locking mechanisms, power-windows and mirrors, and body electronics. (Wolf, Ex. 1082, pp. 2-3.) LIN operates in a “master-slave” architecture with a single master coordinating all message transmissions, making it ideal for simple actuators and sensors that do not require real-time responsiveness. (Wolf, Ex. 1082, pp. 3-4.)

122. Another example system is FlexRay, which was designed as a high-performance, time-triggered bus to support deterministic communication in advanced chassis and powertrain systems. (Wolf, Ex. 1082, pp. 2, 4.) FlexRay provides fault-tolerant, dual-channel communication and has significantly higher

data rates than CAN, enabling synchronized, safety-critical control tasks such as active suspension, steer-by-wire, and advanced driver assistance systems. (Wolf, Ex. 1082, p. 4.)

123. Finally, the Media Oriented System Transport (MOST) bus, a high-bandwidth multimedia bus, is used to “carry audio and video data,” making it suitable for infotainment systems and other high-data-rate features. (Nilsson, Ex. 1087, p. 2⁹.) MOST employs a ring or star topology optimized for continuous streaming data, ensuring stable, low-latency distribution of entertainment content throughout the vehicle cabin. (Wolf, Ex. 1082, p. 4.)

124. In addition to individual bus protocols, vehicles utilize gateway control units to interconnect the various network domains and manage cross-bus communication. (Hoppe, Ex. 1084, pp. 15-16¹⁰.) A gateway ECU “implements a kind of network isolation, which saves bandwidth and especially reduces the impact of harmful messages” circulating across the system. (Hoppe, Ex. 1084, p. 16.)

⁹ Nilsson, Ex. 1087 is a true and accurate copy of a research article that I understand was publicly available and presented at the RTIC in 2008.

¹⁰ Hoppe, Ex. 1084 is a true and accurate copy of an article that I understand was publicly available and presented at SAFECOMP in 2008 and reprinted in 2011 in Reliability Engineering & System Safety, Volume 96, Issue 1, January 2011.

During normal vehicle operation, “internal communication is not accessible from the open diagnostics interface,” underscoring the gateway’s role in regulating traffic between internal networks and externally accessible interfaces. (Hoppe, Ex. 1084, p. 16.) The gateway ECU controls which messages may cross subsystem boundaries, “unlock[ing] these IDs for forwarding between the respective subnetworks for the duration of the session” during diagnostics while leaving other messages confined to their originating networks. (Hoppe, Ex. 1084, p. 16.) As the number of ECUs and subnetworks has expanded, these gateway units have become essential for managing message translations, routing decisions, and isolation between domains, ensuring that only appropriate traffic propagates across the increasingly complex vehicle communication architecture.

125. Beyond wired communication buses, many vehicles now include “the integration of wireless interfaces such as GSM (Global System for Mobile Communications) or Bluetooth,” which “enable[s] the internal vehicle network to communicate with external devices surrounding the car as well as the reception of various broadcast stations.” (Wolf, Ex. 1082, pp. 1, 3.) These wireless interfaces operate alongside traditional buses and allow vehicles to exchange data with backend servers, roadside equipment, and consumer devices, thereby linking previously isolated in-vehicle networks with external communication sources. (Wolf, Ex. 1082, 3.)

126. Alongside in-vehicle connectivity, modern architectures extend outward into external wireless communication systems that augment the vehicle's network environment. Many vehicles participate in larger-scale vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication systems – collectively known as vehicular ad hoc networks (VANETs) – which allow vehicles to exchange information with other vehicles and roadside units. (Lin, Ex. 1085, p. 88¹¹.) These systems broadcast real-time operational data, including “position, current time, direction, speed, brake status, [and] steering angle,” to support cooperative driving and roadway safety. (Lin, Ex. 1085, pp. 88.) They also allow vehicles to exchange traffic and road-condition information that informs route selection and local driving decisions. (Golle, Ex. 1083, p. 29¹².)

127. Intentionally left blank.

128. Intentionally left blank.

¹¹ Lin, Ex. 1085 is a true and accurate copy of a research article that I understand was published by IEEE on April 30, 2008.

¹² Golle, Ex. 1083 is a true and accurate copy of a research article that I understand was published by Association for Computing Machinery on October 1, 2004.

B. Vehicle Network Security

129. As vehicle communication systems evolve, the risk of cyberattacks on both in-vehicle networks and inter-vehicle communication infrastructures have become a significant concern. As discussed above, “[m]odern vehicles contain an in-vehicle network of embedded electronic control units (ECUs) responsible for most of the functionality in the vehicle[,]A” and these ECUs are “highly plausible targets for future attacks.” (Nilsson, Ex. 1087, p. 1.) Because internal networks are interconnected, a compromise in one ECU can propagate to others on different subnetworks. At the same time, the addition of external communication channels—including telematics, wireless key systems, and vehicle-to-vehicle or vehicle-to-infrastructure links—creates attack surfaces through which malicious code or commands can be introduced from outside the vehicle and injected into the in-vehicle network. For these reasons, vehicle security architectures needed to address threats capable of moving laterally within internal networks as well as threats transmitted wirelessly from outside a vehicle’s communication perimeter.

130. Within vehicle-to-vehicle and vehicle-to-infrastructure networks (VANETs), the broadcast of real-time operational data—including “position, current time, direction, speed, brake status, [and] steering angle”—was recognized as essential for cooperative safety systems. (Lin, Ex. 1085, pp. 88.) Attackers in these systems may exploit the lack of centralized control through techniques such as Sybil

attacks, in which a single device masquerades as many, creating situations where a vehicle claims “to be hundreds in order to create the illusion of a congested road.” (Parno, Ex. 1088, p. 2¹³.) VANET environments were also susceptible to intentionally false data, as authentication alone does not prevent a malicious vehicle from “transmitting fraudulent data about road congestion or vehicle position,” a form of attack that “can be quite damaging.” (Golle, Ex. 1083, p. 29.)

131. In-vehicle networks are similarly exposed to a wide range of logical and physical attacks, the consequences of which can vary greatly depending on what network was affected. (Wolf, Ex. 1082, p. 7.) For example, “attacks on LIN or multimedia networks may result in the failure of power windows or navigation software,” however, “successful attacks on CAN networks” or “real-time buses like FlexRay” could result in malfunction of “important driving assistants” or “driving commands like steering or breaking.” (Wolf, Ex. 1082, p. 7.)

132. The integration of wireless interfaces into the vehicle architecture further expanded the attack surface by introducing communication paths that were not previously exposed. As manufacturers began adding capabilities intended to

¹³ Parno, Ex. 1088 is a true and accurate copy of a research article that I understand was publicly available and presented at the Workshop on Hot Topics in Networks in 2005.

support “streaming multimedia and infotainment” as well as “software updates and remote diagnostics,” these additions simultaneously created new risks and vulnerabilities to portions of the in-vehicle network that had been “largely protected from everything except physical access attacks.” (Jusufovic, Ex. 1086, p. 1¹⁴.) The increased connectivity meant that communications once safeguarded by physical isolation were now exposed to interception or manipulation at any point “near the vehicle, at a radio tower or on the Internet,” since “unencrypted traffic can easily be read.” (Jusufovic, Ex. 1086, p. 1.)

133. Wireless access introduced “a higher risk of an attacker injecting, modifying or replaying messages[,]” enabling an adversary to issue altered operational commands—such as “telling the vehicle to unlock the door rather than checking if the door was locked”—or to conduct passive surveillance by “eavesdrop[ping] on the traffic and . . . extract[ing] privacy-related data from the link.” (Jusufovic, Ex. 1086, p. 10.) Remote connectivity also enabled identity-based compromises in which “[b]y impersonating a vehicle, an attacker can set up a connection to the portal[,]” gaining access to confidential information including

¹⁴ Jusufovic, Ex. 1086 is a true and accurate copy of a Master of Science thesis that I understand was published by Chalmers University of Technology in November 2009.

“proprietary software that the portal intended to send to the impersonated vehicle.” (Jusufovic, Ex. 1086, p. 10.) These risks extended to firmware distribution mechanisms as permitting remote diagnostics and firmware downloads opened the possibility that an attacker could “modify the firmware in transit,” causing the “flashing of the firmware” to fail and leaving only partial updates, or enabling the installation of “arbitrary firmware” on an ECU. (Nilsson, Ex. 1087, p. 3) (emphasis removed.)

134. To address these risks, security mechanisms were developed to strengthen both inter-vehicle and in-vehicle communication environments. To protect communication integrity, systems incorporated authenticated exchanges based on “a challenge-response mechanism” in which a verifier issues “a random number (the challenge)” and the claimant generates a cryptographic response using shared secrets. (Bluetooth Specification, Ex. 1052, Vol. 3, p. 393, Vol. 2, p. 247¹⁵.) Authorization procedures further ensured that a remote device could access only

¹⁵ Bluetooth Specification, Ex. 1052 is a true and accurate copy of a specification that I understand was published by Bluetooth Special Interest Group (SIG), Inc. in 2010. Bluetooth Specification, Ex. 1052 is available at <https://www.bluetooth.com/specifications/specs/core-specification-4-0/>, accessed on December 5, 2025.

specific permitted services once its identity had been verified. (Bluetooth Specification, Ex. 1052, Vol. 3, p. 393.) Digital certificates further provided an additional layer of trust by embedding “the public key, permissions and identity related information” needed to secure communications and confirm the legitimacy of software or commands received by the vehicle. (IBM TCP/IP Tutorial, Ex. 1060, pp. 278-279.)

135. Architectural protections were also deployed to contain and filter traffic across network domains. For example, firewalls were implemented as systems that monitor and control incoming and outgoing network traffic based on pre-defined security rules. Gateway connected networks operated different protocols and acted as controlled entry/exit point[s] for data traffic. (See IBM TCP/IP Tutorial, Ex. 1060, p. 280-293 (discussing firewalls); IEEE Dictionary¹⁶, Ex. 1051, p. 477 (defining “gateway”); IBM TCP/IP Tutorial¹⁷, Ex. 1060, p. 16 (discussing “gateway”).)

136. Beyond filtering, a critical aspect of improving vehicle network security involved strengthening the ability to isolate different communication

¹⁶ IEEE Dictionary, Ex. 1051 is a true and accurate copy of a dictionary that I understand was published by IEEE in December 2000.

¹⁷ IBM, Ex. 1060 is a true and accurate copy of a guide that I understand was published by International Business Machines Corporation in October 1998.

domains so that activity on one bus, or on one affected component, could not freely spread to others. Because vehicles relied on interconnected buses to exchange information, the resulting “net-spanning data exchange” meant that a compromise in one network could allow access to additional systems unless safeguards were in place. (Wolf, Ex. 1082, p. 7.) To limit this lateral movement, gateways were configured to forward only the messages necessary for cross-domain coordination while suppressing all others—ensuring that “some messages are to be forwarded” “for further processing” while “[o]thers are only needed within their original subnetwork and therefore are not forwarded anywhere[,]” a strategy that helped reduce “the impact of harmful messages.” (Hoppe, Ex. 1084, p. 16.) Other architectures funneled “all inter-bus communication . . . exclusively . . . over the gateway processor[,]” which kept keys and authorizations in a “protected memory area” and allowed only authenticated controllers to pass data between bus domains. (Wolf, Ex. 1082, p. 10.)

137. Other protective measures included isolating the wireless link from the internal vehicle network, using mutual authentication, and encrypting all portal–vehicle communication so that traffic could “be encrypted and protected against modification” and guarded from replay by incorporating timestamps or freshness indicators (i.e., messages included a timestamp or sequence number so that old messages cannot be replayed, preventing an attacker from capturing and reusing

prior communications to issue unauthorized commands.) (Jusufovic, Ex. 1086, p. 12.)

138. Intentionally left blank.

139. Intentionally left blank.

VII. Overview of the Key Prior Art References Relied Upon

A. Vehicular Networks – Security, Vulnerabilities and Countermeasures, Master of Science Thesis in the program Networks and Distributed Systems (“Amirtahmasebi” Ex. 1019)

140. Amirtahmasebi is a Master of Science thesis in the program Networks and Distributed Systems at the University of Gothenburg in Sweden that was written by Kasra Amirtahmasebi and Seyed Reza Jallinia, and was published on July 8, 2010. (Ex. 1019, Librarian Declaration, Exhibit A, and Exhibit B; “Amirtahmasebi”.) I understand that Amirtahmasebi is prior art to all claims of the ’100 Patent under pre-AIA 35 U.S.C. § 102(b) because it was published more than one year before the earliest claimed priority date of the ’100 Patent.

141. Amirtahmasebi discloses that “[v]ehicular networks are mainly divided into two main categories . . . Inter-vehicle networks . . . called [vehicular ad hoc networks] VANETs and are mainly for distribution of traffic and road conditions among vehicles in range. . . . In-vehicle networks . . . are a combination of Electronic Control Units (ECU), sensors and actuators.” (Amirtahmasebi, Ex. 1019, p. 11.)

142. Amirtahmasebi further discloses that “VANETs consist of a number of On-Board Units (OBU) which are located inside the vehicles and a number of Road-Side Units (RSU) which form the infrastructure of the network.” (Amirtahmasebi, Ex. 1019, p. 13.) Amirtahmasebi further discloses the communication in the VANET is divided into “Vehicle-to-Vehicle (V2V) Communication, were [sic] the nearby vehicles will communicate traffic and road conditions to one another [and] Vehicle-to-Infrastructure (V2I) Communication, were [sic] vehicles communicate their gathered information to the nearest RSU in order to distribute the information faster and more effectively.” (Amirtahmasebi, Ex. 1019, p. 13.)

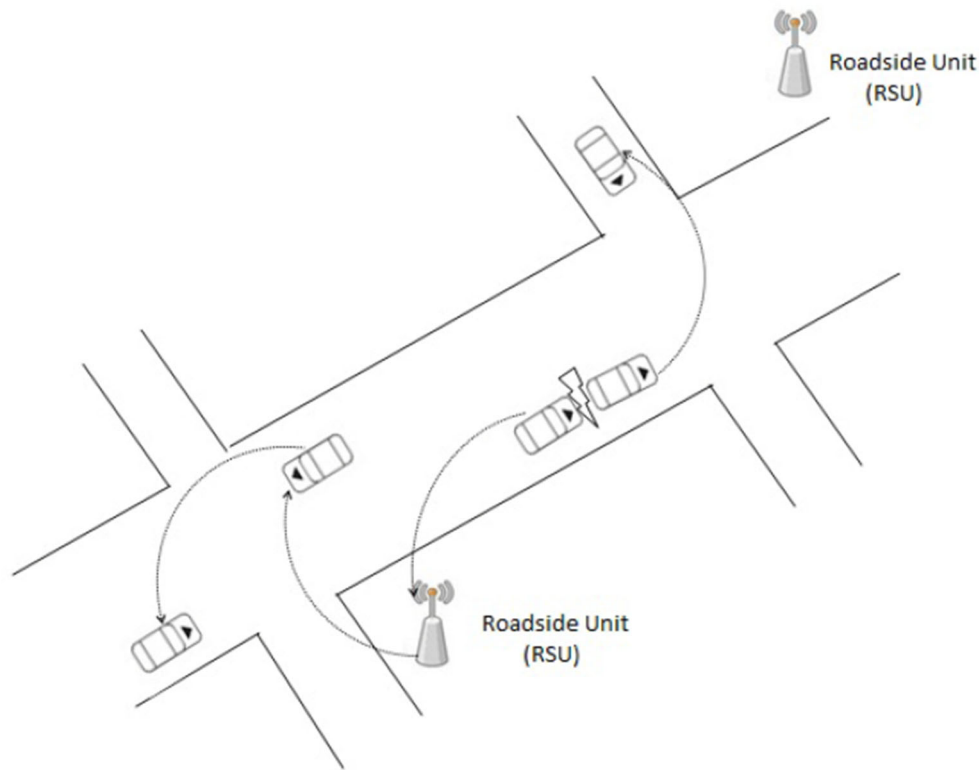


Figure 1. Conceptual VANET Infrastructure

Amirtahmasebi, Ex. 1019, Figure 1

143. As shown in Amirtahmasebi Figure 1 presented above, a vehicle communicates with other vehicles via V2V connections. A vehicle communicates with roadside units RSUs via V2I connections.

144. Amirtahmasebi further discloses that “[a] typical modern car has around 50-70 ECUs onboard. As mentioned above, in order to deliver different messages and information on-time and due to different demands and requirements of ECUs, different network types must be created based on speed and reliability.” (Amirtahmasebi, Ex. 1019, p. 24.)

145. Amirtahmasebi further discloses automotive bus systems, stating: “Apart from ECU classification, in-vehicle networks require different communication buses with different characteristics as well.” (Amirtahmasebi, Ex. 1019, p. 25.) The in-vehicle network may include buses such as Local Interconnect Network (LIN), Controller Area Network (CAN), Media Oriented System Transport (MOST), and FlexRay buses.

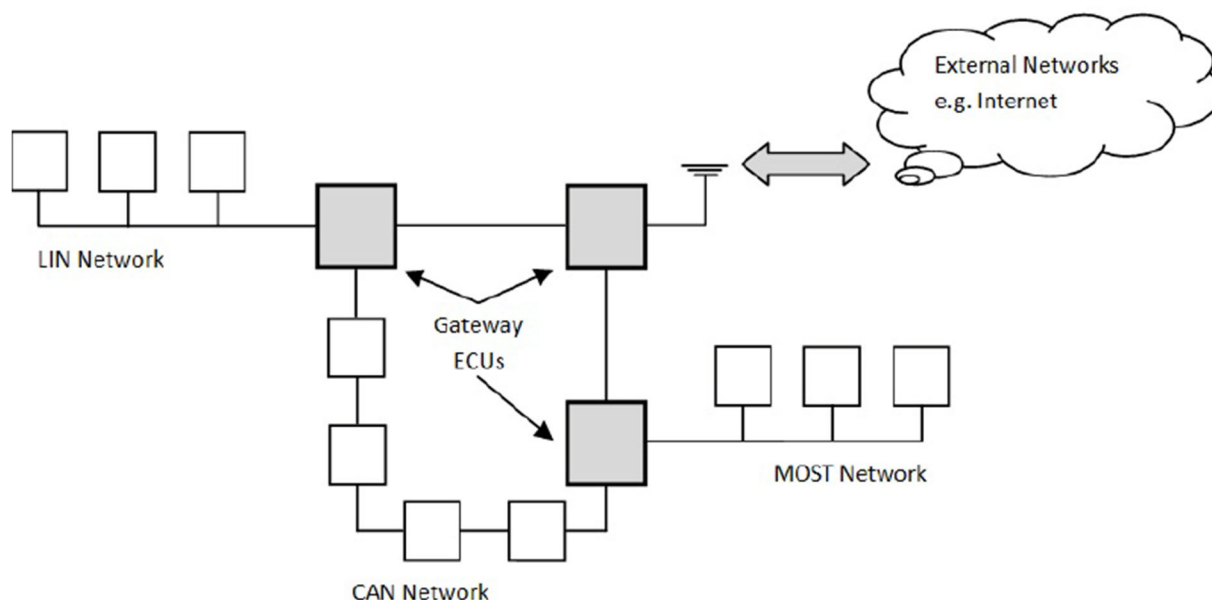


Figure 2. In-vehicle Network Structure

Amirtahmasebi, Ex. 1019, Figure 2

146. As shown in Figure 2 presented above, a plurality of in-vehicle networks (buses) is present in the vehicle system and each may be separated from other networks in the vehicle via one or more gateway ECUs.

147. Amirtahmasebi further discloses in-vehicle network security solutions. For instance, an embedded information security system may include: “Tamper-

resistant software: In order to develop tamper-resistant software, there is a small trusted program embedded into a light-weight ECU within the vehicle. This is done by applying trusted computing techniques which combines both trusted software and hardware” and a “Integrated gatekeeper: A data security gatekeeper can be a connection point between the different existing networks (e.g. LIN, CAN, and MOST) within a vehicle.” (Amirtahmasebi, Ex. 1019, p. 40.)

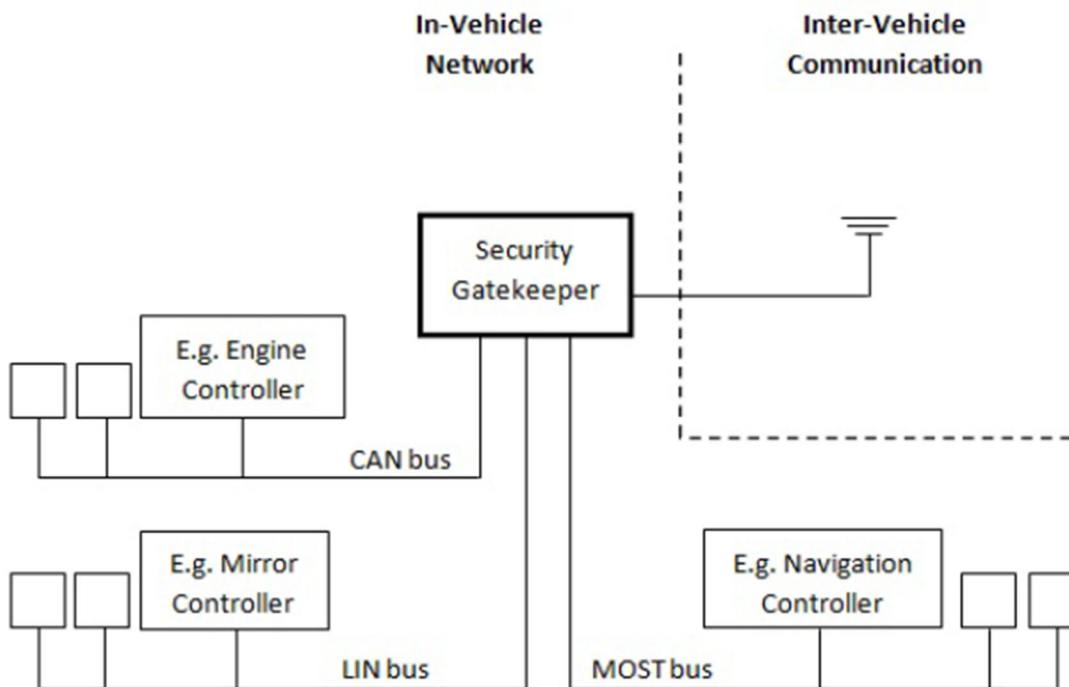


Figure 12. Integrated Data Security Gatekeeper

Amirtahmasebi, Ex. 1019, Figure 12

148. As shown in Figure 12 presented above, a security gatekeeper is connected between various vehicle buses for inspecting and managing the exchanged information passing between the buses. The security gatekeeper also

operates as a central gateway connecting the in-vehicle network to the inter-vehicle communication network.

149. The vehicle security solutions further include an Intrusion Detection System (IDS) for detecting intrusions “by comparing incoming/outgoing messages with predefined patterns, a number of patterns in vehicular networks must be defined as malicious behavior.” (Amirtahmasebi, Ex. 1019, p. 41.)

150. The vehicle security solutions further include digital signature and certificates that perform authentications and encryptions to the data transmissions within the in-vehicle network. (Amirtahmasebi, Ex. 1019, pp. 43-45.)

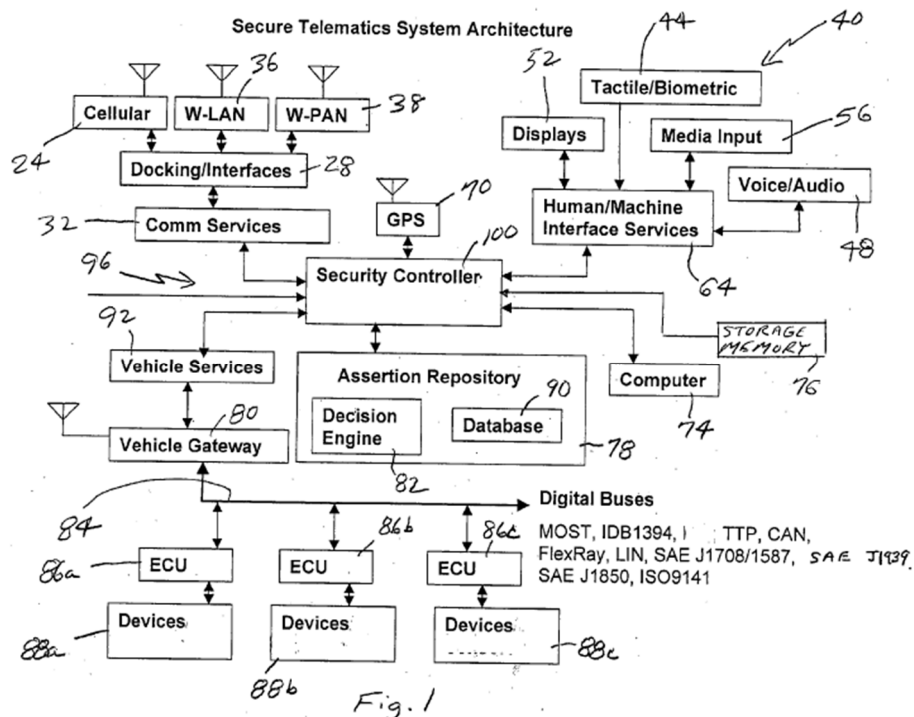
151. The vehicle security solutions further include utilizing a firewall gateway for monitoring data communication and honeypots for detecting attackers. (Amirtahmasebi, Ex. 1019, pp. 45-47.)

B. US 2004/0185842 A1 (“Spaur” Ex. 1020)

152. Spaur is a U.S. patent publication that was filed on January 28, 2004, and published on September 23, 2004. (Spaur, Ex. 1020, Cover.) I understand that Spaur is prior art to all claims of the ’100 Patent under pre-AIA 35 U.S.C. § 102(b) because it was published more than one year before the earliest claimed priority date of the ’100 Patent.

153. Spaur discloses “[a] telematics system that includes a security controller[.]” (Spaur, Ex. 1020, Abstract, Figure 1.) Various communication

subsystems are provided. For instance, the “communication subsystems might include cellular telephones together with their associated interfaces, and other apparatuses for enabling communications with one or more appropriate wireless technologies, such as a wireless LAN (Local Area Network).” (Spaur, Ex. 1020, [0009].)

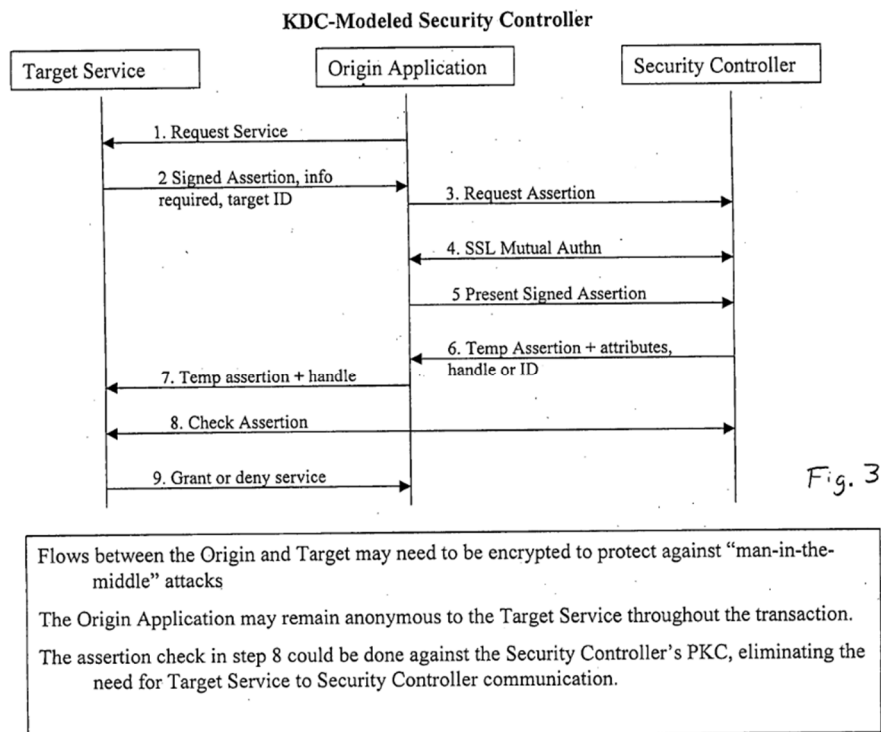


Spaur, Ex. 1020, Figure 1

154. As shown in Figure 1 above, a security controller operates as a central connection device with various subsystems including a wireless PAN 38 which enables wireless communication. Spaur further discloses “[i]n communication with the vehicle gateway 80 is a vehicle services module 92. . . . The functions of the vehicle services module 92 include supporting secure communications on one or

more vehicle or telematics buses 84, contributing to the enablement of intra-vehicle wireless communications (e.g. PAN, such as Bluetooth)[.]” (Spaur, Ex. 1020, [0035].) Thus, the vehicle system may be wirelessly connected to a user device (e.g., a cellphone) via a wireless connection.

155. Spaur further discloses a security controller that performs security measures such as encryptions to protect against “man-in-the-middle” attacks. (Spaur, Ex. 1020, Figure 3.)



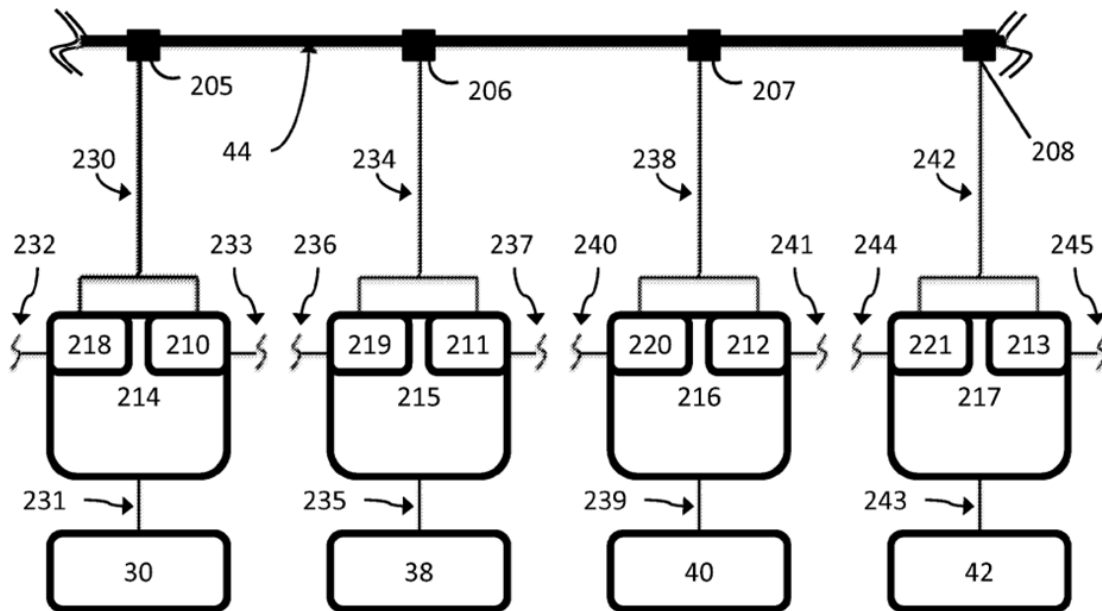
Spaur, Ex. 1020, Figure 3

C. US 8,788,731 B2 (“Peirce” Ex. 1021)

156. Peirce is a U.S. Patent that was filed on July 30, 2012 and was first published on January 30, 2014. (Peirce, Ex. 1021, Cover.) I understand that Peirce is prior art to all the claims of the ’100 Patent under pre-AIA 35 U.S.C. § 102(e).

157. Peirce is directed to “[a] message filtering system for a communications system in a vehicle enabling communication between various systems and subsystems via a vehicle bus.” (Peirce, Ex. 1021, Abstract.)

158. Peirce discloses that its filtering system includes “a plurality of transmit filters 210, 211, 212, 213 [and] a plurality of receive filters 218, 219, 220, 221” each of which “are coupled to each of the ECUs” 214, 215, 216, 217. (Peirce, Ex. 1021, 6:65-7:5.) Peirce discloses that the filtering system also includes “a plurality of VSMs 38, 40, 42.” (Peirce, Ex. 1021, 6:63-7:2.)



Peirce, Ex. 1021, Figure 2

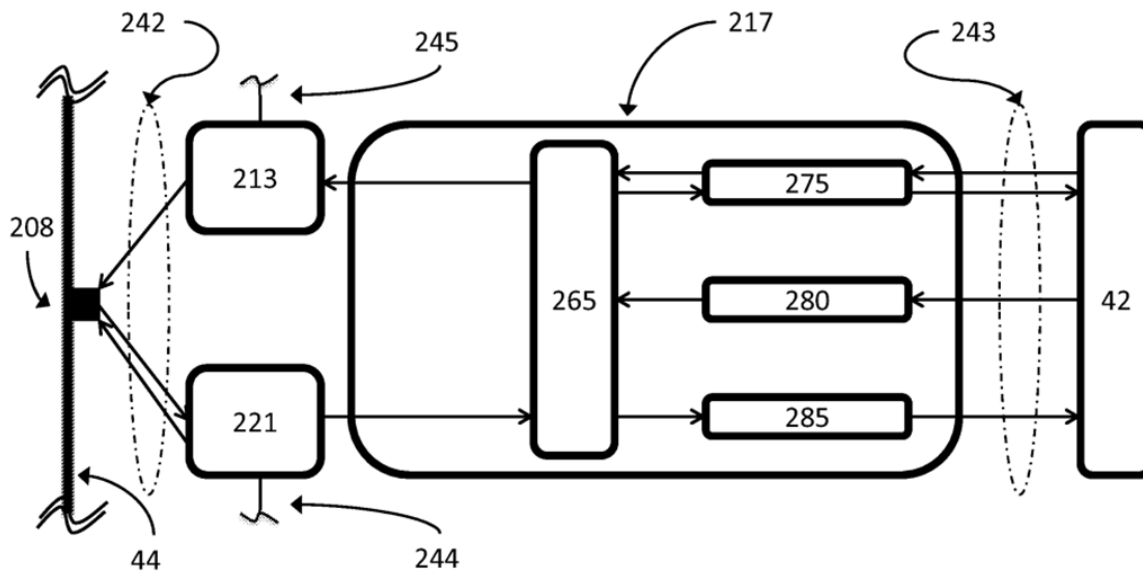
159. Peirce further discloses that “[t]he transmit filters 210, 211, 212, 213, and/or the receive filters 218, 219, 220, 221 may be subject to a filter policy (e.g., one or more rules)” and “[t]he filter policy may include executable instructions for implementing logical functions which may include validating or verifying the authenticity of the message contents.” (Peirce, Ex. 1021, 7:38-43.) Peirce explains that these executable instructions include firmware/software structures used to validate message content (e.g., source ID, destination ID, message ID). (Peirce, Ex. 1021, 7:43-54.)

160. Peirce discloses that the filter policy “minimize[s] or eliminate[s] the transmission of corrupt messages over the bus 44” (Peirce, Ex. 1021, 7:60-61) and

“pertain[s] to validating or verifying the authenticity of [] message contents.” (Peirce, Ex. 1021, 8:41-43.) Peirce explains that the receive filters 218-221 “store known message IDs in accordance with the filter policy” and “then compare the message ID of an incoming message with the known message IDs . . . to validate whether the incoming message should be accepted” by vehicle system modules (VSMs). (Peirce, Ex. 1021, 8:45-50.) If the message IDs do not match, the receive filters will terminate the transmission of the incoming message so that it “never reach[es] the VSM 42.” (Peirce, Ex. 1021, 8:53-55.)

161. Similarly, Peirce discloses that the transmit filter 210-213 validate/verify “the message contents of outgoing messages (i.e., those being sent to the bus 44).” (Peirce, Ex. 1021, 8:56-58.) Peirce explains that the transmit filter 210-213 stores “the source ID of the VSM 42 (and/or the ECU 217) in accordance with the filter policy” (Peirce, Ex. 1021, 8:58-60) and “compare[s] the source ID of an outgoing message” against it, terminating non-matching messages so they “never reach[] the bus 44.” (Peirce, Ex. 1021, 8:62-9:3.)

162. Peirce discloses that “both the transmit filter [210, 211, 212] 213 and the receive filter [218, 219, 220] 221 are shown physically and/or logically isolated from the ECU [or VSM] 217 and/or the protocol controller 265—thus, mitigating the possibility of corruption of both.” (Peirce, Ex. 1021, 9:29-35.)



Peirce, Ex. 1021, Figure 5

D. Bosch Automotive Handbook 6th Edition (“Bosch” Ex. 1050)

163. Bosch is a reference handbook that is “all about automotive engineering in a pocketbook.” (Bosch, Ex. 1050, Back Cover¹⁸.) Bosch describes the common structure of an automotive electronic control unit (ECU) as of 2004, including a “[m]icroprocessor” and “memory.” (Bosch, Ex. 1050, pp. 94, 96.) Bosch explains that:

The microprocessor represents the integration of a computers central processing unit on a single chip. Microprocessor design seeks to avoid individualization in the face of large-scale integration, and the units can

¹⁸ Bosch, Ex. 1050 is a true and accurate copy of a book that I understand was published by Robert Bosch GmbH in October 2004.

be programmed to meet the varied requirements associated with specific operation conditions.

(Bosch, Ex. 1050, p. 94.)

164. Intentionally left blank.

VIII. Grounds for Challenge

A. Ground 1 – The Combination of Amirtahmasebi and Bosch teaches all of the limitations of claims 1-24

3. Independent Claim 1

165. I have used the following break-up for each of the limitations of claim 1, as shown in the chart below:

U.S. Patent No. 9,173,100
1[pre]. A vehicle, comprising:
[1a] 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
[1c] a microprocessor executable network controller operable to (i) detect 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

[1e] (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 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,

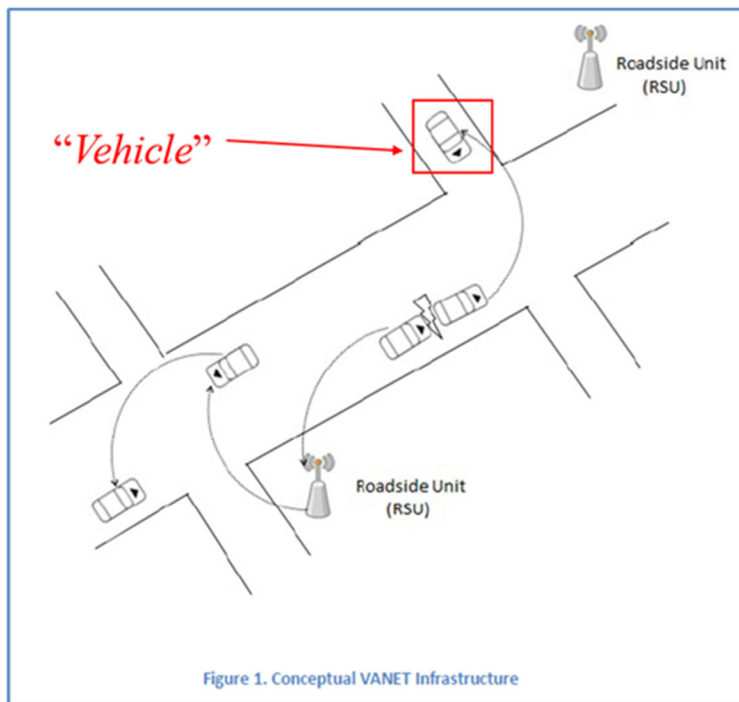
[1f] wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security 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.

1[pre]. A vehicle, comprising:

166. Amirtahmasebi is titled “Vehicular Networks – Security , Vulnerabilities and Countermeasures” and is stated as being a project related to the “robustness of in-vehicle networks with respect to safety and security malfunctions.” (Amirtahmasebi, Ex. 1019, p. 12.)

167. Figure 1 below, is described as representing a “conceptual model for Vehicular Ad hoc Networks (VANETs).” (Amirtahmasebi, Ex. 1019, p. 13, Figure 1.) Amirtahmasebi details the “security vulnerabilities in vehicular networks and their countermeasures, both in inter-vehicle (VANET) and in-vehicle networks, in order to secure the vehicular networks.” (Amirtahmasebi, Ex. 1019, p. 7.) Amirtahmasebi is therefore focused on disclosing security concepts for “[a] vehicle.”



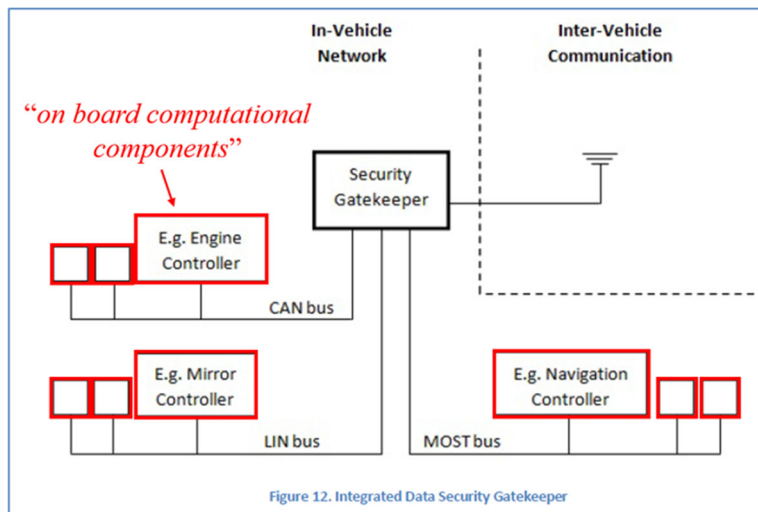
Amirtahmasebi, Ex. 1019, Figure 1 (Annotated)

168. The combination of Amirtahmasebi and Bosch teaches a “*vehicle*.”

[1a] a plurality of on board computational components;

169. Amirtahmasebi discloses “security vulnerabilities in vehicular networks and their countermeasures, both in inter-vehicle (VANET) and in-vehicle networks, in order to secure the vehicular networks.” (Amirtahmasebi, Ex. 1019, p. 7.) Amirtahmasebi discloses that “[i]n-vehicle networks . . . are a combination of Electronic Control Units (ECU), sensors and actuators.” (Amirtahmasebi, Ex. 1019, p. 11.)

170. Amirtahmasebi further discloses that modern vehicles include in-vehicle networks with a plurality of ECUs as illustrated in by white boxes of the network structure shown in Figure 12. (Amirtahmasebi, Ex. 1019, p. 24, 40.)



Amirtahmasebi, Ex. 1019, Figure 12 (Annotated)

171. Amirtahmasebi describes these ECUs as generally being capable of classification into five different categories “based on the criticality of their tasks and the effect of failure on passengers’ safety,” discussing (1) powertrain ECUs, (2) vehicle safety ECUs such as ABS (anti-locking braking system), collision avoidance systems, airbags, and adaptive cruise control, (3) comfort ECUs such as temperature control, (4) infotainment ECUs such as those in charge of navigation systems and audio streams, and (5) telematics ECUs that provide networked software applications to the vehicle. (Amirtahmasebi, Ex. 1019, pp. 24-25.) (citation omitted.)

172. Amirtahmasebi concludes that “critical ECUs, i.e., powertrain ECUs” need to be secured from cyber attacks. (Amirtahmasebi, Ex. 1019, p. 55.) This solution requires the development of “new gateway ECUs” which would need to include “more computational power and resources” than current “gateway ECUs.” (Amirtahmasebi, Ex. 1019, p. 55.)

173. Amirtahmasebi also discloses “VANETs consist of a number of On-Board Units (OBU) which are located inside the vehicles....” (Amirtahmasebi, Ex. 1019, p. 13). A PHOSITA would have understood these OBUs could be designed to be included in a given ECU or could be separate from the ECUs.

174. A PHOSITA would have understood the disclosed ECUs and OBUs with the described functions constitute “*a plurality of on board computational components.*”

175. The combination of Amirtahmasebi and Bosch teaches limitation [1a].

[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

176. Again, Amirtahmasebi is directed to various methods and techniques for securing vehicular networks both “inter-vehicle” (between vehicles or between a vehicle and external device) and “in-vehicle” networks. Given inter-vehicle and in-vehicle networks may be infiltrated and are vulnerable differently, Amirtahmasebi details each separately.

In this work, we have done a survey of existing approaches to solve the problems associated with vehicular networks. We discuss security vulnerabilities in vehicular networks and their countermeasures, both in inter-vehicle (VANET) and in-vehicle networks, in order to secure the vehicular networks. In our work, we found that vehicular networks in general have several vulnerabilities and are exposed to different

cyber attacks. There are a number of suggested countermeasures which will provide short-term security for vehicular networks. Cyber attacks in in-vehicle networks can be a threat to the vehicle and its passengers; therefore, security issues must be carefully addressed in in-vehicle networks. We believe that there will be a need for a new infrastructure to deal with current vulnerabilities in in-vehicle networks. By doing so, current and future advancements in vehicular networks can be applied with less security issues and risks which will culminate in secure and reliable vehicular networks.

(Amirtahmasebi, Ex. 1019, p. 7.)

177. With regard to inter-vehicle networks, Amirtahmasebi explains how Vehicular Ad Hoc Networks (VANETs) are known and deployed for providing network communication between vehicles (vehicle-to-vehicle) and between various road-side units (vehicle-to-infrastructure). The VANET system includes a number of on-board units (OBUs) which are located within a vehicle and connect to road-side units (RSUs) located external to the vehicle. The OBU is a wireless gateway which connects the OBUs and RBUs.

Vehicular Ad hoc Networks (VANETs) are a subcategory of mobile ad hoc networks which are recently being discussed in great extent. The main idea behind VANET is providing communication among vehicles and also among vehicles and a number of fixed equipment located on the road. Several research projects have focused on this interesting and useful area in order to implement it in the best possible way.

The main intention with VANET's is to enhance vehicles' passengers' safety and comfort by distributing traffic, road and weather conditions among nearby vehicles. Among its applications collision warnings, road sign alarms and automatic toll/parking payment can be mentioned.

VANETs consist of a number of On-Board Units (OBU) which are located inside the vehicles and a number of Road-Side Units (RSU) which form the infrastructure of the network. OBU is a wireless gateway which can be connected to other OBUs and RSUs. Each vehicle equipped with the OBU can become a part of the network and will be able to send, relay and receive messages throughout the network. Due to its ad hoc nature, there won't be any centralized servers and vehicles are in charge of network management themselves. Communication in VANET is divided into two different categories:

- Vehicle-to-Vehicle (V2V) Communication, were [sic] the nearby vehicles will communicate traffic and road conditions to one another
- Vehicle-to-Infrastructure (V2I) Communication, were [sic] vehicles communicate their gathered information to the nearest RSU in order to distribute the information faster and more effectively.

(Amirtahmasebi, Ex. 1019, p. 13.)

178. Amirtahmasebi explains that modern vehicles employ multiple distinct in-vehicle networks because “in order to deliver different messages and information on-time and due to different demands and requirements of ECUs,” manufacturers

create different network types. (Amirtahmasebi, Ex. 1019, p. 24.) The networks disclosed include LIN, MOST, CAN, and FlexRay, each serving different classes of ECUs with different real-time or bandwidth requirements. (Amirtahmasebi, Ex. 1019, pp. 25-26.)

179. Amirtahmasebi explains that historically internal networks (*i.e.*, in-vehicle networks like CAN) were intended to work in isolation. As these internal networks have begun to be interconnected to external networks for applications (e.g., firmware over the air (FOTA) updates), the internal networks have become susceptible to potential infiltration, for example by external attacks, including viruses embedded within the firmware updates being sent.

Since in-vehicle networks were originally designed to work in isolation and didn't need to be connected to external networks, security issues were not addressed completely. By connecting in-vehicle networks to external networks without securing them, attackers and malicious users will be able to access the network and perform unauthorized actions. These actions may cause an ECU to stop functioning and lead to safety critical events such as accidents on the road.

(Amirtahmasebi, Ex. 1019, p. 28.)

Apart from the mentioned threats and vulnerabilities, a combination of these attacks can also be built and launched against the in-vehicle network in order to form more sophisticated attacks. The concept is called vehicle virus [28] and can be built into a piece of code and be

sent to the vehicle's network through a FOTA process. By a combination of the mentioned building blocks, the virus can become more intelligent and may be able to cause considerable damage to the vehicle's network or extract invaluable information. Therefore, the mentioned security properties must be considered completely in order to prevent such actions to take place.

(Amirtahmasebi, Ex. 1019, p. 37-38.)

180. To protect the vehicle Amirtahmasebi teaches how a security boundary can be established to ultimately protect the internal network from external, untrusted communications. These external, untrusted communications could come from inter-vehicle networks (e.g., communications sent via VANET networks) or in-vehicle network communication with external systems (e.g., FOTA updates from an external computing system).

Logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications (e.g. C2C cooperative driving system). Likewise, an internal attacker can benefit from available on-board interfaces such as telematics or software update interfaces.

(Amirtahmasebi, Ex. 1019, p. 32) (citation omitted.)

181. Amirtahmasebi teaches external communications may include FOTA communications, software update interfaces, or connections to on-board interfaces

like telematics. (Amirtahmasebi, Ex. 1019, p. 32, 51-52.) Or a PHOSITA would have understood vehicle networks could also be susceptible from external communications sent from other external devices like remote key FOBs, wireless tire pressure monitoring systems, in-vehicle communication connections (e.g., USB or Bluetooth connections), or physical connections using the On-Board Diagnostics (OBD-II) connector common within vehicles. (Amirtahmasebi, Ex. 1019, 35-38.)

182. Amirtahmasebi teaches a PHOSITA how a logical security boundary could be established that separates specified computational components from external, untrusted communications. A PHOSITA would understand a “*security mechanism*” (e.g., firewall mechanism) may form a “*perimeter network*” to control and monitor the flow of data from external sources to protect and prevent unauthorized access to the computational components. For instance, a PHOSITA would have understood the “*perimeter network*” could be logically formed to separate the vehicle ECUs from direct communication from external, untrusted sources. The “*security mechanism*” would form the logical “*perimeter network*” and ensure “*security measures*” control and monitor the flow of data from external sources. But a PHOSITA would understand the “*perimeter network*” could be extended to include devices other than the vehicle ECUs. For instance, a driver’s cellular phone could be included as a computational component that is separated from communications received from external sources.

183. For instance, a “*perimeter network*” could be formed to isolate vehicle ECUs from attacks by externally connected devices (either brought into the vehicle or remote), or it could be formed to isolate (*i.e.*, protect) one group of in-vehicle ECUs from any combination of other internal or external ECUs and devices. Because it creates this logical network, the Amirtahmasebi system, like the claimed system can dynamically isolate devices within the perimeter network when and if they exhibit malicious behavior.

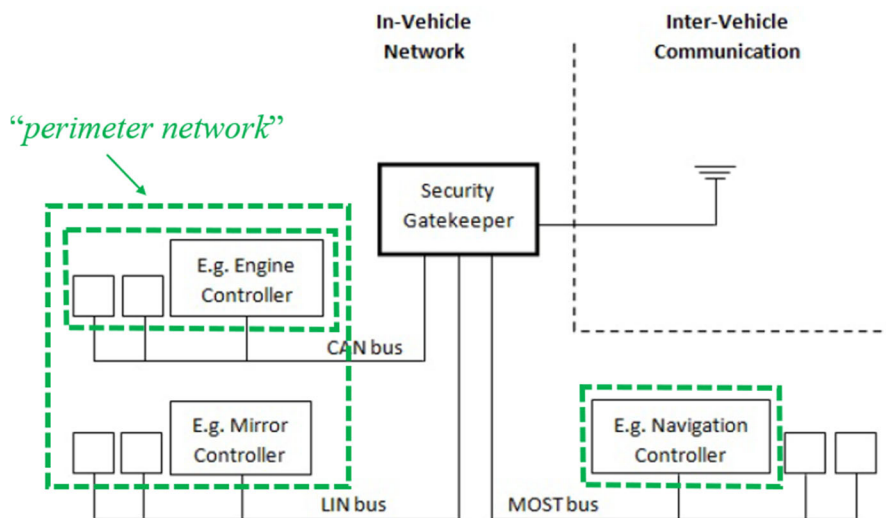


Figure 12. Integrated Data Security Gatekeeper

Amirtahmasebi, Ex. 1019, Figure 12 (Annotated)

184. Amirtahmasebi details numerous security “techniques and methods” (*i.e.*, “Security Methods” or “Security Solutions”) which may be used to establish the “*perimeter network*” to prevent attacks against the plurality of ECUs residing on different networks within the vehicle (*e.g.*, the CAN, LIN, and MOST bus) and to ensure such security requirements are maintained. For instance, Amirtahmasebi

discloses the use of: (1) digital signatures and certificates; (2) digital signatures without certificates; (3) digital signatures with certificates; (4) tamper proof devices; (7) data correlation techniques; and (8) IEEE 1609.2 wireless access in vehicular environments standard. (Amirtahmasebi, Ex. 1019, p. 19-23.)

185. Amirtahmasebi also teaches various “security solutions” (i.e., “Security Solutions”) used to protect from malicious external communications. The “Security Solutions” are disclosed as including “hardware” solutions which may be “different devices such as ECUs, sensors, actuators, gateways, etc.” The “Security Solutions” may also include “software” solutions like “ECU firmware which operates and controls ECU behavior.” Or the “Security Solutions” may be related to the “communication channel” which it identifies is the “basis for different communication types including Vehicle-to-vehicle, vehicle to-infrastructure and in-vehicle.” (Amirtahmasebi, Ex. 1019, p. 39.)

186. Amirtahmasebi then describes in detail the “Security Solutions” known in the automotive industry relating to “physical security”, “software security”, “embedded information security”, “intrusion detection system,” “digital signatures and certificates,” “firewall gateways,” “honeypots,” “FlexRay Bus Guardian” systems, or “Vehicular Security Architectures” detailed by Amirtahmasebi. (Amirtahmasebi, Ex. 1019, p. 39-50.)

187. A PHOSITA would have understood each disclosed “Security Methods” or “Security Solutions” as being a “*security mechanism*” that could be used to enforce a “*security measure*.”

188. For instance, Amirtahmasebi discloses one software solution as being the implementation and use of digital signatures with certificates issued by a trusted Certificate Authority (CA) (*i.e.*, a “*security mechanism*”).

2.4.1.2 Digital Signatures with Certificates

Using certificates provided by a trusted certificate authority provides a system in which only messages from trusted nodes that have a valid certificate are accepted. Therefore, in such a system, the certificate authority will be able to trace back all the signed messages to their real sender's identity based on the link between issued certificate and the key used to encrypt the message.

A public key infrastructure is necessary to implement the concept of certificates issued by an authority. Before sending a message, the sender signs the message with its private key and provides the receiver with its CA's certificate. Before signing the message there is a time stamp concatenated with the message to guarantee message freshness.

Upon receiving, the receiver will decrypt the message (verify the sender's signature) using its certified public key. Sender's public key is verified by the receiver with respect to its certificate [14].

Associating digital signatures with certificates basically targets excluding external attackers such as a road-side attacker using his

laptop computer to launch an attack scenario. Since only valid VANET nodes possess the certificates, other external nodes will not be able to send messages within the corresponding domain. Moreover there exists the possibility to identify and remove the malicious behaving or defective nodes by revoking their certificates [7].

One advantage of using public key infrastructure is the possibility of revoking certificates. By revoking the certificates of an attacker, misbehaving or malfunctioning nodes won't be able to use their keys and thus harm the vehicular network anymore [14].

The basic commonly used mechanism to achieve this concept is implementing CRLs (Certificate Revocation Lists) within the PKI system. CRLs containing the list of revoked certificates or keys are distributed among network nodes by the certificate authority [15].

(Amirtahmasebi, Ex. 1019, pp. 20-21.)

In terms of digital signatures and certificates, two different areas will be discussed in vehicular networks. Recent development in remote software updates have led to the need for a new infrastructure to authenticate the parties which are allowed to generate and send new software patches to vehicles. On the other hand, ECUs within the in-vehicle network as well as the communication bus must be secured against manipulation and eavesdropping as well. In-vehicle protection can be provided by in-vehicle ECU certificates and digital certificates.

A) Digital Signatures and Certificates for Secure Software download

In order to implement digital signatures for secure software downloading to in-vehicle networks, the issuer of the software signs the program code and the control unit in the vehicle verifies it. [29] Suggests six steps from generating the code up to securely downloading it to the control unit. In the first step, the code will be generated and then passed to a trust center in the second step. In the third step, the code is signed by trust center's secret key, passed back and attached to the program object code. Afterwards, in the fourth step the code is stored in a database. The code can now be downloaded to the appropriate control unit. Finally, ECUs can verify the authenticity of downloaded software by using their public keys which are stored in the ECUs (step 6). Figure 13 shows the procedure in more detail.

(Amirtahmasebi, Ex. 1019, pp. 43-44.)

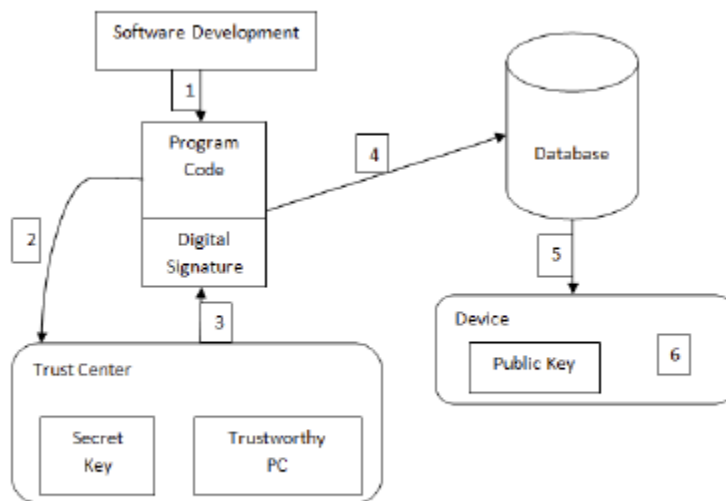


Figure 13. Secure Software Download

Amirtahmasebi, Ex. 1019, Figure 13

189. Amirtahmasebi teaches only messages from trusted nodes possessing valid certificates are accepted, and the CA can trace all signed messages back to their real sender through the link between the issued certificate and the encryption key. A PHOSITA would have understood this as identifying a certificate-based authentication system—a component that performs security-relevant validation and message integrity checks (*i.e.*, a “*security measure*”).

190. Amirtahmasebi explains that implementing this concept requires a Public Key Infrastructure (PKI). Before sending a message, the sender signs it with its private key and appends a timestamp to guarantee freshness, then provides the receiver with its CA-issued certificate. Upon receipt, the receiver verifies the sender’s signature using the certified public key and validates the certificate against the CA. A PHOSITA would have understood that these steps implement at least one cryptographic rules and checks applied by the PKI system to authenticate message sources and ensure integrity (“*security measure*”).

191. Additionally, Amirtahmasebi discloses that associating digital signatures with certificates excludes external attackers transmitting malicious communications to the vehicle (e.g., from roadside attackers in VANET systems). Moreover, PKI enables revocation of certificates for misbehaving or defective nodes, preventing them from using their keys to harm the network. This is achieved through Certificate Revocation Lists (CRLs) distributed by the CA. A PHOSITA

would have therefore understood that the PKI system implements at least one of authentication, integrity enforcement, and dynamic mitigation through certificate revocation (“*security measure*”).

192. Accordingly, a PHOSITA would have understood that Amirtahmasebi’s disclosure of PKI-based authentication (“*security mechanism*”) applies cryptographic “*security measures*” at the boundaries of vehicular communication domains (logical “*perimeter network*” boundary), ensuring that only authorized nodes exchange messages and enabling removal or exclusion of compromised nodes. These measures protect the integrity of communications among the plurality of ECUs and other on-board computational components (“*the plurality of on board computational components*”).

193. The PKI-based authentication solution (“*security mechanism*”) therefore enforces cryptographic rules, checks, authentication integrity enforcement (“*security measures*”) to form a logical “*perimeter network*” formed around one or more ECUs (“*the plurality of on board computational components*”), one or more networks, or the entire vehicle from each point where an external communication may be received. This would ensure that only authorized external communications would be permitted for transmission on the internal vehicle network.

194. Another “software security” solution Amirtahmasebi discloses is an “Intrusion Detection System” or “IDS” (“*security mechanism*”) that “can also be

employed to further enhance the communication and system security.” (Amirtahmasebi, Ex. 1019, p. 46.) Amirtahmasebi describes, “A central gateway equipped with an IDS system will be able to inspect and analyze the exchanged information to detect security-critical abnormalities.” (Amirtahmasebi, Ex. 1019, p. 46.) The IDS could be operable to perform security-relevant monitoring and analysis (“*security measure*”).

195. Amirtahmasebi specifically discusses that the IDS works by “comparing incoming/outgoing messages with predefined patterns” and that detection of deviations from these patterns can identify malicious behavior (*i.e.*, “*security measure*”). (Amirtahmasebi, Ex. 1019, p. 41.) Specifically with attention to the CAN bus, changes in patterns in (1) message frequency and (3) other characteristics such as “voltage amplitudes and their stability, the shape of clock edges, propagation delays, signal attenuation” etc. would allow a central gateway to detect communication misbehavior. (Amirtahmasebi, Ex. 1019, p. 41.) Therefore, a PHOSITA would have understood that the IDS (“*security mechanism*”) is (or implements) at least one “*security measure*”—the rules, checks, and analytic techniques applied by the security mechanism (the IDS-enabled gateway)—to detect and respond to attacks or abnormal message activity.

196. Additionally, Amirtahmasebi discloses implementation of an IDS functionality into an ECU itself, allowing the ECU to detect when an attacker is

sending a malicious command using the ECU's legitimate ID, and to mitigate the threat. (Amirtahmasebi, Ex. 1019, p. 41.) A PHOSITA would have therefore understood that the IDS implements at least one "*security measure*"—the rules, checks, and analytic techniques applied by the security mechanism (the IDS-enabled ECU)—to detect and respond to attacks or abnormal message activity.

197. Accordingly, the IDS solution ("*security mechanism*") to enforce rules, checks, and analytic techniques ("*security measure*") to form a logical "*perimeter network*" around one or more ECUs ("*the plurality of on board computational components*"), one or more networks, or the entire vehicle from each point where an external communication may be received. This would ensure that only authorized external communications would be permitted for transmission on the internal vehicle network.

198. Amirtahmasebi further discloses the implementation of "a firewall mechanism within the network gateways." (Amirtahmasebi, Ex. 1019, p. 45.) The "firewall mechanism" would also be understood as being a "*first security mechanism*."

199. Amirtahmasebi discloses gateway ECUs that may implement the "firewall mechanism" within the gateway, configured to use "message authentication codes (MAC) or digital signatures" to authenticate and authorize

messages sent between ECUs (i.e., “*security measure*”). (Amirtahmasebi, Ex. 1019, p. 45-46.)

200. Amirtahmasebi also discloses 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.” (Amirtahmasebi, Ex. 1019, p. 46.) By implementing these firewalls, Amirtahmasebi 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.” (Amirtahmasebi, Ex. 1019, p. 46.)

201. The “firewall” (i.e., “*first security mechanism*”) could also operate to enforce MAC/digital signatures or rules (“*security measure*”) to form a logical “*perimeter network*” around one or more ECUs (“*the plurality of on board computational components*”), one or more networks, or the entire vehicle from each point where an external communication may be received. This would ensure that only authorized external communications would be permitted for transmission on the internal vehicle network.

202. A PHOSITA would have therefore understood each of the disclosed “Security Methods” and/or “Security Solutions” would be the recited “*security mechanism*” that could be used to enforce the various “*security measures*” (e.g., authentication or verification rules, or digital signatures and keys) disclosed. A PHOSITA would have also understood each of the disclosed “*security mechanisms*”

may be “*a first security mechanism.*” Further, each “*security mechanism*” would also be understood by a PHOSITA as operating to form a logical “*perimeter network*” around one or more ECUs (“*the plurality of on board computational components*”), one or more networks, or the entire vehicle from malicious communications -.

203. Intentionally left blank.

[1c] a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,

204. Amirtahmasebi discloses the internal vehicular networks (e.g., CAN, LIN, and MOST bus networks) could be “connected by gateways in order to be able to communicate with each other as well.” (Amirtahmasebi, Ex. 1019, p. 24.) Amirtahmasebi also identifies these gateways—also described as “Integrated gatekeepers”—as the intermediary ECUs located between the networks, depicted as grey boxes in Figure 2.

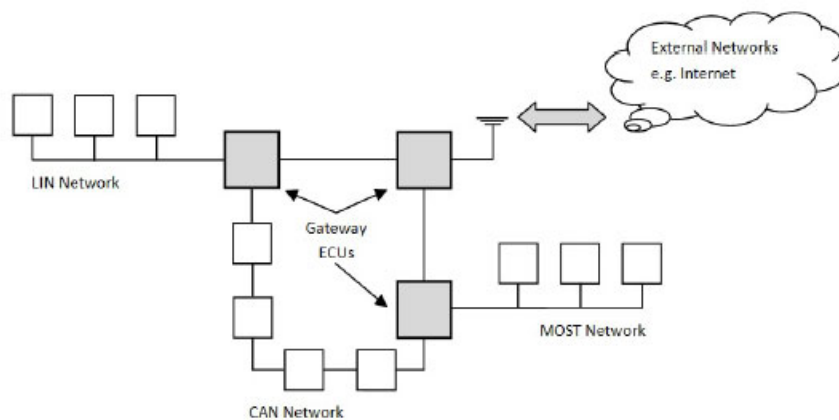


Figure 2. In-vehicle Network Structure

Amirtahmasebi, Ex. 1019, Figure 2

205. Amirtahmasebi discloses how vehicles could include one or more gateway or security gatekeepers¹⁹. These “security gatekeepers” are intended to protect each of the in-vehicle buses (e.g., LIN, CAN, MOST, FlexRay, etc.) and their corresponding ECUs individually or in combination from external communications. (see Amirtahmasebi, Ex. 1019, p. 29-48.) For instance, Figure 12 illustrates a single gatekeeper between the external “inter-vehicle communication” and each of the various bus networks.

¹⁹ Amirtahmasebi uses the terms “gateway,” “gatekeeper,” and “integrated gatekeeper” interchangeably when describing the ECUs that interconnect separate in-vehicle networks. For example, Amirtahmasebi explains that in-vehicle networks “are connected by gateways in order to be able to communicate with each other as well” and depicts these components—shown as gray boxes between the networks in Figure 2—as the intermediary devices positioned between distinct buses. (see Amirtahmasebi, Ex. 1019, pp. 24, 40).

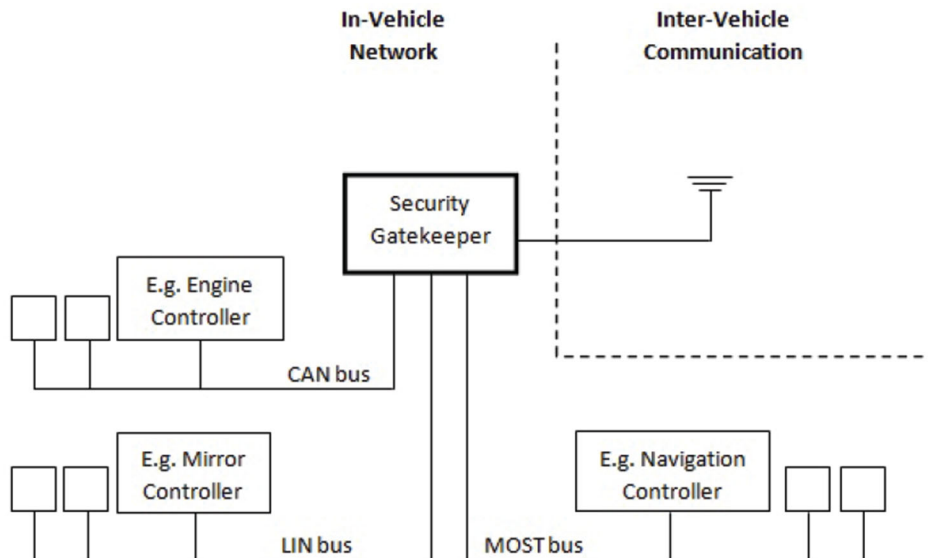


Figure 12. Integrated Data Security Gatekeeper

Amirtahmasebi, Ex. 1019, Figure 12

206. While only one gatekeeper is shown, Amirtahmasebi explains more may be added to protect individual ECUs. (Amirtahmasebi, Ex. 1019, p. 25, Figure 2).

207. Amirtahmasebi details these gatekeepers as one form of “embedded information security” that could be used to implement the various “software security” it discloses. (Amirtahmasebi, Ex. 1019, p. 40-41.)

208. For instance, Amirtahmasebi discloses the gateway ECUs may implement the “firewall mechanism gateway” I discussed above in 1[b].

Another solution to further securing in-vehicle communication is to implement a *firewall mechanism within network gateways*.

(Amirtahmasebi, Ex. 1019, p. 45.)

209. Amirtahmasebi discloses gateways including a “firewall mechanism” could be configured to use “message authentication codes (MAC) or digital signatures” to authenticate and authorize messages sent between ECUs. (Amirtahmasebi, Ex. 1019, p. 45-46.)

210. Amirtahmasebi discloses 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.” (Amirtahmasebi, Ex. 1019, p. 46.) By implementing these firewalls, Amirtahmasebi discloses “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.” (Amirtahmasebi, Ex. 1019, p. 46.)

211. Amirtahmasebi’s discloses that the firewall within the network gateways can regulate cross-network message flow 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.

For instance, 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 [11].

(Amirtahmasebi, Ex. 1019, p. 46.)

212. A PHOSITA would have understood that these detection functions run on a gateway ECU’s microprocessor, meaning each “gateway” or “security

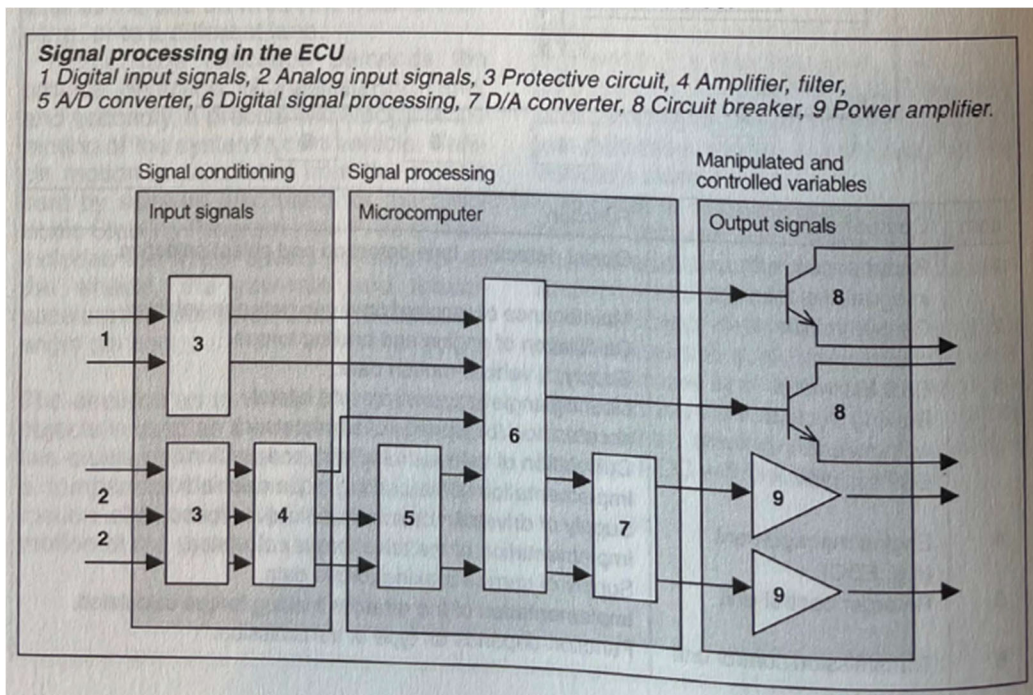
gatekeeper” would include a microprocessor-executable network controller that executes the firewall/IDS algorithms. These algorithms continuously monitor network traffic for abnormal or unauthorized behavior.

213. For instance, the Bosch Handbook teaches how a PHOSITA would have understood that an automotive ECU would include a microcomputer which would include a “*microprocessor*” designed to receive input signals and execute the arithmetic-logic unit to perform specified operations. A PHOSITA would have understood the “*microprocessor*” disclosed by the Bosch Handbook would functionally operate and be structurally the same as the gateway ECU disclosed by Amirtahmasebi.

Electronic control unit (ECU)

ECUs developed for use in motor vehicles all have a similar design. Their structure can be subdivided in the conditioning of input signals, the logic processing of these signals in the microcomputer, and the output of logic and power levels as regulation or control signals....

(Bosch, Ex. 1050, p. 1065.)

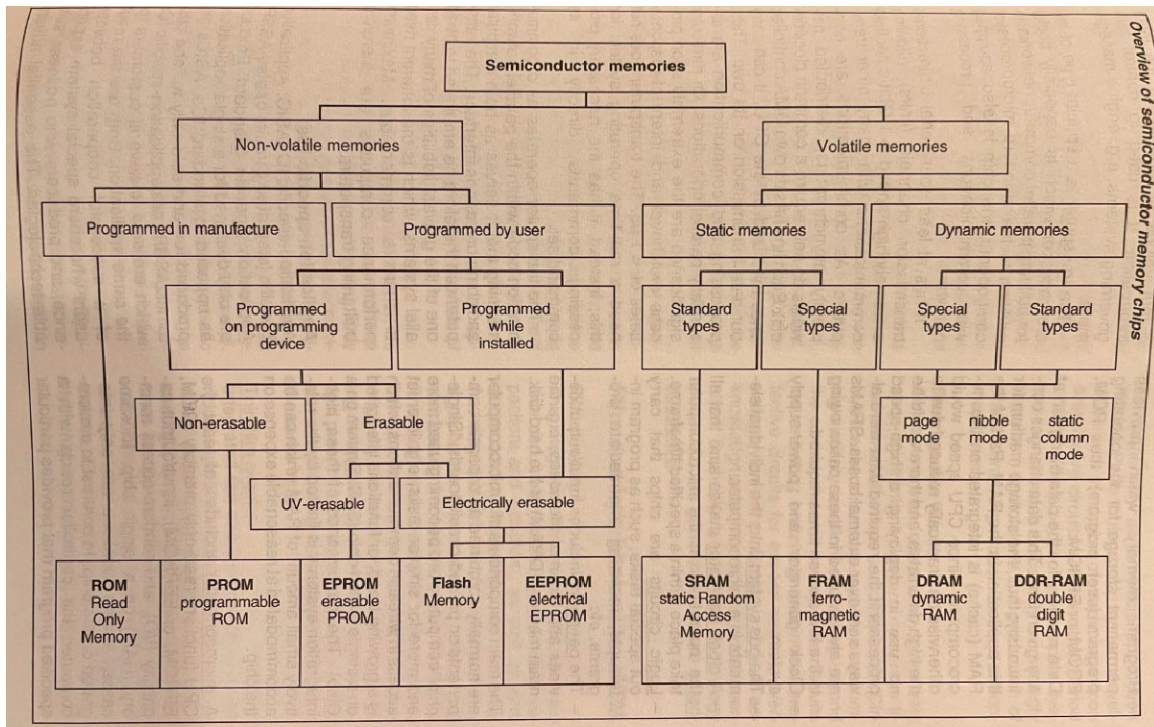


Bosch, Ex. 1050, p. 1064

The microprocessor represents the integration of a computer's central processing unit on a single chip.... A microprocessor cannot operate by itself: it always acts as part of a microcomputer.

A microcomputer consists of: Microprocessor serving as CPU (central processing unit). The microprocessor contains the controller and the arithmetic-logic unit. The arithmetic and logic unit performs the operations indicated by its name, while the controller ensures implementation of the commands stored in the program memory

(Bosch, Ex. 1050, p. 94-96) (emphasis omitted.)



Bosch, Ex. 1050, p. 95

214. Amirtahmasebi describes that gateway ECUs (“*microprocessor*”) may be designed and programmed to execute a “firewall mechanism” (“*first security mechanism*”) because it was understood an attacker may inject “malicious code” into an ECU, causing that ECU to send “malformed or invalid frames with wrong intervals on the bus.” (Amirtahmasebi, Ex. 1019, p. 33.) As explained in section [1b], Amirtahmasebi teaches that such malformed or malicious frames can be detected by the firewall and/or IDS running on the gateway.

215. Accordingly, a PHOSITA would have understood that the gateway’s (or “security gatekeeper’s”) microprocessor executes the network-control logic required to inspect and manage message traffic (“*a microprocessor executable*

network controller”), and that these microprocessor-executed routines detect unauthorized or malicious data attempting to traverse the network boundary—i.e., “*detecting 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

216. Amirtahmasebi discloses that “vehicle 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.” (Amirtahmasebi, Ex. 1019, p. 39) (citation omitted.) Amirtahmasebi proceeds to describe such a vehicle network design. A PHOSITA would have understood this system supports isolating a compromised ECU from those not affected by the compromise.

217. Indeed, Amirtahmasebi even discusses three types of vehicle security architecture that could be implemented to help protect the vehicle ECUs from malicious transmissions from external networks: a central, distributed, and semi-central security architecture. (Amirtahmasebi, Ex. 1019, p. 48-50.) A “central security architecture” includes “a central security module responsible for security operations of all internal and external ECUs and devices.” (Amirtahmasebi, Ex.

1019, p. 48.) A “distributed security architecture” is one where “all ECUs and devices take part in shaping the overall security functionality.” (Amirtahmasebi, Ex. 1019, p. 49.) A “semi-central security architecture” combines both, employing “a central security module along with some individual self-secured ECUs and devices such as critical sensors and actuators.” (Amirtahmasebi, Ex. 1019, p. 49.)

218. Amirtahmasebi therefore teaches a system architecture in which ECUs operate with a degree of functional independence—and that independence is what enables isolation of a compromised component.

219. If the “distributed computing architecture” was implemented, the security responsibilities would not be centralized to a single point of failure. Because the architecture is expressly designed so that a compromise in one ECU does not propagate to the rest of the network, a PHOSITA would have understood that such a system supports isolating any compromised ECU from unaffected components.

220. With regards to a firewall gateway, Amirtahmasebi explains: “restricting the access level of different types of networks to other parts of the bus system can be another approach to defining firewall rules.” (Amirtahmasebi, Ex. 1019, p. 46.) Amirtahmasebi further describes the firewall gateway isolation as “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.” (Amirtahmasebi, Ex. 1019, p. 46.)

221. A PHOSITA would have understood that these firewall determinations inherently decide whether an ECU whose messages fail authentication or authorization (“*a computational component affected by the instance of a breach of the security measure*”) should or can “*be isolated*” from ECUs whose messages remain valid (“*at least one on-board computational component not affected by or potentially affected by the instance of a breach*”). A PHOSITA would have even determined that “*computational components*” could include removable devices like a driver’s cellular phone that may be connected to the vehicle (e.g., using Bluetooth, USB or WiFi) temporally and could therefore be “*affected by the instance of a breach of the security measure.*”

222. With regards to the gateway-implemented IDS, Amirtahmasebi states: “[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.” (Amirtahmasebi, Ex. 1019, p. 46.) A PHOSITA would have understood that “deactivating” the ECU prevents that ECU from transmitting further messages onto the in-vehicle network. In the context of bus-based vehicular networks—where every ECU shares the same communication medium and any transmitted frame is received by all other ECUs—a deactivated ECU is one that can no longer place messages on the bus, respond to bus traffic, or participate in inter-ECU communication.

223. A PHOSITA would have understood this evaluation inherently requires the IDS to determine whether the misbehaving ECU can be isolated—i.e., whether isolating it is an appropriate and feasible countermeasure under the circumstances. For example, when the IDS detects only minor deviations, it may conclude that isolation is not required and instead issue a warning message; when the IDS detects malicious or dangerous traffic patterns, it may determine that the ECU can and should be isolated by deactivation.

224. Thus, a PHOSITA would have understood Amirtahmasebi's IDS performs the claimed determination—whether the ECU affected by the breach (“*a computational component affected by the instance of a breach of the security measure*”) should or can “*be isolated*”—because it may decide, based on the detected misbehavior, whether isolation (via deactivation) is an appropriate and viable measure to protect the remaining ECUs (“*at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure*”).

[1e] (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,

225. As discussed above in [1d] with regards to the firewall gateway, Amirtahmasebi discloses “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.” (Amirtahmasebi, Ex. 1019, p. 46.) A PHOSITA would have understood the firewall gateway of Amirtahmasebi “isolates” an invalid or unauthentic ECU (“*a computational component affected by the instance of a breach of the security measure*”) from unaffected components and ECUs on the in-vehicle bus on the in-vehicle subnetwork (“*at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure*”).

226. Furthermore, discussed above in [1d] with regards to the gateway-implementing IDS, Amirtahmasebi discloses that: “In 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.” (Amirtahmasebi, Ex. 1019, p. 46.) A PHOSITA

would have understood the IDS gateway of Amirtahmasebi “isolates” an invalid or unauthentic ECU (“*a computational component affected by the instance of a breach of the security measure*”) from unaffected components and ECUs on the in-vehicle bus on the in-vehicle subnetwork (“*at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure*”).

227. I also note that by isolating a misbehaving ECU from the unaffected ECUs, as described above by Amirtahmasebi, the system is also isolating the unaffected ECUs from the misbehaving ECU(s), thus Amirtahmasebi also described isolating “*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.*”

[1f] 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/or²⁰ gateway to enforce a security measure, (3) blocking communications to and from the computational component affected

²⁰ I understand that the term “and/or” is interpreted as “one or more.”

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:

228. I understand the term requires only “one or more” of the four options listed. My analysis below focuses on showing this limitation is met based on “the isolation” being satisfied by “(3) blocking communications to and from the computational component affected by the instance of a breach of a security measure[.]” I also note that by “blocking communications to and from the computational component affected by the instance of the breach of a [the] 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.”

229. As explained above with respect to the firewall gateway, Amirtahmasebi discloses that the gateway ECU is the point through which ECU-to-ECU communications pass for authentication and authorization. (Amirtahmasebi, Ex. 1019, p. 45.) Specifically, Amirtahmasebi discloses “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.” (Amirtahmasebi, Ex. 1019, p. 45.; ¶¶188-190 above.) Likewise,

“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.” (Amirtahmasebi, Ex. 1019, p. 46.)

230. A PHOSITA would have understood that when the firewall gateway “discards” messages from an ECU that fails authentication or exhibits signs of compromise, the result is that no messages from that ECU are permitted onto the bus, and likewise the ECU cannot receive functional responses because it has been rejected as an authenticated participant. This constitutes both *directing* communications to and from each ECU, including a computational component affected by the instance of a breach of a security measure, to the firewall gateway to enforce a security measure blocking communications to and from the computational component affected by the instance of a breach, precisely as required by limitations (2) and (3) respectively.

231. As explained above in [1e] with regards to the gateway-implemented IDS, Amirtahmasebi discloses 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.” (Amirtahmasebi, Ex. 1019, p. 46.)

232. A PHOSITA would have understood that IDS-driven “deactivation” of a misbehaving ECU prevents that ECU from transmitting onto or participating in the

shared communication bus thereby denying access to the network. Because a deactivated ECU cannot place messages on the network or receive messages from other ECUs, the IDS thereby blocks all communications to and from the computational component affected by the instance of a breach, satisfying limitation (3), and also denies “network access to the computational component affected by the instance of a breach of a security measure,” satisfying limitation (1) as well.

4. Dependent Claims 2-8

233. Claims 2-8 depend from claim 1, which I understand means that these claims require all of the limitations of claim 1 as well as their additional limitations. The combination of Amirtahmasebi and Bosch teaches all of the limitations of claim 1 as described above.

a. Claim 2

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, caffe latte attack, or denial of a computer network and/or network-accessible resource,

234. Amirtahmasebi discloses various logical attacks and hardware/physical attacks on in-vehicle network systems. (Amirtahmasebi, Ex. 1019, pp. 33-38.) These

attacks include both passive and active attacks and map directly onto several well-established classes of “security breach instances” identified in the claim.

235. For example, Amirtahmasebi discloses “Software Attacks” arising from software bugs or maliciously introduced code. As described: “[B]y injecting malicious code for instance, an attacker can try to exploit the ECU software update functionality. The 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.” (Amirtahmasebi, Ex. 1019, p. 33.)

236. A PHOSITA would have understood this to be an instance of “*malware*” because malicious code that infiltrates an ECU and causes it to behave abnormally—including sending malformed frames—is the very definition of malware: software designed to disrupt, disable, or compromise a computing system. Thus, Amirtahmasebi’s malicious-code attack constitutes a claimed “*security breach instance*” known as “*malware*.”

237. As another example, Amirtahmasebi discloses a more complex combination of attacks, referred to as a “vehicle virus” attack:

Apart from the mentioned threats and vulnerabilities, a combination of these attacks can also be built and launched against the in-vehicle network in order to form more sophisticated attacks. The concept is called vehicle virus [28] and can be built into a piece of code and be sent to the vehicle’s network through a FOTA process. By a

combination of the mentioned building blocks, the virus can become more intelligent and may be able to cause considerable damage to the vehicle's network or extract invaluable information. Therefore, the mentioned security properties must be considered completely in order to prevent such actions to take place.

(Amirtahmasebi, Ex. 1019, p. 37-38.)

238. Such referred to “building blocks” are described in more detail by Amirtahmasebi and include “Read,” “Spoof,” “Drop,” “Modify,” “Flood,” “Steal,” and “Replay” seen in Figures 4-10. (Amirtahmasebi, Ex. 1019, pp. 30-32; Figure 4-10.)

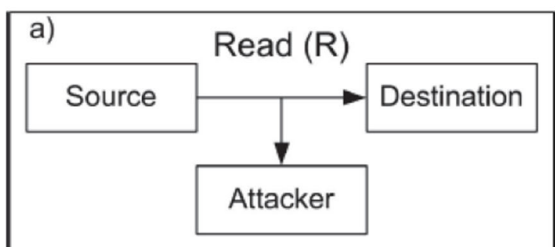


Figure 4. Read Building Block

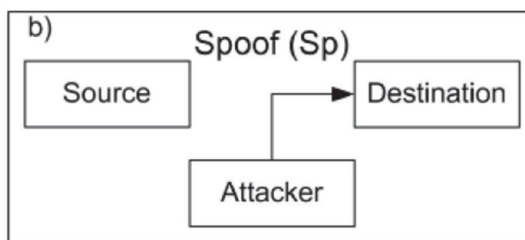


Figure 5. Spoof Building Block

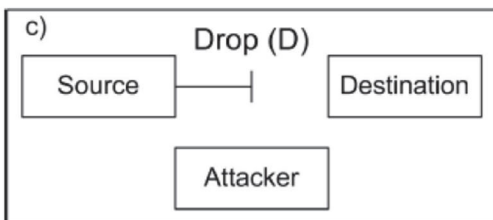


Figure 6. Drop Building Block

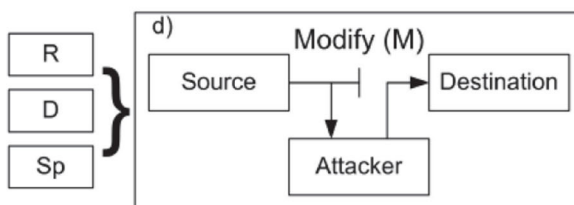


Figure 7. Modify Building Block

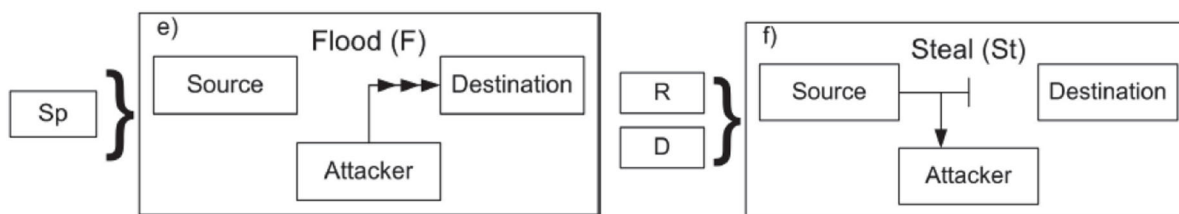


Figure 8. Flood Building Block

Figure 9. Steal Building Block

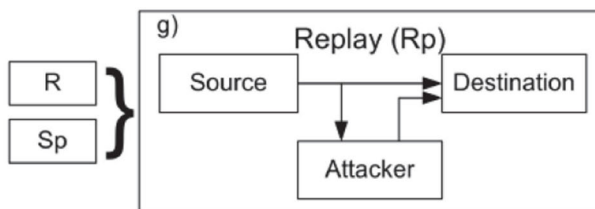


Figure 10. Replay Building Block

Amirtahmasebi, Ex. 1019, Figures 4-10

239. A PHOSITA would have understood that “a vehicle virus built into a piece of code and sent to the vehicle’s network” is, by definition, a virus—i.e., malicious code that propagates through a system and harms or subverts components. Thus, Amirtahmasebi discloses a claimed “*security breach instance*” of a “*virus.*”

240. As another example, Amirtahmasebi further discloses both logical and physical denial-of-service attacks. With regards to “logical denial of service” attacks, Amirtahmasebi discloses:

Logical denial of service attack is a malicious jamming attack which logically prevents or confines the availability of the communication channel. Denial of service attacks generally don’t require bypassing a particular security or cryptographic measure, and are therefore easy to launch. Comparing with physical DoS attacks which will be discussed

later, logical DoS attacks don't deal with physical channel properties, but are rather performed by repeatedly sending faulty messages or excessively running a particular program.

(Amirtahmasebi, Ex. 1019, p. 34.)

241. As to “physical denial of service” attacks, Amirtahmasebi explains:

Denial of service attacks belong to the category of active attacks which can be both invasive and non-invasive. According to [11], physical denial of service attacks refer to disruption of physical availability by preventing or considerably delaying access to critical resources, communication or functionality.

Physical denial of service attacks are mostly done by signal jamming, data deletion or communication deactivation. These can be done by launching non-invasive attacks such as noise distribution using strong electromagnetic fields, as well as invasive attacks such as short-circuits, shielding wired communication channels or detaching transmission devices.

(Amirtahmasebi, Ex. 1019, p. 37.)

242. A PHOSITA would have understood that Amirtahmasebi's disclosure of “logical denial of service” and “physical denial of service” attacks would each constitute a “*security breach instance*” known as a “*denial-of-service attack*.”

243. As another example, Amirtahmasebi discloses a spoofing attack, explaining: “Due to lack of authentication, the attacker can inject messages targeted to the victim ECU(s) into the network, as shown in figure 5.” (Amirtahmasebi, Ex.

1019, p. 30.) As discussed above, Amirtahmasebi details detection and security systems to protect against spoofing attacks.

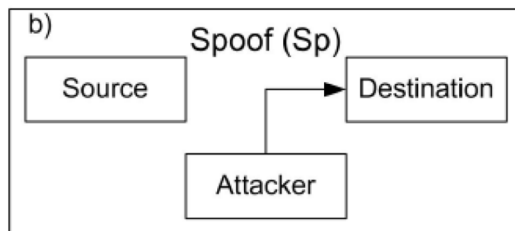


Figure 5. Spoof Building Block

Amirtahmasebi, Ex. 1019, Figure 5

244. A PHOSITA would have understood that Amirtahmasebi's disclosure of a "spoof" attack would constitute a "*security breach instance*" known as a "*spoofing*."

245. As another example, Amirtahmasebi discloses "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. Therefore, the attacker will be able to gain higher privileges, abusing other's identities while not being detected [11]." (Amirtahmasebi, Ex. 1019, p. 34)

246. A PHOSITA would have understood that Amirtahmasebi's "impersonation and masquerading attacks" is a "*security breach instance*" considered "*identity theft*."

247. Thus, Amirtahmasebi discloses “*wherein the security breach instance is one or more of an instance of a virus, malware, [] denial-of-service attack, spoofing, [and] identity theft*”.

[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 instance, and a network probe, and

248. As discussed in section [1c] above, Amirtahmasebi discloses a gateway ECU which itself would include a “*network controller*” that receives messages, status information, and security-related signals from ECUs and gateways throughout the in-vehicle network.

249. For example, as discussed above, Amirtahmasebi discloses “a firewall mechanism within network gateways” capable of reviewing MACs or digital signatures used by ECUs and only allowing messages from “valid and authentic ECUs” to pass through and be transmitted on the in-vehicle bus. (Amirtahmasebi, Ex. 1019, pp. 45-46.) A PHOSITA would have understood such “firewall mechanism” is “*a firewall*.”

250. A PHOSITA would have understood that when the firewall detects a failed authentication or invalid signature, the firewall generates or triggers a security-related alert indicating a breach condition (“*a warning signal associated*

with the security breach”) and that such a warning signal would be received by the “*network controller*” within the gateway ECU.

251. As another example, Amirtahmasebi further discloses a “*honeypot*” gathering attacker’s information and detects malicious attacks:

3.6.4 Honeypots

The vehicle’s wireless communication gateway will provide a vulnerable entry point open to attackers. By having wireless access to a vehicle, an attacker will be able to launch cyber attacks, directly targeting the in-vehicle network. Since the most critical and significant operations of a vehicle are performed and controlled by the in-vehicle network, it is of great importance to secure the in-vehicle communication system from being compromised by such attacks. Learning the attacker’s behavior, techniques and approaches is an effective method which helps to design and develop highly effective security solutions for in-vehicle communication systems.

Regarding this concept, a honeypot can be used for gathering attacker’s information. The basic idea behind honeypots is to provide a vulnerable easy to access target for attackers by intentionally expose system weaknesses toward them and thus analyzing their behavior and techniques. According to [35], honeypots are tools for prevention and early detection of malicious attacks based on studying the attackers’ malicious and unauthorized behavior within the system.

(Amirtahmasebi, Ex. 1019, p. 46.)

252. A PHOSITA would have understood that “*a honeypot*”, once detecting malicious behavior, provides detection output (“*a warning signal associated with the security breach*”) which would be sent to and received by the “*network controller*” within the gateway ECU for further security action.

253. As another example, as discussed in section [1b] above, Amirtahmasebi further discloses each ECU may be provided with an Intrusion Detection System (IDS). Amirtahmasebi discloses detection of “Obvious misuse of Message-IDs,” explaining:

Since authenticity of the message is not supported in in-vehicle networks, an attacker can easily send malicious commands and use a legitimate ECU’s ID and be certain that all victim ECUs will receive and act correspondingly. By doing so, fabricated messages will also arrive at the ECU whose ID has been used. Therefore, by adding some IDS functionality to the ECUs, these attacks can be identified and mitigated by the ECUs themselves.”

(Amirtahmasebi, Ex. 1019, p. 41.)

254. Amirtahmasebi further explains that in a semi-central architecture, individual ECUs operate as “self-secured ECUs” equipped with “autonomous security functionality”:

In this scenario, there exist a central security module along with some individual self-secured ECUs and devices such as critical sensors and actuators. The ECUs, equipped with autonomous security functionality

(which mainly includes secure authentication, communication and storage), will be able to take part in security-sensitive applications, similar to what happens in distributed security architecture explained in the previous section.

(Amirtahmasebi, Ex. 1019, p. 49.)

255. A PHOSITA would have understood that such IDS-enabled ECUs qualify as “*network nodes impacted by the security breach instance*,” and upon detecting misuse or malicious activity, these ECUs would send a “*warning signal associated with the security breach*” to the “*network controller*” within the gateway ECU.

256. As another example, as discussed above, Amirtahmasebi discloses an Intrusion Detection System (IDS) capable of “comparing incoming/outgoing messages with predefined patterns” to detect malicious behavior. (Amirtahmasebi, Ex. 1019, p. 41.) Amirtahmasebi discloses:

- Increased Message Frequency: Some devices in the vehicle network broadcast CAN messages frequently, therefore, single CAN IDs are sent over the network constantly with fixed frequency. Anomaly in sending such CAN messages can be a sign of unauthorized and malicious access to the network. Hence, this can be defined as a pattern in the intrusion detection system.

...

- Low-level communication characteristics: While the two aforementioned patterns will work on link level, CAN networks can be protected on physical layer as well. By analyzing different features such as voltage amplitudes and their stability, the shape of clock edges, propagation delays, signal attenuation, etc. of different manufacturers, a detection mechanism can be developed in order to identify unauthenticated devices which will try to inject messages on the CAN network.

(Amirtahmasebi, Ex. 1019, p. 41.)

257. The ‘100 patent does not explicitly define a “*network probe*.” A PHOSITA would have understood a network probe to be hardware or software that monitors network traffic for security-related anomalies, which is precisely the function performed by the IDS detection modules described by Amirtahmasebi.

258. Thus, a PHOSITA would have understood that the IDS disclosed by Amirtahmasebi operates as a “*network probe*” capable of sending a “*warning signal associated with the security breach*” to the “*network controller*” within the gateway ECU.

259. Thus, Amirtahmasebi discloses “*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*”.

[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:

260. As discussed above in limitation [1b], Amirtahmasebi discloses a “firewall mechanism” within the gateway, configured to use “message authentication codes (MAC) or digital signatures” to authenticate and authorize messages sent between ECUs. (Amirtahmasebi, Ex. 1019, p. 45-46.) Amirtahmasebi also discloses 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.” (Amirtahmasebi, Ex. 1019, p. 46.) Through these mechanisms, Amirtahmasebi 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.” (Amirtahmasebi, Ex. 1019, p. 46.)

261. A PHOSITA would have understood Amirtahmasebi’s MAC authentication is a form of security regarding “*checks on MAC addresses*,” while

Amirtahmasebi's use of digital signatures is a form of "encryption"-based authentication. Both are industry-standard cryptographic techniques for securing message integrity and authenticity within vehicular and wireless networks.

262. A PHOSITA would have understood that the "firewall mechanism" disclosed by Amirtahmasebi is a "*first security mechanism*" because it is the component expressly responsible for performing the core security functions of authenticating, validating, and selectively permitting or blocking messages within the in-vehicle network.

263. A PHOSITA would further have understood that the firewall within the gateway ECU "*isolates the vehicular network*" because Amirtahmasebi teaches that messages from ECUs failing authentication are not permitted to pass through the gateway's firewall. A PHOSITA would have understood that preventing unauthorized messages from traversing the gateway isolates the protected vehicle subnetworks from improperly behaving or compromised ECUs. When a firewall functions as the mandatory chokepoint controlling inter-network communications, a PHOSITA would have recognized this as textbook network isolation.

264. Thus, a PHOSITA would have understood that the firewall mechanism with the gateway ECU disclosed by Amirtahmasebi falls squarely within the claimed category of "*first security mechanism*" that "*isolate[es]the vehicular network by a firewall and/or gateway.*"

b. Claim 3

265. Claims 3 depends from claim 2, which I understand means that this claim requires all of the limitations of claim 2 as well as its additional limitations. The combination of Amirtahmasebi and Bosch teaches all of the limitations of claim 2 as described above.

3[pre] The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational component,

266. As discussed above, Amirtahmasebi discloses vehicle ECUs on board the vehicle (“*on board computational components*”) may be compromised by software attacks, disclosing: “By injecting malicious code for instance, an attacker can try to exploit the ECU software update functionality. The 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.” (Amirtahmasebi, Ex. 1019, p. 33.)

267. Amirtahmasebi explicitly contemplates an ECU with compromised security, stating “Vehicle 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.” (Amirtahmasebi, Ex. 1019, p. 39) (citation omitted.)

268. A PHOSITA would have understood that the misbehaving or compromised ECU in Amirtahmasebi is itself an “*on board computational component*” because ECUs are implemented physically within the vehicle and directly serve as its embedded processing units. Therefore, when Amirtahmasebi describes a compromised ECU, a PHOSITA would have understood that the “*computational component affected by the security breach 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

269. Intentionally left blank.

270. Amirtahmasebi discloses the ECUs on board the vehicle includes safety critical components and non-safety critical components:

3.1.1 ECU Classification

ECUs can be classified into five different categories based on the criticality of their tasks and the effect of failure on passengers’ safety [19].

- *Powertrain ECUs* are used for controlling critical vehicle components such as engine control (e.g. traction control) and braking system (e.g. electronic brake force distribution). Failure in such ECUs will cause

serious risks in vehicle safety and will damage the vehicle; therefore, these ECUs will be classified as safety-critical [20].

- *Vehicle safety ECUs* will provide assistance to the driver in terms of safety and control. Such ECUs use information about road conditions, driving speed, etc. to maximize car safety. Examples of vehicle safety ECUs are adaptive cruise control, ABS, collision avoidance systems and airbag. This category will also be classified as safety-critical.
- *Comfort ECUs* are of less importance compared to other two categories. These ECUs provide services such as temperature control and parking assistance, therefore, on the condition of failure such ECUs will not put the vehicle in danger.
- *Infotainment* is another category which is a non-safety related category of ECUs [20]. This class of ECUs is in charge of entertainment units such as CD/DVD players, audio streams, navigation systems, etc. which will not affect the safety of the vehicle in case of failure. However, this class requires very fast bus since audio/video information need fast transmission.
- *Telematics* are the final category of ECUs which provide networked software applications to the vehicle [19]. This category will also be classified as non-safety related since they won't immediately affect the safety of the vehicle or the driver."

(Amirtahmasebi, Ex. 1019, p. 24-25.) (italicized in original)

271. A PHOSITA would have understood that the "powertrain ECUs" and "vehicle safety ECUs" are "*critical devices*" because they control safety-critical

vehicle functions whose failure poses safety consequences. Likewise, a PHOSITA would have understood that “comfort ECUs,” “infotainment ECUs,” and “telematics ECUs” correspond to “*non-critical devices*” because their failure does not impact vehicle or passenger safety.

272. Therefore, Amirtahmasebi discloses “*one of the plurality of on board computational components*” is a Powertrain ECU, such as the powertrain ECU, that is a “*critical device*.” Similarly, Amirtahmasebi discloses “*one of the plurality of on board computational components*” is a Infotainment ECU, such as an audio stream, that is a “*non-critical device*” , as recited in claim 3(a).

[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.

273. As discussed above in section [1b], Amirtahmasebi discloses multiple in-vehicle subnetworks—e.g., CAN, LIN, MOST, FlexRay—which a PHOSITA would have recognized as each contain ECUs capable of separately or collectively being a part of the “*perimeter network*” formed by the security mechanism as I discussed in limitation 1[b]. As discussed in section [3a] above, each of these subnetworks include *critical* and *non-critical devices*/ECUs which are the “*computational components*” which could be affected by the “*security breach instance*.”

274. Amirtahmasebi further describes distributed and semi-central security architectures in which ECUs possess “autonomous security functionality” and “take part in shaping the overall security functionality,” “which mainly includes secure authentication, communication, and storage.” (Amirtahmasebi, Ex. 1019, p. 49.) This autonomous security functionality may include ECU-level IDS detection. As described above, an ECU can detect misuse of its Message-ID and respond to malicious identity spoofing. (Amirtahmasebi, Ex. 1019, p. 41.)

275. A PHOSITA would have understood that when security protections operate at the ECU-level—without requiring messages to pass through a gateway—the affected ECU and the unaffected ECU(s) it exchanges messages with will be located within the same vehicle subnetwork (e.g., CAN).

276. As such, because the IDS detects misuse occurring within that shared bus and works to protect other ECUs on that same subnetwork, a PHOSITA would have understood that both the compromised ECU (“*computational component affected by the security breach instance*”) and the ECU(s) it interacts with (“*at least one on-board computational component*”) are located within a single “*perimeter network*” as required by limitation [3b].

c. Claim 4

277. Claim 4 depends from claim 2, which I understand means that this claim requires all of the limitations of claim 2 as well as its additional limitations. Amirtahmasebi teaches all of the limitations of claim 2 as described above.

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

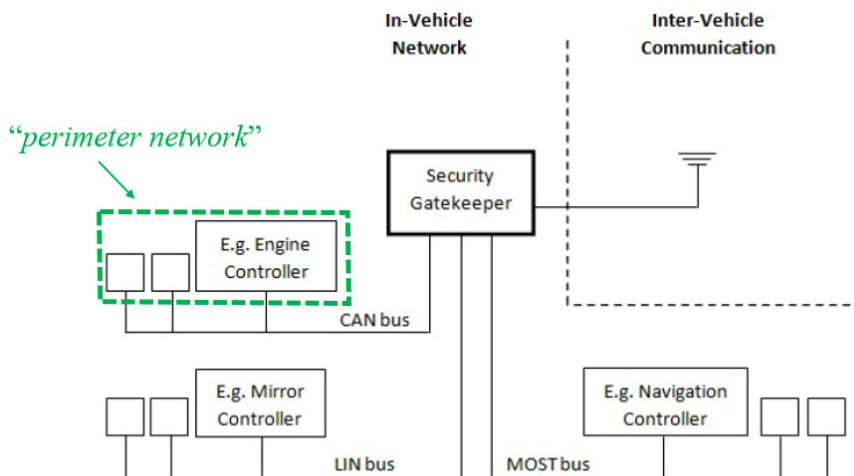
278. Intentionally left blank.

279. Amirtahmasebi discloses that ECUs (“*on board computational components*”) may be compromised by malicious code or other software attacks. (Amirtahmasebi, Ex. 1019, p. 33.) As explained: “By injecting malicious code for instance, an attacker can try to exploit the ECU software update functionality. The 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.” (Amirtahmasebi, Ex. 1019, p. 33.) Amirtahmasebi further states, “Vehicle 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.” (Amirtahmasebi, Ex. 1019, p. 39) (citation omitted.)

280. As discussed in section [1b], Amirtahmasebi discloses creation of a security boundary established to protect the internal networks (in-vehicle network)

from external, untrusted communications (for both inter-vehicle communications and communications to the vehicle from a key FOB or FOTA) and thus would constitute the recited “*perimeter network*.” As Amirtahmasebi details the “*perimeter network*” could be established around one or more of the protected ECUs within the vehicle to protect a given ECU (and ultimately all ECUs) from susceptible attacks from external, untrusted communications.

281. For instance, the “*perimeter network*” could be formed to protect ECUs within an entire network, such as the CAN, MOST, or LIN networks, as seen in Figure 12 below.



Amirtahmasebi, Ex. 1019, Figure 12

282. Amirtahmasebi also discloses architectures in which security operations are centralized or semi-centralized through “a central security module” responsible for “security operations of all internal and external ECUs and devices.”

(Amirtahmasebi, Ex. 1019, p. 48.) As explained in sections [1b] and [1c], the firewall gateway ECU performs this function.

283. Amirtahmasebi further discloses deliberate access-restriction between subnetworks:

Restricting the access level of different types of networks to other parts of the bus system can be another approach to defining firewall rules.

For instance, 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 [11].

(Amirtahmasebi, Ex. 1019, p. 46.)

284. A PHOSITA would have understood that when Amirtahmasebi describes firewall isolation rules that prevent an ECU of one subnetwork (e.g., LIN or MOST) or from an untrusted external device from sending messages to ECUs of another subnetwork (e.g., CAN), Amirtahmasebi describes the ECU or external device as outside the logical “*perimeter network*” that contains the protected ECUs.

285. As such, a PHOSITA would have understood Amirtahmasebi discloses claim 4 because “*the computational component affected by the security breach instance*” for example, an ECU on a LIN network sending malformed or malicious traffic, is “*outside of a perimeter network of the vehicle containing the at least one on-board computational component*” (for example, protected ECUs of the CAN subnetwork), because the firewall gateway disclosed by Amirtahmasebi enforces the

boundary between subnetworks and thereby renders the misbehaving ECU “*outside of*” the protected logical “*perimeter network*” in exactly the structural manner required by limitation [4pre].

286. As explained in sections [1b] and [1c], Amirtahmasebi also discloses isolation rules that address any “vehicle virus” that “can be built into a piece of code and be sent to the vehicle’s network through a FOTA process.” (Amirtahmasebi, Ex. 1019, p. 37-38.) To protect the vehicle Amirtahmasebi teaches how a security boundary can be established to ultimately protect the internal network from external, untrusted communications. These external, untrusted communications could come from inter-vehicle networks (e.g., communications sent via VANET networks) or in-vehicle network communication with external systems (e.g., FOTA updates from an external computing system).

Logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications (e.g. C2C cooperative driving system). Likewise, an internal attacker can benefit from available on-board interfaces such as telematics or software update interfaces.

(Amirtahmasebi, Ex. 1019, p. 32) (citation omitted.)

287. A PHOSITA would have understood that when Amirtahmasebi describes isolation rules that prevent an external computing system “*outside of the perimeter network*” from sending a vehicle virus via a FOTA update to an on-board ECU.

288. As such, a PHOSITA would have understood Amirtahmasebi discloses claim 4 because “*the computational component affected by the security breach instance*” for example, an external computing system containing a vehicle virus, is “*outside of a perimeter network of the vehicle containing one of the plurality of on board computational components*” (for example, protected ECUs of the CAN subnetwork), because the firewall gateway disclosed by Amirtahmasebi enforces the boundary between subnetworks and thereby renders the external computing system containing the vehicle virus “*outside of*” the protected “*perimeter network*” in exactly the structural manner required by claim [4pre].

[4a] wherein the at least one board computational component is one or more of an onboard 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 onboard 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.

289. This limitation is substantially similar to that of limitation [3a], discussed above. As best understood by a PHOSITA, this claim also intends to claim “*the at least one on board computational component*”.

290. Amirtahmasebi discloses the ECUs on board the vehicle includes safety critical components (“*critical system controller*”) and non-safety critical components (“*non-critical system controller*”):

3.1.1 ECU Classification

ECUs can be classified into five different categories based on the criticality of their tasks and the effect of failure on passengers’ safety [19].

- *Powertrain ECUs* are used for controlling critical vehicle components such as engine control (e.g. traction control) and braking system (e.g. electronic brake force distribution). Failure in such ECUs will cause serious risks in vehicle safety and will damage the vehicle; therefore, these ECUs will be classified as safety-critical [20].

- *Vehicle safety ECUs* will provide assistance to the driver in terms of safety and control. Such ECUs use information about road conditions, driving speed, etc. to maximize car safety. Examples of vehicle safety ECUs are adaptive cruise control, ABS, collision avoidance systems and airbag. This category will also be classified as safety-critical.

- *Comfort ECUs* are of less importance compared to other two categories. These ECUs provide services such as temperature control and parking assistance, therefore, on the condition of failure such ECUs will not put the vehicle in danger.
- *Infotainment* is another category which is a non-safety related category of ECUs [20]. This class of ECUs is in charge of entertainment units such as CD/DVD players, audio streams, navigation systems, etc. which will not affect the safety of the vehicle in case of failure. However, this class requires very fast bus since audio/video information need fast transmission.
- *Telematics* are the final category of ECUs which provide networked software applications to the vehicle [19]. This category will also be classified as non-safety related since they won't immediately affect the safety of the vehicle or the driver."

(Amirtahmasebi, Ex. 1019, pp. 24-25.) (italicized in original)

291. A PHOSITA would have understood that Amirtahmasebi's "powertrain ECUs" and "safety ECUs" comprise "*one of the plurality of on board computational components*" that are "*critical system controllers*" that are within the "*perimeter network*" discussed above. Further, a PHOSITA would have understood that Amirtahmasebi's "comfort ECUs," "infotainment ECUs" and "telematics ECUs" comprise "*one of the plurality of on board computational components*" that are "*non-critical system controllers*" that are within the "*perimeter network*" discussed above.

d. Claim 5

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

292. Claim 5[pre] is largely duplicative of claim 4[pre]. To illustrate, the table below shows a side-by-side comparison of claims 5[pre] and 4[pre].

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	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
--	--

293. Because the claim language is materially the same, my analysis for claim 4[pre] applies equally to claim 5[pre], and Amirtahmasebi teaches this limitation for the same reasons explained above.

[5a] 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.

294. Amirtahmasebi discloses an IDS-enabled gateway as capable of “comparing incoming/outgoing messages with predefined patterns, a number of patterns in vehicle networks must be defined as malicious behavior.” (Amirtahmasebi, Ex. 1019, p. 41.) As discussed in section [2a], these patterns include message-frequency profiles and low-level physical-layer characteristics. (Amirtahmasebi, Ex. 1019, p. 41.)

295. Amirtahmasebi continues, stating “IDS systems must compare its existing data with some reference data in order to be able to perform intrusion detection.” (Amirtahmasebi, Ex. 1019, p. 41). Amirtahmasebi discusses “Rule-based detection,” wherein “a number of predefined actions, behaviors and combinations are stored in a signature/rule database and network traffic will be compared with the values in the database.” (Amirtahmasebi, Ex. 1019, p. 42.) Amirtahmasebi also discloses a second approach in “Anomaly-based intrusion detection” by which “Normal actions are predefined for the IDS and an action will be considered malicious if it is deviating from the normal behavior.” (Amirtahmasebi, Ex. 1019, p. 42) (citation omitted.) These disclosures show that the IDS compares behavior to pre-established templates of known attack signatures and templates of acceptable behavior.

296. A PHOSITA would have understood that the “*microprocessor executable network controller*” in Amirtahmasebi “*analyzes a security-breach instance*” because the IDS reviews message behavior over time—i.e., “*historical behavior*”—in order to identify deviations from expected patterns. This is because both the message-frequency analysis and the low-level signal-characteristic analysis disclosed by Amirtahmasebi require comparing current message behavior to previously observed baselines.

297. A PHOSITA would further have understood that the IDS “*compares that behavior to templates characteristic of differing types of attacks,*” since Amirtahmasebi expressly discloses rule-based detection in which predefined malicious actions, behaviors, and combinations stored in a rule or signature database are used as templates against which incoming traffic is evaluated, as well as anomaly-based detection in which “normal actions” serve as templates for identifying deviations. For the same reasons, a PHOSITA would have understood that the IDS applies rules to the observed behavior because the system evaluates traffic by applying the predefined rules and signatures stored in its database.

298. Accordingly, a PHOSITA would have recognized that Amirtahmasebi teaches the claimed analysis of a security-breach instance by reviewing “*historical behavior,*” comparing that behavior to attack-characteristic templates, and applying rules to determine whether malicious activity is present.

e. Claim 6

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

299. The '100 Patent identifies an “*external computational device*” as a computing device that is external to the vehicle and may connect to the vehicle using, for example, a wireless connection. Examples of external devices include cell phones, laptops, or remote computers.

In one vehicle configuration, the wireless interface 280 connects, via a short distance protocol such as Bluetooth™ or WiFi™, to an external computational device, such as a cell phone, personal digital assistant, laptop, personal computer, or tablet computer, for access to remote nodes over the Internet.

(’100 Patent, Ex. 1001, 16:56-61.)

The vehicle 100 includes a transceiver 1508 to send and receive signals over a selected one of the first, second, . . . networks 1504 *a*, *b*, . . . , a gateway/firewall 1512 to provide secure connectivity between the various components of the vehicle 100 and the first, second, . . . networks 1504*a*, *b*, . . . , primary and secondary processing modules 124*a* and *b*, memory/ storage 220 or 230, on board sensors 1516 (discussed above with reference to FIG. 1), input/output system(s) 1520 and associated media controller (discussed below) to manage and control the output presented by the input/output system(s) to the user, network controller 1528 to supervise local networks and nodes thereof

and identify and, if possible, isolate malfunctioning networks and/or nodes to avoid detrimental impact on other networks and/or nodes of the vehicle 100, and external computational device(s) 1532 of occupants, such as wireless capable mobile phones, personal digital assistants, tablet computers, laptop computers, and the like.

(’100 Patent, Ex. 1001, 22:51-23:1.)

300. Amirtahmasebi expressly discloses the existence of external attackers who use external computing devices including to launch attacks through wireless channels:

Logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications (e.g. C2C cooperative driving system).

(Amirtahmasebi, Ex. 1019, p. 32.)

301. With regards to Amirtahmasebi discloses the integrated gatekeeper, as show in Figure 12 below, is “used as a connection boundary between inner and outer vehicle networks.” (Amirtahmasebi, Ex. 1019, p. 40.)

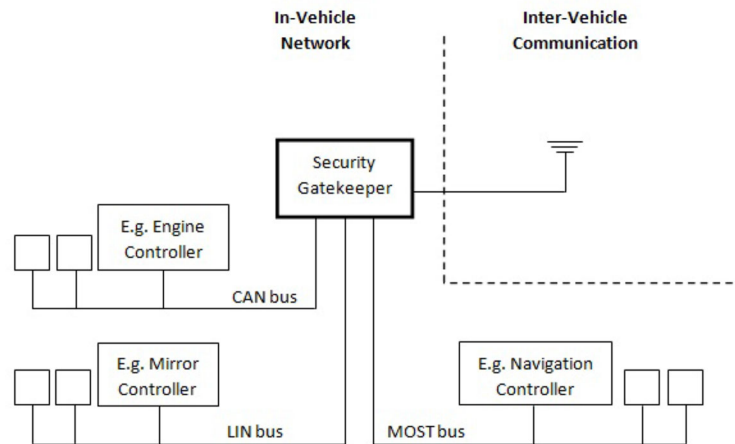


Figure 12. Integrated Data Security Gatekeeper

Amirtahmasebi, Ex. 1019, Figure 12

302. Amirtahmasebi also states: “From the attackers’ point of view, the communication channel seems the best entry point to the whole vehicular network since there is no need for external attackers to gain physical access to the vehicle and they can perform their attacks and damages remotely.” (Amirtahmasebi, Ex. 1019, p. 33.) This disclosure directly contemplates attacks launched from outside the vehicle by remote computing devices.

303. Similarly, Amirtahmasebi describes “Bogus Information” attacks in which external attackers transmit falsified messages into the network:

This attack particularly targets messages transmitted between vehicles. An attacker can affect other drivers’ behavior by spreading wrong information in the network. For instance a driver can simulate a heavy traffic and thus preventing other drivers to choose the road he is driving on. This attack can be launched by both legitimate network nodes as well as outsiders.

(Amirtahmasebi, Ex. 1019, p. 15.)

304. Amirtahmasebi further reinforces that such external attackers operate from off-vehicle computing devices—including roadside laptops—when discussing certificate-based measures intended to exclude them:

Associating digital signatures with certificates basically targets excluding external attackers such as a road-side attacker using his laptop computer to launch an attack scenario. Since only valid VANET nodes possess the certificates, other external nodes will not be able to send messages within the corresponding domain. Moreover there exists the possibility to identify and remove the malicious behaving or defective nodes by revoking their certificates [7].

(Amirtahmasebi, Ex. 1019, p. 21.)

305. A PHOSITA would have understood that when Amirtahmasebi describes attacks launched wirelessly by “outsiders,” those outsiders act through external computing devices (such as laptops, mobile devices, or roadside units) that generate the malicious messages.

306. Because these devices initiate the attack and produce the malicious data at issue, a PHOSITA would have further understood them to be the “*computational component affected by the security breach instance*” and, by virtue of being external to the vehicle’s internal network, an “*external computational device*” as required by claim 6.

[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.

307. I understand this limitation to require that the vehicle's wireless network deny access to the external device launching the attack, thereby isolating protected on-board components.

308. Amirtahmasebi discloses excluding external attackers from accessing the vehicle wireless network using digital signatures with certificates:

Associating digital signatures with certificates basically targets excluding external attackers such as a road-side attacker using his laptop computer to launch an attack scenario. Since only valid VANET nodes possess the certificates, other external nodes will not be able to send messages within the corresponding domain. Moreover there exists the possibility to identify and remove the malicious behaving or defective nodes by revoking their certificates [7].

(Amirtahmasebi, Ex. 1019, p. 21.)

309. The disclosure also notes the ability to “identify and remove malicious... nodes by revoking their certificates.” (Amirtahmasebi, Ex. 1019, p. 21.)

310. A PHOSITA would have understood that when an external attacker's device lacks the required digital certificates—or when its certificates have been

revoked—the vehicular wireless network will refuse to accept any of its transmissions, thereby preventing the external device from communicating with the in-vehicle network.

311. Because this certificate-based exclusion stops the external computational device from placing messages onto the wireless link or interacting with any on-board ECUs, a PHOSITA would have recognized that the on-board computational components are effectively isolated from the attacker. In this way, Amirtahmasebi discloses “*the vehicular wireless network denying vehicular wireless network access by the external computational component,*” which is exactly the form of isolation required by claim 6(a).

312. Intentionally left blank.

313. Intentionally left blank.

314. Intentionally left blank.

f. Claim 7

[7] 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.

315. As best understood in light of the specification, I understand this claim to mean:

At least one of the following can be true about the isolation: (a) communications between the one or more other on board computational component(s) in the vehicular wireless network not affected by the security breach event and the computational component affected by the security breach event, the communications not normally passing through a gateway and/or firewall, can be redirected through and filtered by the gateway and/or firewall and (b) communications between the one or more other on board computational component(s) in a vehicular wireless network not affected by the security breach event and the computational component affected by the security breach event can be blocked in whole or part.

(’100 Patent, Ex. 1001, 5:11-23.)

316. Amirtahmasebi discloses that ECUs may communicate wirelessly to external networks in connection with remote services, including FOTA updates and remote diagnostics:

Remote software updates will not require an authorized service center and needs a secure manufacturer’s web portal and a secure communication channel instead. Vehicles can connect to the

manufacturer's web portal and download the software to their respective ECUs. The concept is called Firmware Updates Over the Air (FOTA) and is to the benefit of owners and manufacturers in terms of time and money. The procedure works by re-flashing current ECU software and installing new firmware. By having downloaded the new ECU firmware, the ECU will reboot and work with the new firmware [24].

(Amirtahmasebi, Ex. 1019, pp. 27-28.)

Apart from FOTA, by connecting in-vehicle networks to external networks, vehicles can be diagnosed remotely without being taken to service centers. A car can be checked up over the Internet and can alert the driver about the resulting diagnosis.

(Amirtahmasebi, Ex. 1019, p. 28.)

317. A PHOSITA would have understood that any ECU capable of FOTA updates or remote diagnosis participates in a vehicular wireless network and therefore qualifies as an “*on board computational component in a vehicular wireless network.*” These ECUs communicate through wireless interfaces that form part of the vehicle's external communication channels.

318. Additionally, Amirtahmasebi discloses Infotainment ECUs, “in charge of entertainment units such as CD/DVD players, audio streams, [and] navigation systems.” (Amirtahmasebi, Ex. 1019, p. 25.) A PHOSITA would have understood that such navigation and infotainment ECUs exchange data via wireless networks

(e.g., GPS, telematics, Internet connectivity), and therefore each also qualify as “*on board computational component in a vehicular wireless network.*”

319. As discussed above, Amirtahmasebi discloses a firewall gateway in which “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.” (Amirtahmasebi, Ex. 1019, p. 46.)

320. 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 an unaffected ECU operating on the vehicular wireless network (such as a navigation ECU).

321. This is because when the gateway discards messages originating from an unauthenticated or malicious ECU, those messages never reach the unaffected on-board components, thereby achieving the claimed form of isolation by “*block[ing] in whole or in part*” the communications between the two components.

322. Intentionally left blank.

323. Intentionally left blank.

324. Intentionally left blank.

325. Intentionally left blank.

g. Claim 8

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,

326. As discussed above with respect to claim limitation 1[a], Amirtahmasebi discloses that vehicles include “a combination of Electronic Control Units (ECU)” (“*a plurality of on board computational components*”). (Amirtahmasebi, Ex. 1019, p. 11.)

327. Amirtahmasebi also explains that ECUs are classified by function and safety criticality, including safety-critical powertrain and vehicle-safety ECUs, and non-critical comfort, infotainment, and telematics ECUs:

3.1.1 ECU Classification

ECUs can be classified into five different categories based on the criticality of their tasks and the effect of failure on passengers’ safety [19].

- *Powertrain ECUs* are used for controlling critical vehicle components such as engine control (e.g. traction control) and braking system (e.g. electronic brake force distribution). Failure in such ECUs will cause serious risks in vehicle safety and will damage the vehicle; therefore, these ECUs will be classified as safety-critical [20].

- *Vehicle safety ECUs* will provide assistance to the driver in terms of safety and control. Such ECUs use information about road conditions, driving speed, etc. to maximize car safety. Examples of vehicle safety ECUs are adaptive cruise control, ABS, collision avoidance systems and airbag. This category will also be classified as safety-critical.
- *Comfort ECUs* are of less importance compared to other two categories. These ECUs provide services such as temperature control and parking assistance, therefore, on the condition of failure such ECUs will not put the vehicle in danger.
- *Infotainment* is another category which is a non-safety related category of ECUs [20]. This class of ECUs is in charge of entertainment units such as CD/DVD players, audio streams, navigation systems, etc. which will not affect the safety of the vehicle in case of failure. However, this class requires very fast bus since audio/video information need fast transmission.
- *Telematics* are the final category of ECUs which provide networked software applications to the vehicle [19]. This category will also be classified as non-safety related since they won't immediately affect the safety of the vehicle or the driver.

(Amirtahmasebi, Ex. 1019, p. 24-25.) (italicized in original)

328. As I have explained in claim 1, a PHOSITA would have recognized one of the vehicle ECUs may be the “*at least one on board computational component*” that is “*not affected by the security breach instance.*” Amirtahmasebi explicitly identifies “critical ECUs,” including powertrain ECUs, as components that must be

secured against cyberattacks. (Amirtahmasebi, Ex. 1019, p. 55.) The Powertrain ECU, for example, would therefore be an “*on board computational component*” that is a “*a critical component.*”

329. Amirtahmasebi further details malicious communications from external wireless devices that are transmitted to the vehicle wireless network, and therefore proposes the use of security mechanisms like an integrated gateway, firewall, and intrusion-detection system (IDS). (Amirtahmasebi, Ex. 1019, pp. 40-41, Figure 12.) I also explained with regard to claim 1, the “*perimeter network*” is a logical boundary intended to separate “*the at least one computational component*” from other malicious components. A PHOSITA would have understood “*the at least one computational component*” could be either the vehicle’s internal computational components (e.g., ECUs, sensors, *etc.*) or an external device connected to the vehicle (e.g., a driver’s cell phone).

330. I have also explained above that Amirtahmasebi discloses a “ECU firmware must be possible to update in order to have maximum performance and fix occasional software bugs.” (Amirtahmasebi, Ex. 1019, p.23.) Amirtahmasebi also discloses how “[v]ehicles can connect to the manufacturer’s web portal and download the software to their respective ECUs.” This is done using “Firmware Over the Air (FOTA)” wireless connections where the ECU is “reflash[ed]” and new firmware is “installed.” (Amirtahmasebi, Ex. 1019, p.24.) Amirtahmasebi

recognizes this FOTA process 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. (Amirtahmasebi, Ex. 1019, pp. 33, 47.) A PHOSITA would therefore understand that an ECU that may receive such a FOTA update, e.g., a Powertrain ECU, would therefore be indirectly “*in a vehicular wireless network*” as it is connected to a gateway that is meant to receive FOTA requests intended for that ECU.

331. For these reasons, it is my opinion that Amirtahmasebi teaches the subject matter of dependent claim 8.

332. Intentionally left blank.

333. Intentionally left blank.

[8a] 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

334. Amirtahmasebi describes a firewall mechanism located “within the network gateway[.]” (Ex. 1019, p. 45, Figure 12.) This gateway monitors and controls message flow to prevent malicious communication being sent to the vehicle:

From a security point of view, the gatekeeper will be responsible for inspecting and managing the exchanged information passing through the gatekeeper. By secure communication and applications interaction

control, the gatekeeper will be able to provide the system with both integrity and confidentiality. In figure 12, there is a data gatekeeper used as a connection boundary between inner and outer vehicle networks.

(Amirtahmasebi, Ex. 1019, p. 40)

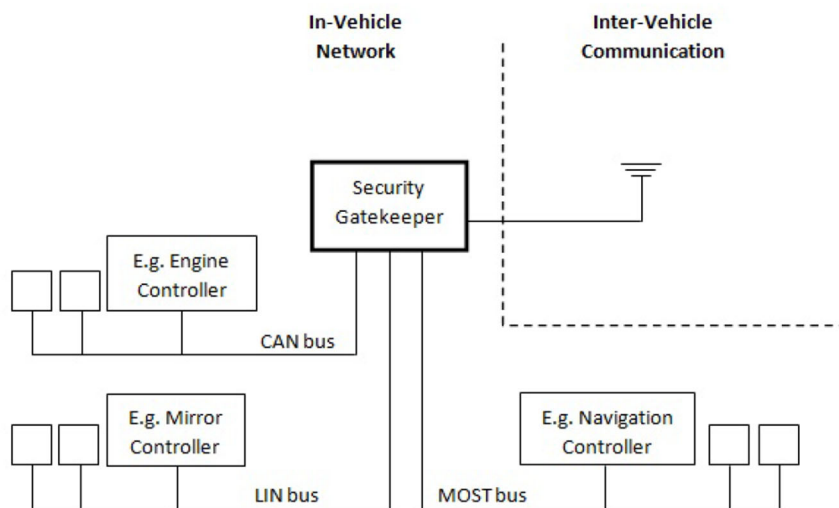


Figure 12. Integrated Data Security Gatekeeper

Amirtahmasebi, Ex. 1019, Figure 12

335. Amirtahmasebi discloses that “[l]ogical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications....” (Amirtahmasebi, Ex. 1019, p. 32.) Amirtahmasebi further discusses: “From the attackers’ point of view, the communication channel seems the best entry point... since there is no need for external attackers to gain physical access to the vehicle and they can perform their attacks... remotely.” (Amirtahmasebi, Ex. 1019, p. 33.)

336. The “*computational component affected by the security breach*” could be either the vehicle’s internal computational components (e.g., ECUs, sensors, *etc.*) or an external device connected to the vehicle (e.g., a driver’s cell phone). For example, the “*computational component affected by the security breach*” could be a Bluetooth module or key FOB transceiver which would be “*a node on the vehicular wireless network.*” Or the “*computational component affected by the security breach*” could be a driver’s cellular phone which is also connected to the vehicle’s Bluetooth or WiFi systems and is therefore “*a node on the vehicular wireless network.*” (Amirtahmasebi, Ex. 1019, pp. 40-41; Figure 12.) A PHOSITA would understand either of these devices could be the “*computational components*” susceptible to malicious communication and therefore “*affected by the security breach.*”

337. For instance, Amirtahmasebi states that the IDS can be employed to “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.” (Amirtahmasebi, Ex. 1019, p. 46.) Amirtahmasebi therefore teaches a PHOSITA that there could exist a “*computational component affected by the security breach instance*” (i.e., a “misbehaving ECU”).

338. Amirtahmasebi also discloses that a vehicle may include a variety of ECUs which could include “[t]elematics ... ECUs which provide networked software applications to the vehicle.” (Amirtahmasebi, Ex. 1019, p. 21.) Amirtahmasebi also teaches the telematics ECUs could be susceptible to the security breach instance. The Telematics ECU is networked and a PHOSITA would understand it could be a “*node on the vehicular wireless network.*”

Logical attacks are basically launched by both internal and external attackers who have access to built-in interfaces as well as external communication. An external attacker, for instance, can exploit the available wireless communication interface used for VANET applications (e.g. C2C cooperative driving system). Likewise, an internal attacker can benefit from available on-board interfaces such as telematics or software update interfaces [11].

(Amirtahmasebi, Ex. 1019, p. 32.)

339. Amirtahmasebi also teaches other “*computational components affected by the security breach*” on the vehicle may be located as a “*node on the vehicular wireless network.*” For instance, Amirtahmasebi teaches that from “the attackers’ point of view, the communication channel seems the best entry point to the whole vehicular network since there is no need for external attackers to gain physical access to the vehicle and they can perform their attacks and damages remotely.” (Amirtahmasebi, Ex. 1019, p. 33.) Amirtahmasebi further discloses attacks launched

from outside the vehicle would be directed to these “*computational components*” from external sources.

This attack particularly targets messages transmitted between vehicles. An attacker can affect other drivers’ behavior by spreading wrong information in the network. For instance a driver can simulate a heavy traffic and thus preventing other drivers to choose the road he is driving on. This attack can be launched by both legitimate network nodes as well as outsiders.

(Amirtahmasebi, Ex. 1019, p. 15.)

340. Intentionally left blank.

341. Claim 8[a] recites the “*computational component*” that is “*affected by the security breach instance*” is “*physically and/or logically positioned outside of but interiorly and/or internally to the perimeter network.*” In reviewing the ’100 Patent, I have not found an explanation as to how a “*computational component*” could be “*positioned outside of [the perimeter network] but ... internally to the perimeter network.*” Neither the claim nor the specification disclose how the affected “computational component” could be both inside and exterior to the perimeter network at the same moment. As best understood, I assume this limitation is satisfied by an ECU that is initially not affected by the security breach instance and therefore logically positioned within the perimeter network. The same ECU then could become affected by the security breach thereby resulting in the logical perimeter

network being re-established such that the affected ECU is now isolated and logically positioned outside the perimeter network. It is between this re-establishment that the ECU was internal and then becomes external based on it becoming affected by the security breach instance. As such, a PHOSITA would have understood that the “*computational component*” could be both internal and external when the logical “*perimeter network*” is being formed and reformed based on a given security breach.

342. Alternatively, a PHOSITA would have understood that a “*computational component*” like a cellular phone which is a “*node on the vehicular network*” could be a component “*affected by the security breach instance.*” The computational component would have been understood by a PHOSITA as being logically positioned outside the “*perimeter network*” as it is a cellular phone which may be removed from the vehicle. But a PHOSITA would have also understood that when connected to the vehicular network it could be logically internal to the “*perimeter network*” as it would be a device that—when affected by the security breach—could further affect other components connected to or within the vehicle (e.g., the Powertrain ECU), and thus would have security measures enforced over it.

343. Intentionally left blank.

344. Intentionally left blank.

[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 MACID 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, WPAv1, and/or WPAv2 protocols, and using end-to-end encryption.

345. Amirtahmasebi discloses using encryption for communication between ECUs (“*end-to-end encryption*”):

Encryption: Another possible security consideration is to encrypt the transmitted information between ECUs within the bus system. Since there are some limitations regarding CPU computational power, memory capacity and timing issues in vehicular network systems, a combination of symmetric and asymmetric encryption is needed to achieve the highest degree of security and performance at the same time.

(Amirtahmasebi, Ex. 1019, p. 45.)

346. A PHOSITA would have understood that Amirtahmasebi’s disclosure of “encrypt the transmitted information between ECUs within the bus system” indicates that the data transmitted between the ECUs is end-to-end encrypted. By performing the encryption for on the bus, the vehicle effectively enables a “*critical*

communication security mechanism” to prevent the “*computational component affected by the security breach instance*” from accessing other nodes of the bus, which effectively isolates the computational component.

347. A PHOSITA would therefore have recognized that such encryption isolates the compromised computational component from other computational components not affected, satisfying the isolation requirement of Limitation 8[b].

348. Intentionally left blank.

349. Intentionally left blank.

350. Intentionally left blank.

351. Intentionally left blank.

352. Intentionally left blank.

353. Intentionally left blank.

5. Independent Claim 9

a. Claim 9

354. Independent claim 9 is largely duplicative of independent claim 1. To illustrate, the table below shows a side-by-side comparison of claims 1 and 9. Claim 9 is “marked up” to show the minor differences.

Claim 1	Claim 9
1[pre]. A vehicle, comprising:	9[pre]. A <u>method</u> , comprising:

[1a] a plurality of on board computational components;	[9a] in a vehicle comprising 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
[1c] a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,	[9c] <u>a microprocessor executable network controller</u>, the microprocessor executable network controller identifying a possible security breach instance;

[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
[1e] (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	[9e] 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 instance of a breach of the security measure, at least one of	affected by or potentially affected by the possible security breach instance,
	the microprocessor executable network controller 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	(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) 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	(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

instance of a breach of a security measure,	potentially affected by the possible security breach instance,
[1f] 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	[9f] 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 instance of a breach of a security measure, and	affected by the possible security breach instance, and
(4) activating a second security mechanism in response to the instance of a breach of a security measure.	(4) activating a second security mechanism in response to the possible security breach instance.

9[pre]. A method, comprising:

355. Amirtahmasebi discloses various methods implemented on vehicle networks. For instance, Amirtahmasebi discloses an intrusion detection system (IDS) to “alert the driver about the attack so the driver can take appropriate measures.” (Amirtahmasebi, Ex. 1019, p. 41.) Amirtahmasebi further discloses the use of digital signatures and certificates in vehicular communication, describing the method by which messages are cryptographically signed, timestamped, transmitted, and verified:

A public key infrastructure is necessary to implement the concept of certificates issued by an authority. Before sending a message, the sender signs the message with its private key and provides the receiver with its CA's certificate. Before signing the message there is a time stamp concatenated with the message to guarantee message freshness.

Upon receiving, the receiver will decrypt the message (verify the sender's signature) using its certified public key. Sender's public key is verified by the receiver with respect to its certificate [14].

Associating digital signatures with certificates basically targets excluding external attackers such as a road-side attacker using his laptop computer to launch an attack scenario. Since only valid VANET nodes possess the certificates, other external nodes will not be able to send messages within the corresponding domain. Moreover there exists the possibility to identify and remove the malicious behaving or defective nodes by revoking their certificates [7].

(Amirtahmasebi, Ex. 1019, pp. 20-21.)

356. A PHOSITA would have understood that these disclosures describe security-enhancing “*methods*” performed within a vehicle, including detecting an intrusion, verifying a digital signature, and excluding unauthorized nodes from network communication.

357. Therefore, Amirtahmasebi discloses “*a method*”.

[9a] in a vehicle comprising a plurality of on board computational components,

358. Claim limitation [9a] is substantially similar to limitation [1a] of claim 1. Claim [9a] requires “*in a vehicle comprising a plurality of on board computational components.*” Whereas claim [1a] requires “*a plurality of on board computational components.*”

359. As established in the analysis for [1a], Amirtahmasebi discloses that in-vehicle networks contain a plurality of ECUs, sensors, actuators, and other computing modules—each of which constitutes an “*on board computational component*.” (Amirtahmasebi, Ex. 1019, pp. 11, 24–25.)

360. Accordingly, I refer back to my analysis of this limitation in claim 1., limitation [1a] to establish that it is met by Amirtahmasebi.

[9b] a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components, and

361. Claim limitation [9b] is identical to limitation [1b] of claim 1. Therefore, I refer back to my analysis of claim 1, limitation [1b] to establish that a PHOSITA would have understood this limitation is disclosed by Amirtahmasebi.

362. Intentionally left blank.

[9c] a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance;

363. Claim limitation [9c] is substantially similar to limitation [1c] of claim 1. Claim [9c] requires “*a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance*.” Whereas claim [1c] requires “*a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure*.”

Compared with [1c], there [9c] recites “*identify*” instead of “*detect*”. In addition, [9c] further recites “*a possible security breach*” instead of “*a breach of the security measure.*” These minor differences do not alter the meaning of the limitation.

364. For the same reasons discussed for claim 1, limitation [1c], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

[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

365. Claim limitation [9d] is substantially similar to limitation [1d] of claim 1. The following marked up claim [9d] shows the differences between [9d] and [1d] “*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.*” These minor differences do not alter the meaning of the limitation.

366. For the same reasons discussed for claim 1, limitation [1d], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

[9e] 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,

367. Claim limitation [9e] is substantially similar to limitation [1e] of claim 1. The following marked up claim [9e] shows the differences between [9e] and [1e]

“[] *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.” These minor differences do not alter the meaning of the limitation.

368. As discussed above, 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....” (Amirtahmasebi, Ex. 1019, pp. 24, 51.) Further, Bosch teaches that the “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.” (Bosch, Ex. 1050, pp. 94-96.) A PHOSITA would have understood that Amirtahmasebi’s ECU is a microprocessor controller that operates to execute stored software programs, in accordance with Bosch.

369. For the same reasons discussed for claim 1, limitation [1e], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

[9f] 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:

370. Claim limitation [9f] is substantially similar to limitation [1f] of claim 1. The following marked up claim [9f] shows the differences between [9f] and [1f] “*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.*” These minor differences do not alter the meaning of the limitation.

371. As discussed in claim 1, limitation [1f], Amirtahmasebi discloses multiple forms of isolation, including: blocking communications from unauthenticated ECUs, denying access to external wireless nodes, routing messages through a gateway firewall, and using IDS countermeasures such as deactivation. (See ¶¶ 228-232.)

372. For the same reasons discussed for claim 1, limitation [1f], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

6. Dependent Claims 10-16

373. Claims 10-16 depend from claim 9, which I understand means that claims 10-16 require all of the limitations of claim 9 in addition to their additional limitations.

a. Claim 10

374. Claim 10 is largely duplicative of claim 2. To illustrate, the table below shows a side-by-side comparison of claims 2 and 10. Claim 10 is “marked up” to show the minor differences.

Claim 2	Claim 10
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,	10[pre]. The <u>method of claim 9</u> , 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,	identity theft (or MAC spoofing), network injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,
[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 instance, and a network probe, and	[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 instance, and a network probe, and
[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,	[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.	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.
--	--

10[pre] 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), net-work injection, caffe latte attack, or denial of a computer network and/or network-accessible resource,

375. Limitation 10[pre] is substantially similar to limitation 2[pre]. Given that claim 10[pre] encompasses claim 9 which discloses a “*method*,” the rest of the

language is identical to claim 2[pre]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

[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 instance, and a network probe, and

376. Limitation [10a] is identical to limitation [2a]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

[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:

377. Limitation [10b] is identical to limitation [2b]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

b. Claim 11

378. Claims 11 depends from claim 10, which I understand means that this claim requires all of the limitations of claim 10 in addition to its additional limitations. The combination of Amirtahmasebi and Bosch teaches all of the limitations of claim 10 as described above.

379. Claim 11 is largely duplicative of claim 3. To illustrate, the table below shows a side-by-side comparison of claims 3 and 11. Claim 11 is “marked up” to show the minor differences.

Claim 3	Claim 11
b. The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational component,	11[pre]. <u>The method of claim 10,</u> wherein the computational component affected by 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,	[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	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.

11[pre] The method of claim 10, wherein the computational component affected by the security breach instance is an on board computational component,

380. Limitation 11[pre] is substantially similar to limitation 3[pre]. Given that claim 11[pre] encompasses claim 9 which discloses a “method,” the rest of the language is identical to claim 3[pre]. Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by Amirtahmasebi.

[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

381. Limitation [11a] is identical to limitation [3a]. Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by Amirtahmasebi.

[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:

382. Limitation [11b] is identical to limitation [3b]. Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by Amirtahmasebi.

c. Claim 12

383. Claim 12 is largely duplicative of claim 4. To illustrate, the table below shows a side-by-side comparison of claims 4 and 12. Claim 12 is “marked up” to show the minor differences.

Claim 4	Claim 12
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	12[pre] . <u>The method of claim 10,</u> 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	containing the at least one on board computational component and
[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	[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.	selector, a remote control module, a computational module selector, an expansion module, an application, and a plug-in module.
--	--

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 vehicle containing the at least one on board computational component and

384. Limitation 12[pre] is substantially similar to limitation 4[pre]. Given that claim 12[pre] encompasses claim 9 which discloses a “*method*,” the rest of the language is identical to claim 4[pre]. Therefore, I refer back to my analysis of this limitation in claim 4 to establish that it is met by Amirtahmasebi.

[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:

385. Limitation [12b] is identical to limitation [4b]. Therefore, I refer back to my analysis of this limitation in claim 4 to establish that it is met by Amirtahmasebi.

d. Claim 13

386. Claim 13 is largely duplicative of claim 5. To illustrate, the table below shows a side-by-side comparison of claims 5 and 13. Claim 13 is “marked up” to show the minor differences.

Claim 5	Claim 13
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	13[pre] . <u>The method of claim 9,</u> 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
[5a] wherein the microprocessor executable network controller analyzes the security breach instance	[13a] wherein the microprocessor executable network controller detects a possible security breach

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.	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.
---	--

13[pre] 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

387. Limitation 13[pre] is substantially similar to limitation 5[pre]. Given that claim 13[pre] encompasses claim 9 which discloses a “*method*,” the rest of the language is identical to claim 5[pre]. Therefore, I refer back to my analysis of this limitation in claim 5 to establish that it is met by Amirtahmasebi.

[13a] 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:

388. Limitation [13a] is identical to limitation [5a]. Therefore, I refer back to my analysis of this limitation in claim 5 to establish that it is met by Amirtahmasebi.

e. Claim 14

389. Claim 14 is largely duplicative of claim 6. To illustrate, the table below shows a side-by-side comparison of claims 6 and 14. Claim 14 is “marked up” to show the minor differences.

Claim 6	Claim 14
6[pre] . The vehicle of claim 1, wherein the computational component affected by the security breach instance is an external computational device and	14[pre] . <u>The method of claim 9</u> , wherein the computational component affected by the security breach instance is an external computational device and
[6a] wherein the at least one on board computational component not affected by the security breach instance is isolated from the external	[14a] wherein the at least one on board computational component not affected by the security breach instance <u>isolation</u> is isolated from the

computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.	external computational device by the vehicular wireless network denying vehicular wireless network access by the external computational component.
---	--

14[pre] The method of claim 9, wherein the computational component affected by the security breach instance is an external computational device and

390. Limitation 14[pre] is substantially similar to limitation 6[pre]. Given that claim 14[pre] encompasses claim 9 which discloses a “*method*,” the rest of the language is identical to claim 6[pre]. Therefore, I refer back to my analysis of this limitation in claim 6 to establish that it is met by Amirtahmasebi.

[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:

391. Limitation [14a] is substantially similar to limitation [6a]. Claim [14a] recites the additional term of “*wherein the at least one on board computational component not affected by the security breach instance isolation is isolated from the external computational device[.]*”

392. As best understood, [14a] means “*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,*” wherein the addition of “*isolation*” is in error.

393. Therefore, limitation [14a] is identical to limitation [6a]. I refer back to my analysis of this limitation in claim 6 to establish that it is met by Amirtahmasebi.

394. Notwithstanding, even if claim [14a] is meant to recite “*the security breach instance isolation*”, the above difference is not substantial to the meaning of the claim. Therefore, I refer back to my analysis of this limitation in claim 6 to establish that it is met by the combination of Amirtahmasebi and Bosch.

f. Claim 15

395. Claim 15 is largely duplicative of claim 7. To illustrate, the table below shows a side-by-side comparison of claims 7 and 15. Claim 15 is “marked up” to show the minor differences.

Claim 7	Claim 15
[7]. The vehicle of claim 1, wherein at least one of the following is true about the isolation:	[15]. The <u>method of claim 9</u> , 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	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.	breach instance are blocked in whole or part.
--	--

[15] 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 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:

396. Limitation [15] is substantially similar to limitation [7]. Given that claim [15] encompasses claim 9 which discloses a “*method*,” the rest of the language is identical to claim [7]. Therefore, I refer back to my analysis of this limitation in claim 7 to establish that it is met by Amirtahmasebi.

g. Claim 16

397. Claim 16 is largely duplicative of claim 8. To illustrate, the table below shows a side-by-side comparison of claims 8 and 16. Claim 16 is “marked up” to show the minor differences.

Claim 8	Claim 16
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,	16[pre]. <u>The method of claim 9</u>, 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,
[8a] 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	[16a] 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	and/or internally to the perimeter network, and
[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,	[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.	WPAv 1, and/or WPAv2 protocols, and using end-to-end encryption.
---	---

16[pre] 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,

398. Limitation 16[pre] is substantially similar to limitation 8[pre]. Given that claim 16[pre] encompasses claim 9 which discloses a “*method*,” the rest of the language is identical to claim 8[pre]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

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

399. Limitation [16a] is identical to limitation [8a]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

[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 MACID 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.

400. Limitation [16b] is identical to limitation [8b]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

7. Independent Claim 17

a. Claim 17

401. Independent claim 17 is largely duplicative of independent claim 1. To illustrate, the table below shows a side-by-side comparison of claims 1 and 17. Claim 17 is “marked up” to show the minor differences.

Claim 1	Claim 17
1[pre]. A vehicle, comprising:	17[pre]b <u>In</u> a vehicle comprising
[1a] 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	[17b] <u>a non-transient, tangible computer readable medium comprising</u> a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components and
[1c] a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,	[17c] a microprocessor executable network controller <u>on board a selected vehicle that, when executed,</u> detects an instance of a breach of the security measure,
[1d] (ii) determine whether a computational component affected	[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	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,
[1e] (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	[17e] 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

(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	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 <u>the</u> security measure
(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,	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 <u>the</u> security measure,

[1f] 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	[17f] 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 <u>the</u> security measure, (2) directing communications to and from the computational component affected by the instance of a breach of <u>the</u> 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 <u>the</u> security measure, and
--	--

(4) activating a second security mechanism in response to the instance of a breach of a security measure.	(4) activating a second security mechanism in response to the instance of a breach of <u>the</u> security measure.
---	--

17[pre] In a vehicle comprising

402. Limitation 17[pre] is substantially similar to limitation 1[pre]. Therefore, I refer back to my analysis of these limitations in claim 1 to establish that it is met by Amirtahmasebi.

17[a] a plurality of on board computational components,

403. Limitation 17[a] is substantially similar to limitation 1[a]. Therefore, I refer back to my analysis of these limitations in claim 1 to establish that it is met by Amirtahmasebi.

[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

404. Compared with claim [1b], claim [17b] requires the additional limitation of “*a non-transient, tangible computer readable medium.*”

405. Amirtahmasebi discloses non-transient, tangible computer readable medium. Specifically, Amirtahmasebi discloses various electronics control units (ECUs) controlled by firmware in charge of communication and performing specific tasks, and a secure storage for storing sensitive a valuable information:

Modern vehicles consist of Electronic Control Units (ECUs) which are in charge of controlling electronic components in the vehicle. Apart from the hardware, each ECU is controlled by firmware which is in charge of communication and performing specific tasks. ECUs perform different tasks such as engine control, entertainment units, mirror controls, etc. which need different requirements in terms of speed and criticality of message transfer. Since ECUs must communicate their information with each other and also receive data from sensors and controls, a network bus must be designed to transfer the generated information to the proper component. This structure is the basis for the in-vehicle network, which is used extensively in vehicles these days.

(Amirtahmasebi, Ex. 1019, p. 24.)

Vehicular networks perform critical functions and must be secured against malicious behavior. As mentioned before, unauthorized access can result in serious financial or physical damage to the vehicle or its passengers. Therefore, the vehicular network framework must be designed with great care and should meet several design challenges. Although security considerations might have different perspectives, there are general security requirements which are common in many embedded systems [27]:

...

- Secure storage, sensitive and valuable information must be securely stored in order to be protected against unauthorized access and requests.

(Amirtahmasebi, Ex. 1019, p. 51.)

406. Bosch also teaches the “microprocessor contains the controller . . . which ensures implementation of the commands stored in the program memory.” (Bosch, Ex. 1050, p. 94-96.) A PHOSITA would have understood that an ECU is a non-transient, tangible microcomputer that includes readable program memory (“*readable medium*”).

407. A PHOSITA would have understood that firmware and secure storage reside on “*non-transient, tangible computer readable media*” (e.g., flash memory, EEPROM) within each ECU. The firmware and persistent memory implement communication protocols and security functions, including those associated with gateways, firewalls, and IDS modules.

408. The remainder of limitation 17[b] is substantively identical to limitation 1[b], which requires a “*first security mechanism*” to “*enforce a security measure*” and “*form a perimeter network*.” As described in claim 1[b], Amirtahmasebi discloses integrated gatekeepers and gateway ECUs having firewall mechanisms.

409. Accordingly, I refer back to my analysis of limitation 1[b] to establish that Amirtahmasebi teaches the remainder of claim 17[b].

[17c] a microprocessor executable network controller on board a selected vehicle that, when executed, detects an instance of a breach of the security measure,

410. Claim limitation [17c] is substantially similar to limitation [1c] of claim 1. Claim [9c] requires “*a microprocessor executable network controller on board a selected vehicle that, when executed, detects an instance of a breach of the security measure*”, whereas claim [1c] requires “*a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure.*”

411. As explained in the analysis of claim 1[c], Amirtahmasebi discloses gateway ECUs equipped with microprocessors that execute firewall logic, perform MAC/digital-signature verification, and analyze IDS patterns to identify malicious or malformed messages. A PHOSITA would have recognized that these operations constitute the detection of a breach of a security measure.

412. Bosch also teaches the “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.” (Bosch, Ex. 1050, pp. 94-96.) A PHOSITA would have understood that the controller would operate to execute the stored software programs like those disclosed by Amirtahmasebi.

413. Accordingly, I refer back to my analysis of limitation 1[c] to establish that Amirtahmasebi teaches the remainder of claim 17[c].

[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,

414. Limitation [17d] is identical to limitation [1d]. As explained in that analysis, Amirtahmasebi discloses architectures—central, distributed, and semi-central—in which ECUs operate independently and can be functionally isolated when compromised.

415. Therefore, I refer back to my analysis of this limitation [1d] in claim 1 to establish that it is met by Amirtahmasebi.

[17e] 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 onboard 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,

416. Claim limitation [17e] is substantially similar to limitation [1e] of claim 1. Compared with claim [1e], claim [17e] differs in a few antecedents “*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*”. Both limitations require performing one or both forms of isolation—isolating the affected ECU from the unaffected component or vice versa—once the system determines that isolation is possible. These minor differences do not alter the meaning of the limitation.

417. For the same reasons discussed for claim 1, limitation [1e], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

[17f] 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 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:

418. Claim limitation [17f] is substantially similar to limitation [1f] of claim 1. Compared with claim [1f], claim [17f] differs in a few antecedents “*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 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.*” These minor differences do not alter the meaning of the limitation.

419. As discussed in claim 1, limitation [1f], Amirtahmasebi discloses multiple forms of isolation, including: blocking communications from unauthenticated ECUs, denying access to external wireless nodes, routing messages through a gateway firewall, and using IDS countermeasures such as deactivation.

420. For the same reasons discussed for claim 1, limitation [1f], a PHOSITA would have understood Amirtahmasebi discloses this limitation.

8. Dependent Claims 18-24

421. Claims 18-24 depend from claim 17, which I understand means that claims 18-24 require all the limitations of claim 17 in addition to their own limitations.

a. Claim 18

422. Claim 18 is largely duplicative of claim 2. To illustrate, the table below shows a side-by-side comparison of claims 2 and 18. Claim 18 is “marked up” to show the minor differences.

Claim 2	Claim 18
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	18[pre]. The <u>computer readable medium of claim 17</u> , 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,	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 <u>and</u>
[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 instance, and a network probe, and	[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 instance, and a network probe, and
[2b] wherein the first security mechanism is one or more of:	[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.	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.
---	---

18[pre] 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

423. Limitation 18[pre] is substantially similar to limitation 2[pre]. Given that claim 18[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium,*” the rest of the language is identical to claim 2[pre]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

[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 instance, and a network probe, and

424. Limitation [18a] is identical to limitation [2a]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

[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.

425. Limitation [18b] is identical to limitation [2b]. Therefore, I refer back to my analysis of this limitation in claim 2 to establish that it is met by Amirtahmasebi.

b. Claim 19

426. Claim 19 is largely duplicative of claim 3. To illustrate, the table below shows a side-by-side comparison of claims 3 and 19. Claim 19 is “marked up” to show the minor differences.

Claim 3	Claim 19
3[pre]. The vehicle of claim 2, wherein the computational component affected by the security breach instance is an on board computational component,	19[pre]. The <u>computer readable medium of claim 18</u> , wherein the computational component affected by the security breach instance is an on board computational component,
[3a] wherein the at least one board computational component is one or	[19a] wherein the at least one on board computational component is

more of an on-board sensor, processing module, software application, expansion module, critical device, non-critical device, and cellular upgrade module, and	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.	[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.

19[pre] The computer readable medium of claim 18, wherein the computational component affected by the security breach instance is an on board computational component,

427. Limitation 19[pre] is substantially similar to limitation 3[pre]. Given that claim 19[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium,*” the rest of the language is identical to claim 3[pre].

Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by Amirtahmasebi.

[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

428. Limitation [19a] is identical to limitation [3a]. Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by Amirtahmasebi.

[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.

429. Limitation [19b] is identical to limitation [3b]. Therefore, I refer back to my analysis of this limitation in claim 3 to establish that it is met by the combination of Amirtahmasebi and Bosch.

c. Claim 20

430. Claim 20 is largely duplicative of claim 4. To illustrate, the table below shows a side-by-side comparison of claims 4 and 20. Claim 20 is “marked up” to show the minor differences.

Claim 4	Claim 20

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	20[pre]. <u>The computer readable medium of claim 18,</u> 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
[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	[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.	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.
--	--

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 vehicle containing the at least one on board computational component and

431. Limitation 20[pre] is substantially similar to limitation 4[pre]. Given that claim 20[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium*,” the rest of the language is identical to claim 4[pre]. Therefore, I refer back to my analysis of this limitation in claim 4 to establish that it is met by Amirtahmasebi.

[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.

432. Limitation [20a] is identical to limitation [4a]. Therefore, I refer back to my analysis of this limitation in claim 4 to establish that it is met by Amirtahmasebi.

d. Claim 21

433. Claim 21 is largely duplicative of claim 5. To illustrate, the table below shows a side-by-side comparison of claims 5 and 21. Claim 21 is “marked up” to show the minor differences.

Claim 5	Claim 21
5[pre]. The vehicle of claim 1,	21[pre]. <u>The computer readable medium of claim 17,</u>

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	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
[5a] 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.	[21a] wherein the microprocessor executable network controller <u>detects a possible</u> 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.

21[pre] 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

434. Limitation 21[pre] is substantially similar to limitation 5[pre]. Given that claim 21[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium,*” the rest of the language is identical to claim 5[pre]. Therefore, I refer back to my analysis of this limitation in claim 5 to establish that it is met by Amirtahmasebi.

[21a] 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.

435. Limitation [21a] is identical to limitation [5a]. Therefore, I refer back to my analysis of this limitation in claim 5 to establish that it is met by Amirtahmasebi.

e. Claim 22

436. Claim 22 is largely duplicative of claim 6. To illustrate, the table below shows a side-by-side comparison of claims 6 and 22. Claim 22 is “marked up” to show the minor differences.

Claim 6	Claim 22

6[pre]. The vehicle of claim 1, wherein the computational component affected by the security breach instance is an external computational device and	22[pre]. <u>The computer readable medium of claim 17,</u> wherein the computational component affected by the security breach instance is an external computational device and
[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.	[22a] 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.

22[pre] The computer readable medium of claim 17, wherein the computational component affected by the security breach instance is an external computational device and

437. Limitation 22[pre] is substantially similar to limitation 6[pre]. Given that claim 22[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium*,” the rest of the language is identical to claim 6[pre]. Therefore, I refer back to my analysis of this limitation in claim 6 to establish that it is met by Amirtahmasebi.

[22a] 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.

438. Limitation [22a] is identical to limitation [6a]. Therefore, I refer back to my analysis of this limitation in claim 6 to establish that it is met by Amirtahmasebi.

f. Claim 23

439. Claim 23 is largely duplicative of claim 7. To illustrate, the table below shows a side-by-side comparison of claims 7 and 23. Claim 23 is “marked up” to show the minor differences.

Claim 7	Claim 23
7[pre]. The vehicle of claim 1,	23[pre]. <u>The computer readable medium of claim 17,</u>

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	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.	instance and the computational component affected by the security breach instance are blocked in whole or part.
---	---

[23] 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:

440. Limitation [23] is substantially similar to limitation [7]. Given that claim [23] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium*,” the rest of the language is identical to claim [7]. Therefore, I refer back to my analysis of this limitation in claim 7 to establish that it is met by Amirtahmasebi.

g. Claim 24

441. Claim 24 is largely duplicative of claim 8. To illustrate, the table below shows a side-by-side comparison of claims 8 and 24. Claim 24 is “marked up” to show the minor differences.

Claim 8	Claim 24
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,	24[pre]. <u>The computer readable medium of claim 17,</u> 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,

[8a] 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	[24a] 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
[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	[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 other 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.	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.
--	--

24[pre] 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,

442. Limitation 24[pre] is substantially similar to limitation 8[pre]. Given that claim 24[pre] encompasses claim 17 which discloses a “*non-transient, tangible computer readable medium*,” the rest of the language is identical to claim 8[pre]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

[24a] 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

443. Limitation [24a] is identical to limitation [8a]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

[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.

444. Limitation [24b] is identical to limitation [8b]. Therefore, I refer back to my analysis of this limitation in claim 8 to establish that it is met by Amirtahmasebi.

9. Rationale to Combine

445. It would have been obvious to a PHOSITA at the time of the invention to combine the vehicle network security system disclosed in Amirtahmasebi with the known electronic control unit, including a microprocessor and memory, as disclosed in Bosch, e.g., to improve a similar device in the same way, e.g., to reduce cost for a high-volume component. A PHOSITA would have understood that Amirtahmasebi and Bosch are complementary technologies that are combinable.

446. Amirtahmasebi and Bosch are from the same field – vehicle network systems that include controllers or electronic control units (ECUs). Amirtahmasebi classifies ECUs by criticality and mentions a central security module as part of the main control unit for managing security operations.

Modern vehicles consist of Electronic Control Units (ECUs) which are in charge of controlling electronic components in the vehicle. Apart from the hardware, each ECU is controlled by firmware which is in charge of communication and performing specific tasks. ECUs perform different tasks such as engine control, entertainment units, mirror controls, etc. which need different requirements in terms of speed and criticality of message transfer. Since ECUs must communicate their information with each other and also receive data from sensors and controls, a network bus must be designed to transfer the generated information to the proper component. This structure is the basis for the in-vehicle network, which is used extensively in vehicles these days.

(Amirtahmasebi, Ex. 1019, p. 24.)

447. A PHOSITA would have understood the Bosch Automotive Handbook (Ex. 1050) has been published for decades and is now in multiple editions, each updated to reflect advancements in automotive technology. It is known to a PHOSITA that Robert Bosch GmbH is a global leader in automotive systems and components and published the Automotive Handbook to provide practitioners in the field with comprehensive disclosure of many automotive fundamentals.

448. A PHOSITA would have understood the Bosch Handbook is a well-known and often cited reference in the automotive field, relied upon by engineers, researchers, and manufacturers worldwide for technical guidance on vehicle systems and electronics covering virtually every major aspect of automotive engineering, including:

- Electronic Control Units (ECUs) and their architecture.
- Microprocessors, CPUs, and microcomputers for signal processing and control.
- Data processing and communication networks in vehicles.
- Powertrain, safety systems, infotainment, and emerging technologies.

449. While Amirtahmasebi describes ECUs generally by function and criticality, it does not expressly provide well-known details about the internal processing components required to execute firmware.

450. While such knowledge of function and design would have been known to a PHOSITA in the field of automotive engineering, the Bosch Handbook expressly provides the details of what a PHOSITA would have understood with regards to the architecture of ECUs, including microcomputers, CPUs, and microprocessors. A PHOSITA implementing Amirtahmasebi's system would have understood—or been instructed by the teachings of the Bosch Handbook—well-known ECUs existed for performing the tasks described by Amirtahmasebi. As

shown below, Bosch details the design and operation of existing ECUs used within automotive applications:

ECUs developed for use in motor vehicles all have a similar design. Their structure can be subdivided in the conditioning of input signals, the logic processing of these signals in the microcomputer, and the output of logic and power levels as regulation or control signals.

(Bosch, Ex. 1050, p. 1065.)

A microcomputer consists of:

- Microprocessor serving as CPU (central processing unit). . . .
- Input and output units (I/O) . . .
- Program memory . . .
- Data memory . . .

(Bosch, Ex. 1050, p. 94.)

The main components of a microcomputer are normally combined as separate components on printed-circuit boards. “Single-chip” computers are becoming used more and more for simpler tasks, e.g., internet access in wireless communications, which is a growing trend, or functions integrated on a single silicon chip (SoC: System on a chip). The performance of these high integrations systems is limited by the relatively small amount of RAM which can be accommodated at reasonable expense on the chip.

(Bosch, Ex. 1050, p. 96.)

The microprocessor represents the integration of a computers central processing unit on a single chip. Microprocessor design seeks to avoid individualization in the face of large-scale integration, and the units can be programmed to meet the varied requirements associated with specific operation conditions.

(Bosch, Ex. 1050, p. 94.)

451. A PHOSITA would have been motivated to use a microprocessor (as taught by the Bosch Handbook) to execute software code implementing Amirtahmasebi vehicle network system to “avoid individualization in the face of large-scale integration,” as described in Bosch, to provide a common microprocessor for high-volume automotive application, for relatively simple tasks like discovering mobile devices and refreshing content on a display, to reduce the piece-price of the microprocessor. (Bosch, Ex. 1050, p. 94.)

452. Amirtahmasebi also identifies ECUs as essential for vehicular networks and security but does not expressly disclose their internal structure. Bosch discloses the well-known design of ECUs based on microcomputers and CPUs. A PHOSITA would have predictably combined Amirtahmasebi’s functional requirements (ECUs controlling engine, safety, infotainment) with Bosch’s known architecture (microprocessor, memory, I/O) to create a physical, workable ECU. This is routine engineering: applying standard microcomputer architecture to implement ECUs

described in Amirtahmasebi. The result—functional ECUs capable of executing firmware.

453. By 2010, a PHOSITA would have understood automotive systems demanded sophisticated control and security features. Amirtahmasebi addresses these high-level requirements (networking, security modules), while Bosch provides how established and well-known automotive ECUs could be used to provide such solutions. A PHOSITA would have been motivated to consult Bosch for the well-known and proven ECU architectures. A PHOSITA would have relied on Bosch's teachings regarding microcomputers and CPUs given they teach well-known industry standards regarding processing power in modern automotive electronics.

454. Amirtahmasebi identifies vulnerabilities and security challenges within automotive applications, but Amirtahmasebi does not expressly disclose how ECUs should be architected to meet real-time requirements. Bosch provides known and obvious solutions regarding microcomputers with CPUs, memory, and peripheral interfaces for signal conditioning and control. A PHOSITA would have recognized that implementing Amirtahmasebi's security teachings and ECU functions with Bosch's disclosure of automotive ECU and microprocessor design is nothing more than applying a known solution for implementation in a known problem.

455. A PHOSITA would have known how to implement Amirtahmasebi vehicle network strategies on a microprocessor to achieve predictable results, e.g.,

cost reduction. As explained by Bosch, “[w]ith modern semiconductor technology [in 2004], powerful microcomputers can be integrated on relatively few chips together with their accompanying program and data memories, and special peripheral circuits designed specifically for real-time applications.” (Bosch, Ex. 1050, p. 1064.) As stated above, Bosch is a widely recognized authoritative source for automotive engineering fundamentals. A PHOSITA tasked with implementing Amirtahmasebi’s concepts would have naturally referred to Bosch for detailed ECU architecture. Consulting the Bosch Handbook is consistent with common sense and industry practice because Bosch provides standardized information on microprocessors, CPUs, and ECU structure that Amirtahmasebi does not expressly disclose. The combination of these two references would be an ordinary and routine solution to implementing the teachings of Amirtahmasebi.

B. Ground 2 – The Combination of Spaur and Peirce Teaches all of the Limitations of Claims 1, 9, and 17

10. Independent Claim 1

456. I have given each of the limitations of claim 1 a unique numerical identifier, as shown in the chart below:

U.S. Patent No. 9,173,100	
1[pre].	A vehicle, comprising:
[1a]	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

[1c] a microprocessor executable network controller operable to (i) detect 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

[1e] (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 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,

[1f] 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.

1[pre]. A vehicle, comprising:

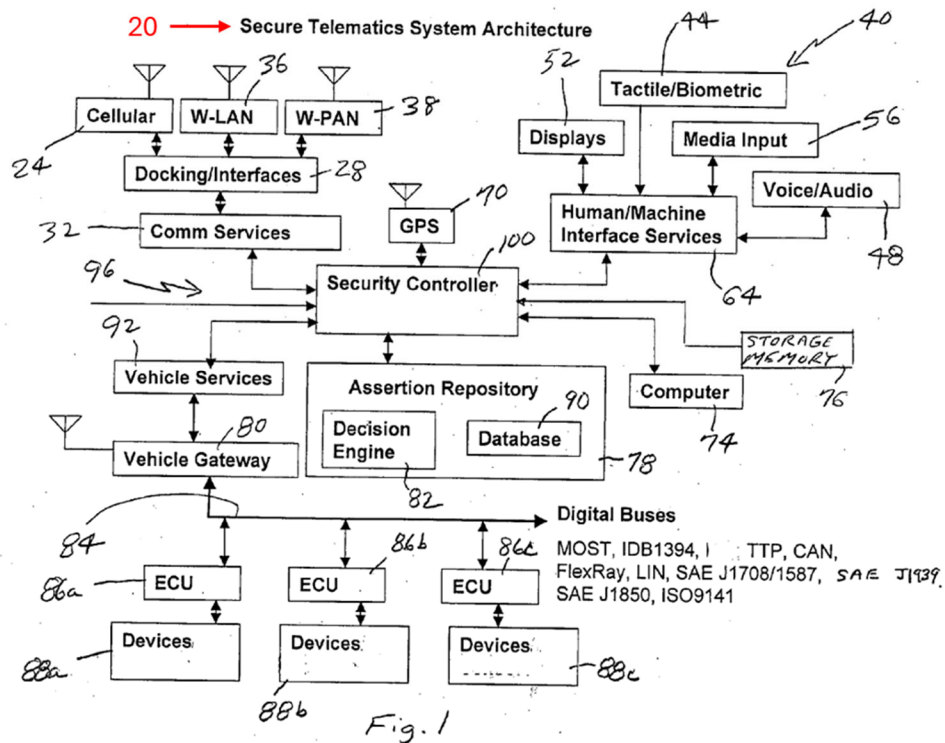
457. Spaur discloses a “system and method . . . provided for utilizing resources, including proprietary resources in a vehicle.” (Spaur, Ex. 1020, [0006].)

Spaur further discloses that “[t]he proprietary resources can include one or more of the following: vehicle buses, vehicle devices, interfaces, subsystems, storage memory in the vehicle, applications executed in the vehicle, connectivity hardware/software and communication devices.” (Spaur, Ex. 1020, [0007].)

458. Thus, the combination of Spaur and Peirce teaches a “*vehicle*.”

[1a] a plurality of on board computational components:

459. Spaur discloses, with reference to Figure 1, a “telematics secure system 20” that includes multiple subsystems and apparatuses “for providing communications to and from the vehicle.” (Spaur, Ex. 1020, [0027].)



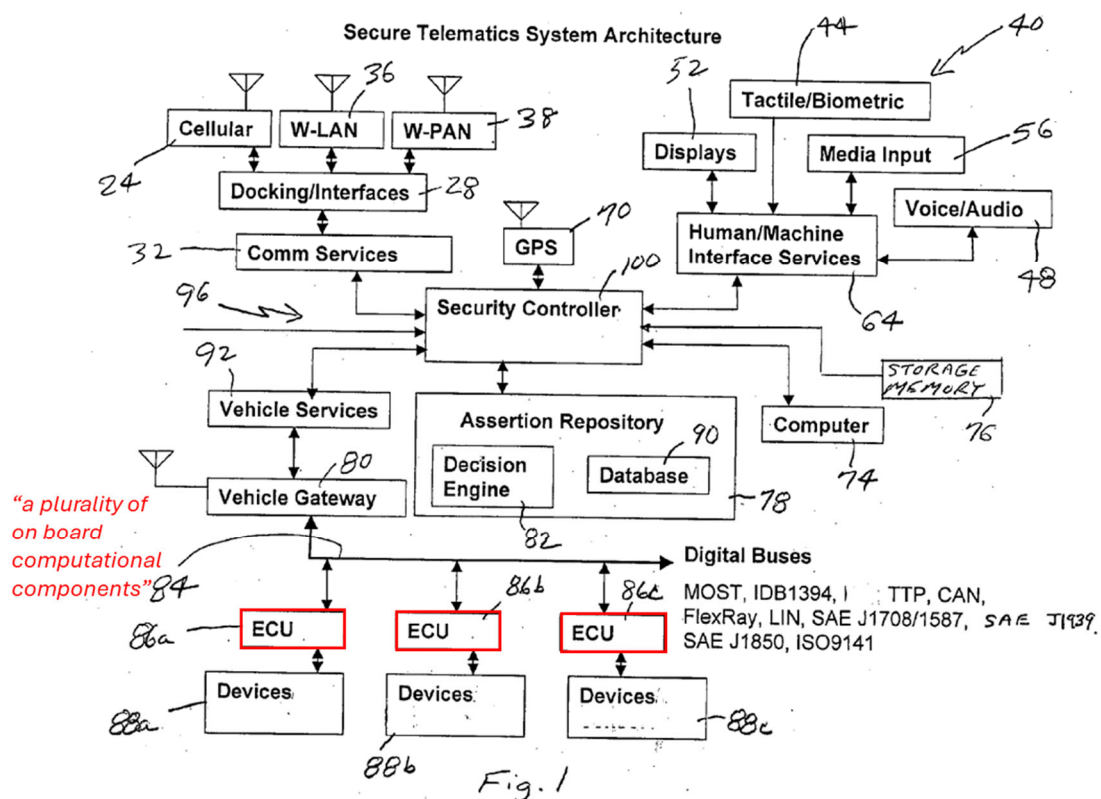
Spaur, Ex. 1020, Figure 1 (Annotated)

460. Spaur discloses that additional resources are found in the vehicle, including multiple vehicle buses “84” that communicate with various ECUs “86” that include different subsystems:

Additional resources found in the vehicle can include a vehicle gateway 80. The vehicle gateway 80 conventionally communicates with one or more vehicle buses 84 to which one or more vehicle devices 88 are connected or communicate with using electronic control units (ECUs) 86. Each ECU 86 interfaces one or more of the digital buses 84 with a

particular vehicle device 88 and each such ECU can be individually designated as 86a, 86b, 86c. . . . The ECU 86 can include one more of a number of different control subsystems such as a body control, a chassis control, an engine control, a transmission control and a telematics control.

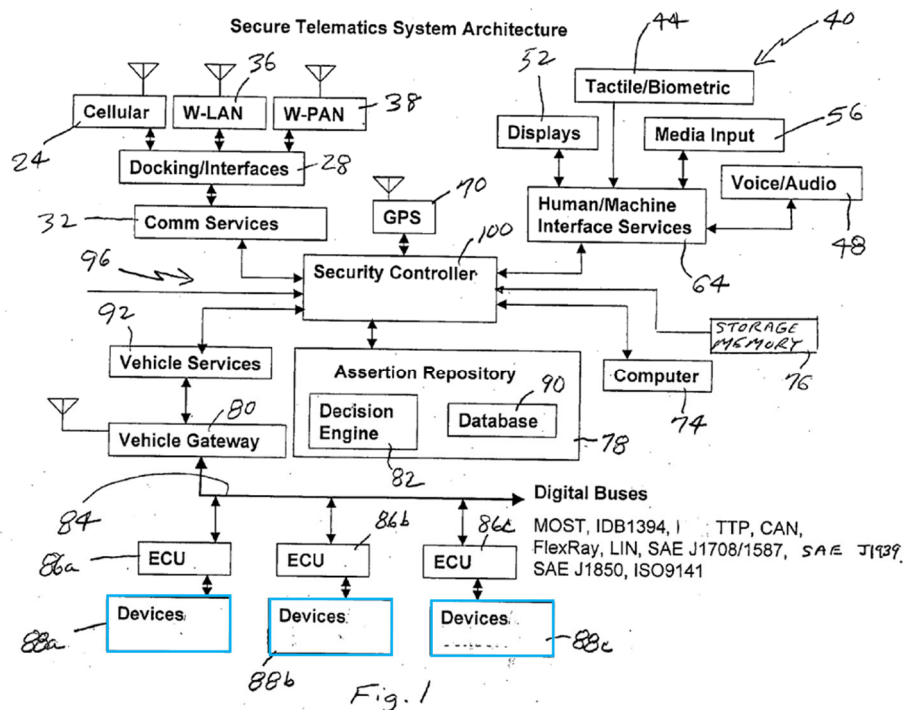
(Spaur, Ex. 1020, [0034].)



Spaur, Ex. 1020, Figure 1 (Annotated)

461. 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).” (Spaur, Ex. 1020, [0034].)



Spaur, Ex. 1020, Figure 1 (Annotated)

462. A PHOSITA would have understood that Spaur’s disclosure of the ECUs 86 including various subsystems within a vehicle (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. (Spaur, Ex. 1020, [0034].) A PHOSITA would have further understood that for the ECUs 86 to communicate with the vehicle devices 88, which include various sensors and actuator systems (e.g., engine monitor, temperature sensor), the ECUs 86 receive, interpret, and act upon data

originating from the vehicle devices 88. (Spaur, Ex. 1020, [0034].) Such data processing and control operations are readily understood functions of “*on board computational components*.”

463. Additionally, because many of the vehicle devices 88 themselves generate, preprocess, or condition sensor data (e.g., monitoring engine parameters, detecting temperatures or pressures), a PHOSITA would have also recognized that these devices 88 perform embedded processing functions and therefore may likewise qualify as “*on board computational components*.”

464. Thus, the combination of Spaur and Peirce teaches a plurality of “ECUs 86” which satisfy the recited “*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

465. As stated above in [1a], Spaur discloses that “[t]he vehicle gateway 80 conventionally communicates with one or more vehicle buses 84 to which one or more vehicle devices 88 are connected or communicate with using electronic control units (ECUs) 86.” (Spaur, Ex. 1020, [0034].) Spaur further explains that the vehicle gateway 80 mediates access to the vehicle buses 84, which indirectly governs the ability of other components to communicate with the connected vehicle devices 88:

The vehicle gateway 80 controls access to and use of the vehicle buses 84. Relatedly, by means of the vehicle gateway 80, commands can be

sent on one or more buses 84 to one or more selected devices 88 that are connected to the particular bus or buses 84. The vehicle gateway 80 can also have wireless communication interfaces, as well as directly receive remote wireless input(s) by means of an antenna or the like. Such input(s) could be used to supply control signals to vehicle devices 88 including those used in supporting the locking/unlocking of vehicle doors and remote vehicle engine starting.

(Spaur, Ex. 1020, [0034].)

466. Spaur discloses that “[t]he vehicle buses 84 can be one or more digital buses and can include known buses identified as MOST, IDB 1394, TTP, CAN, FlexRay, LIN, SAE J1708/1587, SAE J1939, SAE J1850, ISO9141.” (Spaur, Ex. 1020, [0034].)

467. Spaur further discloses that the vehicle gateway 80 is “[i]n communication . . . [with] a vehicle services module 92” to support secure communication within the vehicle network (e.g., by arbitrating communications on vehicle buses 84, enabling wireless communication, enforcing rules related to communications with the vehicle gateway 80):

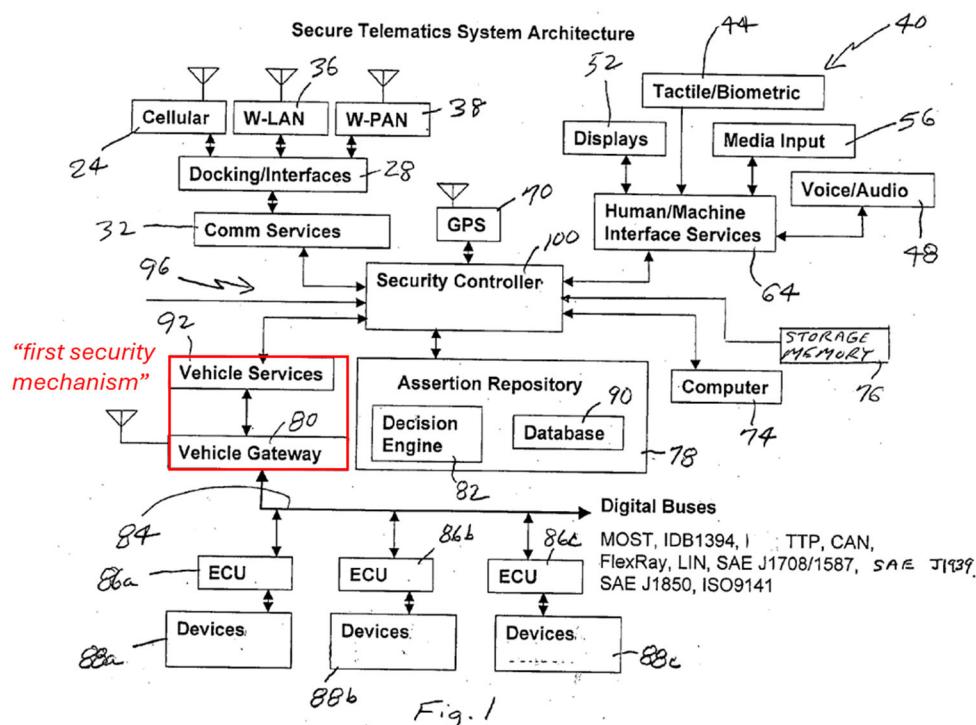
In communication with the vehicle gateway 80 is a vehicle services module 92. Similar to the communication services module 32 and the human/machine interface services module 64, communications relative to the vehicle gateway 80 pass through the vehicle services module 92 in order to control access to vehicle gateway controlled vehicle buses 84 and vehicle devices 88. The functions of the vehicle services module

92 include supporting secure communications on one or more vehicle or telematics buses 84, contributing to the enablement of intra-vehicle wireless communications (e.g. PAN, such as Bluetooth), arbitrating vehicle bus access for outgoing requests, providing fault notification related to vehicle gateway operations, monitoring and logging usage of the vehicle gateway 80, vehicle buses 84 and/or vehicle devices 88, enforcing rules related to uses of such resources that communicate with the vehicle gateway 80, and managing tools related to providing security, such as access keys and certificates approving access.

(Spaur, Ex. 1020, [0035].)

468. A PHOSITA would have understood that Spaur's disclosure of the vehicle gateway 80 and the vehicle services module 92 coordinating the control and mediation of communications within the vehicle network, indicates that these components collectively provide and enforce security within the system. Spaur explains that "communications relative to . . . the vehicle buses 84 and/or vehicle devices 88" first "pass through the vehicle service module 92" and the vehicle gateway 80, where the vehicle service module 92 enforces security policies (e.g., controlling access, supports secure communications, arbitrates bus access, enforces rules, manages access keys and certificates, logs and monitors gateway usage), while the gateway 80 mediates and governs the actual transmission of commands to the vehicle busses 84, the ECUs 86, and the devices 88. (Spaur, Ex. 1020, [0035].) Thus, a PHOSITA would have recognized that these components collectively enforce

“*security measure[s]*” (e.g., authenticating communication, access control, rule-based command filtering), and therefore operate as a unified “*security mechanism*” that regulates and protects vehicle network communications.



Spaur, Ex. 1020, Figure 1 (Annotated)

469. My opinion is supported by Claims 27-28 of Spaur, which specifies that the (1) vehicle gateway 80 and vehicle services module 92; (2) comm services module 32; and (3) HMI services module 64 provide security functionality by enforcing usage rules for the first vehicle bus and associated devices, monitoring and logging usage, providing fault notifications, and supporting security on the first vehicle bus (Spaur, Ex. 1020, Claims 27-28.) This demonstrates that one or all three of these service modules (i.e., 92, 32, 64) act as a “*first security mechanism*” to

enforce “*security measures*”—such as usage rules—primarily for the vehicle bus and its devices, thereby protecting vehicle electronics (e.g., ECUs, sensors) from external, untrusted communications, including inter-vehicle communications and those from a key FOB or FOTA. A PHOSITA would also have understood that the logical “*perimeter network*” could be formed around and include external devices, such as a cell phone connected to the vehicle (e.g., using comm services 32). Or the logical “*perimeter network*” could be formed around one or more ECUs (using vehicle gateway 80 and services 92) to protect a specific ECU 86 or all ECUs within the vehicle.

470. For instance, Claim 28 discloses the security functionality of the vehicle gateway and vehicle services module as including: (1) enforcing one or more usage rules associated with said first vehicle bus and said vehicle devices, (2) monitoring and logging usage related to said first vehicle bus and said vehicle devices; (3) providing fault notification related to said first vehicle bus and said vehicle devices and (4) supporting security on said first vehicle bus.

28. A system of claim 23 further including a vehicle gateway and a vehicle services module, wherein said first bus includes one or more vehicle buses including a first vehicle bus communicating with said vehicle gateway that allows access to information obtained from vehicle devices in communication with said vehicle bus, said vehicle services module involved with at least one of the following functions:

managing said first certificate and at least a first key related to use of one or more vehicle devices including said first vehicle device communicating with said first vehicle bus; enforcing one or more usage rules associated with said first vehicle bus and said vehicle devices; monitoring and logging usage related to said first vehicle bus and said vehicle devices; providing fault notification related to said first vehicle bus and said vehicle devices; upgrading said first vehicle bus access for outgoing requests; and supporting security on said first vehicle bus.

(Spaur, Ex. 1020, Claim 28.)

471. Alternatively, Spaur discloses that the communication services module 32 operates as a security-enforcing component. Spaur states that communication services module 32 “can be software comprised of executable program code that protects and arbitrates access to communication resources in or involved with the vehicle.” (Spaur, Ex. 1020, [0028].) Spaur explains that the “fundamental functions” of the communication services module 32 include “supporting communication paths to the Internet,” “contributing to secure communications on one or more buses found in the vehicle[,]” “monitoring and logging usage of communications-related resources,” “enforcing usage rules for communication resources,” and “managing tools involved with security control, including authentication and authorization related to usage of links and/or resources associated with the vehicle.” (Spaur, Ex. 1020, [0028].) Spaur further teaches that external wireless systems (e.g., wireless LAN 36, wireless PAN 38) communicate with the vehicle through interfaces whose

transmissions are “properly arbitrated and protected using the communication services module 32.” (Spaur, Ex. 1020, [0028].) A PHOSITA would have understood that because the communication services module 32 executes program code to protect, arbitrate, authenticate, and authorize external communications before they reach internal vehicle buses, it performs security-enforcing functions and therefore may form part of the “*security mechanism*” that enforces the “*security measure[s]*” governing access to the in-vehicle network.

472. Claim 26 of the patent even discloses the communication services module is not only designed to protect and arbitrate access to a plurality of proprietary resources (e.g., GPS system, vehicle memory, sensors for the vehicle devices), but this service module also performs at least some of the following security related functions: (1) managing at least said first certificate and at least a first key; (2) enforcing one or more usage rules for said first proprietary resource; monitoring and logging usage associated with said first proprietary resource; providing fault notification; (3) supporting communications outside the vehicle, including over the Internet; and (4) supporting communication on said first bus. This claim helps emphasize that the communication services module 32 operates as a “*security mechanism*” to enforce “*security measures*” (e.g., usage rules) primarily related to the computing devices located within the vehicle and which communicate on the vehicle bus.

26. A system of claim 23 further including at least one of: a communication services module in communication with at least said first proprietary resource that is involved with communications, said communication services module for use in protecting and arbitrating access to said first proprietary resource and performing at least some of the following functions: managing at least said first certificate and at least a first key; enforcing one or more usage rules for said first proprietary resource; monitoring and logging usage associated with said first proprietary resource; providing fault notification; supporting communications outside the vehicle, including over the Internet; and supporting communication on said first bus.

(Spaur, Ex. 1020, Claim 26.)

473. As another alternative, Spaur discloses that the human/machine interface services module 64 can also function as a security-enforcing component. (Spaur, Ex. 1020, [0030].) Spaur explains that the HMI services module 64 “is similar . . . to the communication services module 32” and “support[s] secure communications on one or more of the vehicle buses,” “provides fault notification,” “monitor[s] and log[s] resource usage,” “polices usage rules,” and “manag[es] tools involved with verifying proper usage” of operator-related subsystems. (Spaur, Ex. 1020, [0030].) Spaur further teaches that HMI services 64 processes user-originating inputs such as “tactile/biometric input 50,” “voice/audio inputs 48,” “displays 52,” and “media input 56,” and that these inputs are routed through the HMI services

module 64 before being provided to other vehicle components. (Spaur, Ex. 1020, [0029].) A PHOSITA would have understood that because HMI services 64 process, route, and regulate user-initiated signals before they are communicated to ECUs or vehicle resources, it performs security-enforcing functions and may also form part of the “*security mechanism*” that enforces the “*security measure[s]*” governing which user-originated commands or data may access the in-vehicle network.

474. Claim 27 of the patent even discloses the human/machine interface services module 64 performs at least some of the following security related functions: (1) managing said first certificate and at least a first key related to use of said first display; (2) enforcing one or more usage rules associated with said first display; and (3) providing fault notification related to said first display and supporting communication on said first bus. This claim helps emphasize that the human/machine interface services module 64 operates as a “*security mechanism*” to enforce “*security measures*” (e.g., usage rules) primarily related to the computing devices located within the vehicle and which communicate on the vehicle bus.

27. A system of claim 23 further including a human/machine interface services module in communication with said security controller that protects and arbitrates access to said first display and performs at least some of the following functions: managing, responding to, handling or otherwise being involved with: (a) tactile inputs such as steering wheel controls, buttons, switches, (b) audio and voice recognition, text-to-

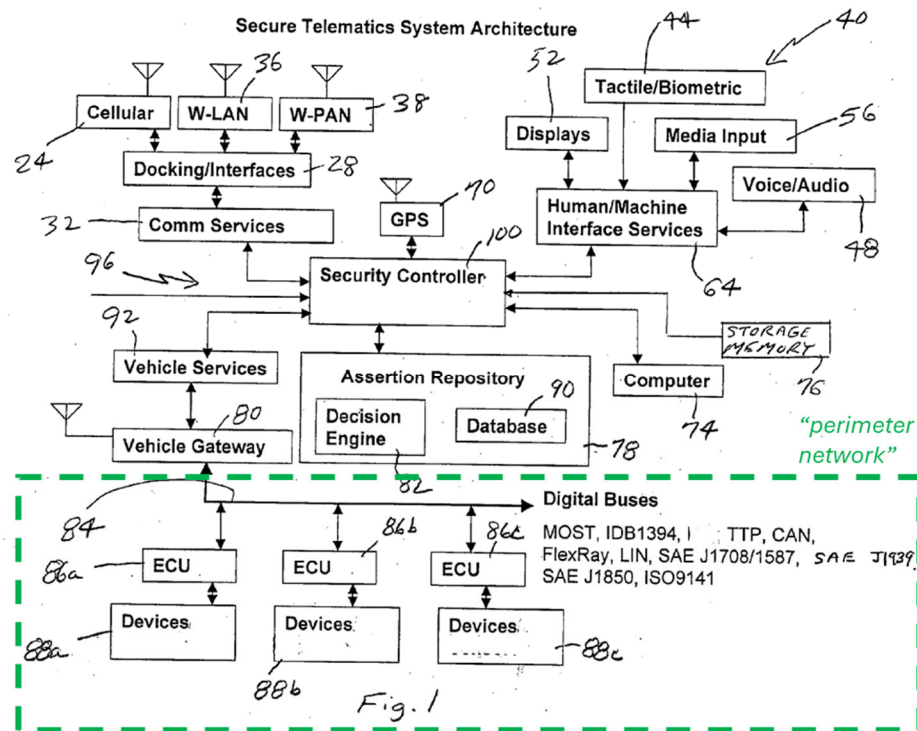
speech and/or voice prompts; (c) multiple displays including said first display; managing said first certificate and at least a first key related to use of said first display; enforcing one or more usage rules associated with said first display; monitoring and logging usage information related to said first display; providing fault notification related to said first display and supporting communication on said first bus.

(Spaur, Ex. 1020, Claim 27.)

475. In another example, a PHOSITA would have understood that Spaur’s “*security mechanism*” may encompass a broader set of components that jointly implement the system’s security functionality. Spaur discloses that the security controller 100 authenticates entities, mediates traffic, and arbitrates bus usage; the vehicle services module 92 enforces rules, manages access keys and certificates, and supports secure communications; and the vehicle gateway 80 controls access to the vehicle buses. (Spaur, Ex. 1020, [0010], [0034]-[0035].) Spaur further explains that an assertion repository 78 stores security assertions and associated relationships and includes a decision engine 82 that evaluates those assertions to determine permissible communication and resource access. (Spaur, Ex. 1020, [0032]-[0033].) Additionally, Spaur describes a database 90 that stores the data, relationships, and policy information used by the assertion repository 78 and decision engine 82. (Spaur, Ex. 1020, [0033].) A PHOSITA would have recognized that these components—security controller 100, services module 92, gateway 80, assertion

repository 78, decision engine 82, and database 90—operate together to store, evaluate, and enforce the policies governing communication within the vehicle network, collectively constituting the “*security mechanism*.”

476. With respect to the example above where the vehicle gateway 80 and the vehicle services module 92 forms a “*security mechanism*,” this can be further defined as a “*first security measure*.” A PHOSITA would have understood that the vehicle gateway 80 and the vehicle service module 92 creates a logical security boundary (“*perimeter network*”) that protects specified computational components (e.g., one or more of the vehicle ECUs or sensors) from external, untrusted communications. Spaur explains that external inputs, including wireless commands, are received through the vehicle gateway 80 and vehicle services module 92 before reaching any ECU 86 or vehicle device 88, and that only after passing through these components may a message be introduced onto the internal buses 84. (Spaur, Ex. 1020, [0034]-[0035].) By requiring that all external communication paths terminate at the vehicle gateway 80/vehicle service module 92 boundary before entering the in-vehicle network, Spaur teaches a logical perimeter that protects the internal ECUs from unauthorized or malformed external traffic (an example of which is shown below in Figure 1).



Spaur, Ex. 1020, Figure 1 (Annotated)

477. A PHOSITA would have further understood that the security boundary (“*perimeter network*”) can also be established around individual ECUs. Because Spaur discloses that all communication to a particular ECU must first pass through the vehicle gateway 80 and the vehicle services module 92—where access control, rule enforcement, secure-communication checks, and authentication occur—the boundary created by these components defines a logical perimeter for each ECU whose operation depends on messages entering through its associated bus. (Spaur, Ex. 1020, [0034]-[0035].) For example, where an ECU (such as a telematics, infotainment, or gateway-exposed subsystem) receives external or wireless inputs, the perimeter is effectively formed around that specific ECU because the gateway

80 and services module 92 regulate messages entering or leaving the ECU's bus connection. (Spaur, Ex. 1020, [0034]-[0035].) Therefore, Spaur's disclosed architecture supports a perimeter network that can surround a single ECU, a subset of ECUs on a particular bus, or the entire collection of ECUs residing on the vehicle networks (*i.e.*, the CAN, MOST, FlexRay, or LIN networks).

478. Thus, the combination of Spaur and Peirce teaches “*a first security mechanism [vehicle gateway 80 and vehicle service module 92] to enforce a security measure [e.g., authenticating communication, access control, rule-based command filtering] and form a perimeter network logically including the plurality of on board computational components [ECUs 86].*”

479. Intentionally left blank.

480. Intentionally left blank.

[1c] a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,

481. Spaur discloses that the telematics secure system 20 “includes a common bus 96 with which a number of, if not all, communicable resources in the vehicle communicate.” (Spaur, Ex. 1020, [0036].) Spaur further discloses that “the common bus 96 can link these resources to a security controller 100,” to facilitate security within the vehicle network:

With regard to enabling communications in a secure manner, the system 20 preferably includes a common bus 96 with which a number of, if not all, communicable resources in the vehicle communicate. In this embodiment, the common bus 96 can link these resources to a security controller 100, which acts as a hub or switch through which communications pass relative to the communicable resources. Although represented in FIG. 1 as separate lines or connections to the security controller 100, it should be appreciated that all such lines when linked together represent a common bus. The common bus 96 can be based on one of a number of available bus technologies including those that provide or implement the vehicle or digital buses 84. The common bus 96 could also be implemented using wireless technologies.

(Spaur, Ex. 1020, [0036].)

The system also includes a security controller that is connected to the common bus. The security controller can act as a hub through which all information passes in connection with achieving desired security, especially controlling usage of resources by more than one entity. The security controller is involved with security authentication of entities and/or resources, facilitates secure channel establishment between or among entities and/or resources and provides bus and bandwidth arbitration services.

(Spaur, Ex. 1020, [0010].)

25. A system of claim 23 wherein said security controller is involved with performing at least one of the following: authenticating said first application using said stored certificate information; authenticating a

user associated with said first application using stored identification information; verifying use of said at least first proprietary resource utilizing at least one of location and time; relying on at least a first key in determining whether to allow execution of said first application; enabling a number of applications including said first application and said second application to execute simultaneously using a plurality of said proprietary resources; enabling access to at least non-proprietary resources of said resources; arbitrating use of said first bus; and monitoring activity on said first bus.

(Spaur, Ex. 1020, Claim 25.)

482. Spaur discloses that all traffic (i.e., communication) is routed or mediated by the security controller 100:

The security controller essentially acts as a switch in the system and can act as a proxy for other resources or services. All traffic between or among entities and/or resources is routed by or initiation is mediated by the security controller. After a secure session has been established, the security controller need only be involved as necessary to monitor traffic. Monitoring can relate to verifying that the traffic conforms to the predetermined profile, for example, of one or more particular applications. In one embodiment, the security controller is not integrated into the common bus as a hub or switch, but communicates with the common bus and monitors activities related to security in order to effect its control in connection with assuring that conditions associated with the established relationships are met.

(Spaur, Ex. 1020, [0010].)

483. Spaur explains that “the security controller 100 monitors common bus 96 activity and vehicle bus 84 activity . . . to ensure that the security conditions established during configuration or authentication continue to be met over time.” (Spaur, Ex. 1020, [0042].)

25. A system of claim 23 wherein said security controller is involved with performing at least one of the following: authenticating said first application using said stored certificate information; authenticating a user associated with said first application using stored identification information; verifying use of said at least first proprietary resource utilizing at least one of location and time; relying on at least a first key in determining whether to allow execution of said first application; enabling a number of applications including said first application and said second application to execute simultaneously using a plurality of said proprietary resources; enabling access to at least non-proprietary resources of said resources; arbitrating use of said first bus; and monitoring activity on said first bus.

(Spaur, Ex. 1020, Claim 25.)

484. A PHOSITA would have understood that Spaur’s disclosure of authenticating communication and routing traffic between components indicates that the security controller 100 executes software instructions to evaluate security conditions. Spaur further discloses that “the security controller 100 can include one or more secure processors” and that “the security controller 100 can be implemented as a single chip.” (Spaur, Ex. 1020, [0039].) A PHOSITA would have recognized

that a controller equipped with “secure processors” and “implemented as a single chip” indicates that the security controller 100 is built as an integrated circuit containing a processor core, memory, and executable logic—features that are standard and well-known characteristics of a microprocessor-based device. Additionally, Peirce discloses that a “[p]rocessor 52 can be any type of device capable of processing electronic instructions including microprocessors, microcontrollers, host processors, controllers, vehicle communication processors, and application specific integrated circuits (ASICs).” (Peirce, Ex. 1021, 3:44-55.)

485. Spaur also explains that the security controller 100 takes action when security deviations arise. For example, Spaur discloses that “if there were a time condition related to bus activity, the security controller 100 could dynamically discontinue the secure channel connection after a predetermined time event.” (Spaur, Ex. 1020, [0042].)

486. A PHOSITA would have understood that Spaur’s disclosure of the security controller 100 “monitor[ing] common bus 96 activity and vehicle bus 84 activity . . . to ensure that the security conditions . . . continue to be met over time” and “dynamically discontinu[ing] the secure channel” when those conditions are not met indicates that the security controller 100 (“*network controller*”) evaluates whether the required conditions remain satisfied and determines when they fail (“*detect an instance of a breach of the security measure*”).

487. Spaur further reinforces that the security controller 100 enforces security measures by operating as a firewall against unsafe or untrusted communications. Spaur discloses a “[c]arry-in device firewall—to support any interface to a computer 74 that can be used in the vehicle,” and explains that “security firewall functions can be built into the security controller 100.” (Spaur, Ex. 1020, [0048].) Spaur teaches that this firewall “protects resources in the vehicle from invalid, unwanted or malformed requests[,]” and that applications running on external (“carry-in”) computers must be “certified” before being granted access to vehicle services. (Spaur, Ex. 1020, [0048].) Spaur further explains that “the security controller 100 handles authentication and key exchange with such applications[,]” and that if an “application is not certified, the security controller 100 can allow certain, predetermined vehicle services to be made available” while restricting others. (Spaur, Ex. 1020, [0048].) A PHOSITA would have understood that identifying an invalid, malformed, or non-certified request indicates that the security controller 100 detects that the request violates a required security condition before the communication is rejected (“*detect an instance of a breach of the security measure*”).

488. Further, as discussed in the Rationale to Combine section (¶¶546-563), Peirce discloses a vehicle network that includes “a plurality of transmit filters” (210-213 annotated below in red) and “a plurality of receive filters” (218-221 annotated

below in blue). (Peirce, Ex. 1021, 6:63-7:2.) Piece further discloses that the transmit filters 210-213 and the receive filters 218-221 “are coupled to each of the ECUs” 214-217. (Peirce, Ex. 1021, 7:3-5.)

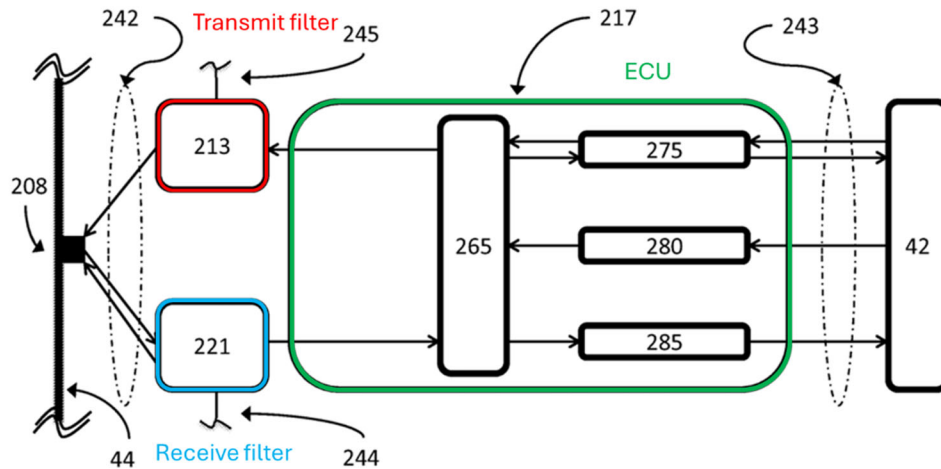


Figure 5

Peirce, Ex. 1021, Figure 5 (Annotated)

489. Peirce discloses that “[t]he transmit filters 210-213 and/or the receive filters 218-221 filters may be subject to a filter policy (e.g., one or more rules)” which “may include executable instructions for implementing logical functions [such as] validating or verifying the authenticity of the message contents.” (Peirce, Ex. 1021, 7:38-43.) Peirce explains that these executable instructions include firmware/software structures used to validate message content (e.g., source ID, destination ID, message ID):

Executable instructions of the policy include software or firmware and is not limited to routines, modules, objects, components, data structures, and/or the like, for performing particular tasks and/or implementing particular abstract data types. The message contents include any part or portion of the message. Thus, the message contents may include the message identity. In CAN networks for example, the message identity may include the source ID, the destination ID, the message ID, or any combination thereof.

(Peirce, Ex. 1021, 7:43-51.)

490. Peirce further discloses that the filter policy minimizes or eliminates corrupt messages, including maliciously generated messages:

The filter policy may minimize or eliminate the transmission of corrupt messages over the bus 44. Corrupt messages include any undesirable or invalid or improper message. They may be generated by a malicious third party (e.g., a hacker) or simply by a corrupted or damaged bus, ECU, VSM, or other subsystem. When the corrupted message is sent over the bus (e.g., 44), other subsystems (including VSMs) may reply and/or take action resulting in an inaccurate, improper, and even harmful effect on the vehicle and its occupants. For example, a hacked or damaged infotainment system may send a corrupt message onto the bus 44 which it might not normally send—for instance a corrupt message regarding the vehicle's wheel speed. This corrupt message may then be received by a traction control system within the vehicle resulting in below-normal traction-control performance.

(Peirce, Ex. 1021, 7:60-8:8.)

491. A PHOSITA would have understood that Peirce's disclosure that the transmit and receive filters apply a policy with "executable instructions for . . . validating or verifying the authenticity of the message contents" and that this policy "minimize[s] or eliminate[s] the transmission of corrupt messages," including those from "a malicious third party (e.g., a hacker)," indicates that the filters identifying messages and determine whether those messages violate the filter policy before they are allowed onto the bus (*"detect an instance of a breach of the security measure"*). (Peirce, Ex. 1021, 7:38-43, 7:60-8:8.)

492. As stated in the Rationale to Combine (§§546-563), the combined system of Spaur and Peirce includes Spaur's security controller 100 (*"network controller"*) and Peirce's filter-policy logic, allowing the vehicle system to detect and validate message authenticity, filter corrupt or malicious messages, and prevent their propagation (*"detect an instance of a breach of the security measure"*).

493. Thus, the combination of Spaur and Peirce teaches *"a microprocessor executable network controller [security controller 100] operable to (i) detect 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

494. As discussed above in limitation [1a], Spaur discloses various ECUs 86 that include subsystems within a vehicle (e.g., body control, engine control, telematics control), indicating that the ECUs act as “*on board computational components*” because each of these subsystems requires active processing, software execution, and real-time decision making. (Spaur, Ex. 1020, [0034].)

495. Spaur discloses that in addition to the vehicle-integrated subsystems, the telematics secure system 20 also includes other components that receive and analyze data. For example, Spaur discloses “one or more computers 74” which can be “portable and removable from the vehicle or embedded with the vehicle.” (Spaur, Ex. 1020, [0031].) Spaur further discloses that the computer(s) 74 include “a personal digital assistant (PDA) a laptop or any other intelligent and/or processing unit.” (Spaur, Ex. 1020, [0031].) Spaur also discloses that the telematics secure system 20 includes an assertion repository 78 with a policy decision engine 82 that “is responsible for deciding which information of a plurality of stored information is to be released to a particular request.” (Spaur, Ex. 1020, [0033].)

496. A PHOSITA would have understood that, besides ECUs 86, Spaur discloses various components that receive, process, and analyze data, indicating that any of these other components function as a “*computational component*” (e.g., computer(s) 74, assertion repository 78 with policy decision engine 82).

497. 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 violated a filter policy.

498. Spaur discloses that the security controller 100 performs continuous monitoring of “common bus 96 activity and vehicle bus 84 activity between or among resources to ensure that the security conditions established during configuration or authentication continue to be met over time.” (Spaur, Ex. 1020, [0042].) Spaur explains that resources can include “vehicle buses, vehicle devices, interfaces, subsystems [e.g., computers 74, assertion repository 78], storage memory in the vehicle, applications executed in the vehicle, connectivity hardware/software and communication devices.” (Spaur, Ex. 1020, [0007], *see also* [0031]-[0032].) Spaur further discloses that the security controller 100 “dynamically discontinue[s] the secure [communication] channel connection” when those conditions are no longer satisfied (e.g., after a predetermined time event). (Spaur, Ex. 1020, [0042].)

499. 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 [ECU] not affected by or potentially affected by the instance of a breach of the security measure*”).

500. Spaur further discloses that the security controller 100 provides “authentication of entities and/or resources,” mediates the flow of “traffic between or among entities and/or resources” and “provides bus and bandwidth arbitration services” within the vehicle network. (Spaur, Ex. 1020, [0010].) A PHOSITA would have understood that these responsibilities require the security controller 100 to decide whether a particular ECU, device, or resource should be permitted to communicate and, conversely, when communication should be halted due to unauthorized or abnormal activity. In performing these authentication, mediation, and arbitration functions, the security controller 100 determines when a compromised component should be prevented from interacting with other “*computational component[s]*” or “*on board computational components.*”

501. Thus, the combination of Spaur and Peirce teaches “*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.*”

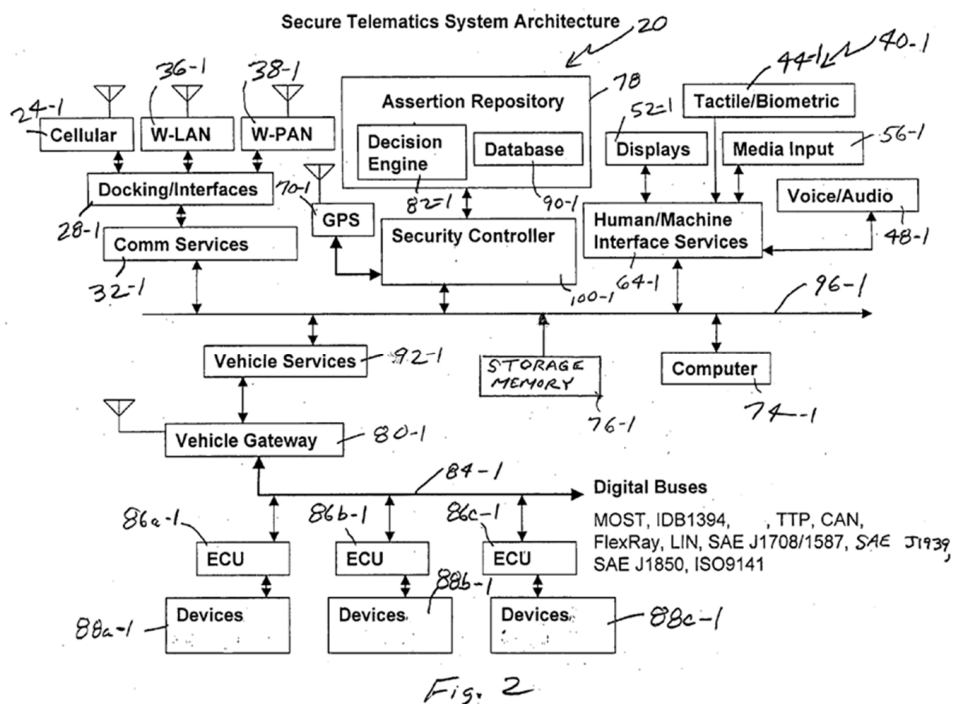
[1e] (iii) when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of

(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,

502. As explained above in limitations [1c] and [1d], Spaur discloses 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. (Spaur, Ex. 1020, [0007], [0010], [0031]-[0032], [0042].) Spaur's teaching of "isolat[ion]" is further confirmed by Spaur's comparison between the embodiment shown in Figure 1 and a second embodiment shown to Figure 2. Spaur discloses that "unlike the FIG. 1 embodiment," in Figure 2, "the security controller 100-1 is included in the system 20-1 as another apparatus or resource on the common bus 96-1," which no longer allows the security controller 100-1 to "serve as a switch on the

common bus 96-1.” (Spaur, Ex. 1020, [0049].) Spaur explains that “[t]his can be a drawback to the effectiveness of the security controller 100-1 since its ability to isolate segments of the common bus 96-1 does not exist” because “it is no longer a switch or central hub through which all communications pass between and among resources on the common bus 96-1.” (Spaur, Ex. 1020, [0049].)



Spaur, Ex. 1020, Figure 2

503. Further, Peirce discloses that “the filter policy may pertain to validating or verifying the authenticity of the message contents.” (Peirce, Ex. 1021, 8:41-43.) Peirce discloses that the receive filter 221 validates incoming messages by “compar[ing] the message ID of an incoming message with the known message IDs in its storage to validate whether the incoming message should be accepted or not

by the VSM 42.” (Peirce, Ex. 1021, 8:47-50.) Peirce explains that if the message IDs match “the incoming message may be validated and may be sent to the VSM 42.” However, if the message IDs do “not match, the message may be corrupt and the transmission of the incoming message may be terminated never reaching the VSM 42.” (Peirce, Ex. 1021, 8:52-55.)

504. Similarly, Peirce discloses a parallel action of validating or verifying outgoing messages by the transmit filter 213, explaining that the transmit filter 213 “compare[s] the source ID of an outgoing message with the source ID of the VSM 42 to validate whether the outgoing message should be sent or not.” (Peirce, Ex. 1021, 8:62-64.) If the source ID of “the outgoing message matches the source ID of the VSM 42, then the outgoing message may be validated and may be sent to the bus 44.” (Peirce, Ex. 1021, 8:65-67.) However, if the source IDs do “not match, the message may be corrupt and the transmission of the outgoing message may be terminated never reaching the bus 44.” (Peirce, Ex. 1021, 8:67-9:3.)

505. A PHOSITA would have understood that by terminating incoming or outgoing message transmission before it reaches the bus contains the effect of a breach to the component where it occurs and functionally “*isolate[s]*” the computational component affected from those not affected by the breach.

506. As stated in the Rationale to Combine, the combined system of Spaur and Peirce includes Spaur’s security controller 100 and Peirce’s filters 213 and 221

and filter-policy logic, allowing the vehicle system to monitor and terminate unauthorized communication channels, and physically and logically separate corrupted ECUs (or resources as discussed above in limitation [1d]) from the communication path. (¶¶546-563.)

507. Thus, the combination of Spaur and Peirce teaches “*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 . . . (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.*”

[1f] 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:

508. As explained above in limitation [1c], Spaur discloses that the security controller 100 monitors “[a]ll traffic between or among entities and/or resources.” (Spaur, Ex. 1020, [0010], *see also* [0034]-[0035].) Further, the security controller 100 “monitors . . . bus activity . . . to ensure that the security conditions . . . continue to be met over time” and “dynamically discontinue[s] the secure channel connection” when those conditions are not met. (Spaur, Ex. 1020, [0042].)

509. A PHOSITA would have understood that because all communication flows through the security controller 100, discontinuing the secure channel for a component prevents that component from transmitting or receiving any further messages. Therefore, when the security controller 100 terminates the secure channel when a security condition failure/breach is detected, this is effectively “*blocking communications to and from the computational component affected by the instance of a breach of a security measure.*”

510. I also note that 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.*”

511. Spaur also discloses that the vehicle gateway 80 and the vehicle services module 92 collectively “controls access to and use of the vehicle buses 84”

and supports “secure communications,” “enforces rules,” “arbitrates bus access,” and “manages access keys and certificates.” (Spaur, Ex. 1020, [0010], [0034]-[0035].) As discussed above in limitation [1b], as well as limitation [1c], when the security controller detects that a security condition is no longer satisfied and “dynamically discontinue[s] the secure channel connection,” the security controller 100—acting together with the vehicle gateway 80 and vehicle services module 92—cuts off the affected component’s ability to communicate across the vehicle buses. (Spaur, Ex. 1020, [0042].) Because these components collectively mediate all message flow, termination of the secure channel “*block[s] communications to and from the computational component affected by the breach.*”

512. I also note that 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.*”

513. In addition, as discussed above, Peirce expressly discloses the use of filter policies within both transmitting filters and receiving filters to block disallowed or suspicious traffic. Peirce explains that these filters enforce transmission and reception rules based on message characteristics, thereby

preventing certain ECUs or nodes from placing messages onto the network or receiving them. (Peirce, Ex. 1021, 10:4-23.)

514. A PHOSITA would have understood that Peirce's transmit-filter and receive-filter blocking mechanisms provide precisely the type of selective communication denying/blocking identified in limitation [1f], specifically form (1) *"denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure"* and (3) *"blocking communications to and from the computational component affected by the instance of a breach."* A PHOSITA would further have understood that when Peirce's filters are combined with Spaur's ability to discontinue secure channels or deny certificates, the combined architecture provides multiple, independent ways to block, deny, or redirect communications for security enforcement.

515. Thus, the combination of Spaur and Peirce teaches *"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... [and] (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure."*

11. Independent Claim 9

a. Claim 9

516. Independent claim 9 is largely duplicative of independent claim 1. To illustrate, the table below shows a side-by-side comparison of claims 1 and 9. Claim 9 is “marked up” to show the minor differences.

Claim 1	Claim 9
1[pre] . A vehicle, comprising:	9[pre] . A <u>method</u> , comprising:
[1a] a plurality of on board computational components;	[9a] <u>in a vehicle comprising</u> 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
[1c] a microprocessor executable network controller operable to	[9c] a microprocessor executable network controller [], the

(i) detect an instance of a breach of the security measure,	microprocessor executable network controller <u>identifying a possible</u> security breach instance;
[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] <u>in response, the microprocessor executable network controller</u> determining whether a computational component affected by the <u>possible</u> security <u>breach instance</u> can be isolated from at least one on board computational component not affected by or potentially affected by the <u>possible security breach instance</u> ; and

[1e] (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	[9e] when the computational component affected by the <u>possible security breach instance</u> can be isolated from the at least one on board computational component not affected by or potentially affected by the <u>possible security breach instance, the microprocessor executable network controller at least one of</u> (a) isolating the at least one on board computational component not affected by or potentially affected by the <u>possible security breach instance</u> from the computational component affected by the possible security breach instance 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,	(b) isolating the computational component affected by the <u>possible security breach instance</u> from the at least one on board computational component not affected by or potentially affected by the <u>possible security breach instance</u>,
[1f] 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	[9f] wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the <u>possible security breach instance</u>, (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,	affected by the <u>possible security breach instance</u> 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	(3) blocking communications to and from the computational component affected by the <u>possible security breach instance</u> , and
(4) activating a second security mechanism in response to the instance of a breach of a security measure.	(4) activating a second security mechanism in response to the <u>possible security breach instance</u> .

9[pre]. A method, comprising:

517. Spaur discloses that “[i]n accordance with the present invention, system and method are provided for utilizing resources, including proprietary resources in a vehicle.” (Spaur, Ex. 1020, [0006].)

518. Spaur further discloses:

1. A method for controlling use of proprietary resources associated with a vehicle, comprising: providing resources including proprietary resources associated with a vehicle including a plurality of the following: a first bus, a first interface, a first display, a first vehicle device, a first subsystem, a first application, and a second application;

(Spaur, Ex. 1020, Claim 1.)

519. Thus, the combination of Spaur and Peirce teaches “[a] *method*”.

[9a] in a vehicle comprising a plurality of on board computational components,

520. Claim limitation [9a] is substantially similar to limitation [1a] of claim 1; however, limitation [9a] requires “*in a vehicle comprising a plurality of on board computational components,*” whereas limitation [1a] requires “*a plurality of on board computational components.*”

521. As the differences between claim limitations [9a] and [1a] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[9b] a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components, and

522. As claim limitation [9b] is identical to limitation [1b] of claim 1, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[9c] a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance;

523. Claim limitation [9c] is substantially similar to limitation [1c] of claim 1; however, limitation [9c] requires “*a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance*,” whereas limitation [1c] requires “*a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure.*”

524. As the differences between claim limitations [9c] and [1c] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[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

525. Claim limitation [9d] is substantially similar to limitation [1d] of claim 1, however, claim [9d] requires “in response, the microprocessor executable network controller” and “the possible security breach instance,” whereas claim [1d] does not.

526. As the differences between claim limitations [9d] and [1d] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[9e] 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,

527. Claim limitation [9e] is substantially similar to limitation [1e] of claim 1, however, claim [9e] requires “*the possible security breach instance,*” whereas claim [1e] does not.

528. As the differences between claim limitations [9e] and [1e] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[9f] 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:

529. Claim limitation [9f] is substantially similar to limitation [1f] of claim 1, however, claim [9f] requires “*the possible security breach instance,*” whereas claim [1f] does not.

530. As the differences between claim limitations [9f] and [1f] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

12. Independent Claim 17

a. Claim 17

531. Independent claim 17 is largely duplicative of independent claim 1. To illustrate, the table below shows a side-by-side comparison of claims 1 and 17. Claim 17 is “marked up” to show the minor differences.

Claim 1	Claim 17
1[pre]. A vehicle, comprising:	17[pre]. <u>In</u> a vehicle comprising
[1a] a plurality of on board computational components;	[17a] a plurality of on board computational components,
[1b]	[17b] <u>a non-transient, tangible computer readable medium comprising</u>
a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and	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 operable to (i) detect an instance of a breach of the security measure,	[17c] a microprocessor executable network controller <u>on board a selected vehicle that, when executed,</u> <u>detects</u> 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	[17d] <u>determines</u> 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,

[1e] (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	[17e] 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 <u>isolates</u> the at least one on board computational component not affected by or potentially affected by the instance of a breach of <u>the</u> security measure from the computational component affected by the instance of a breach of <u>the</u> security measure []
--	--

(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,	<u>isolates</u> 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 <u>the</u> security measure,
[1f] 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	[17f] 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 <u>the</u> 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,	of <u>the</u> 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	(3) blocking communications to and from the computational component affected by the instance of a breach of <u>the</u> security measure, and
(4) activating a second security mechanism in response to the instance of a breach of a security measure.	(4) activating a second security mechanism in response to the instance of a breach of <u>the</u> security measure.

17[pre] In a vehicle comprising

532. Claim limitation 17[pre] is substantially similar to limitation 1[pre] of claim 1. As the differences between claim limitations 17[pre] and 1[pre] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

17[a] a plurality of on board computational components,

533. Claim limitation [17a] is identical to limitation [1a], therefore, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce

[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

534. Claim limitation [17b] is substantially similar to claim limitation [1b], however, limitation [17b] requires “*a non-transient, tangible computer readable medium,*” whereas limitation [1b] does not.

535. Spaur discloses that various subsystems can be incorporated as part of the telematics secure system 20. (Spaur, Ex. 1020, [0031].) Spaur explains that one of the subsystems includes a storage memory 76 which “can contain proprietary data and/or program code that involves use of other resources located within and/or outside of the vehicle.” (Spaur, Ex. 1020, [0031].) Spaur further explains that “[t]he storage memory 76 can also encompass one or more hard disks and/or removable memory, such as CD-ROMs.” (Spaur, Ex. 1020, [0031].)

536. As stated above in limitation [1b], Spaur explains that the vehicle services module 92 enforces rules, supports secure communications, manages keys and certificates, and arbitrates access to the vehicle buses, while the vehicle gateway 80 controls access to the buses and governs the introduction of messages into the in-

vehicle network. (Spaur, Ex. 1020, [0034]-[0035].) A PHOSITA would have understood that these security functions are executed by software logic stored in the system's program memory, including the program code described in connection with storage memory 76.

537. A PHOSITA would have further understood that hard disks and CD-ROMs are physical, non-transitory storage media, in contrast to transient media such as signals. Accordingly, Spaur's disclosure that "[t]he storage memory 76 can also encompass one or more hard disks and/or removable memory, such as CD-ROMs" (Spaur, Ex. 1020, [0031]) demonstrates that Spaur teaches "*a non-transient, tangible computer readable medium*" that stores program code used to implement the security-enforcing functionality of the vehicle gateway 80 and the vehicle services module 92 ("*first security mechanism*").

538. As the rest of claim limitation [17b] is identical to limitation [1b], I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[17c] a microprocessor executable network controller on board a selected vehicle that, when executed, detects an instance of a breach of the security measure,

539. Claim limitation [17c] is substantially similar to limitation [1c] of claim 1; however, limitation [9c] requires "*a microprocessor executable network*

controller on board a selected vehicle that, when executed, detects an instance of a breach of the security measure”, whereas limitation [1c] requires “a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure.”

540. As the differences between claim limitations [17c] and [1c] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[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,

541. Limitation [17d] is identical to limitation [1d], thus, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[17e] 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 onboard 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,

542. Claim limitation [17e] is substantially similar to limitation [1e] of claim 1, however, claim [1e] recites “*the instance of a breach of a security measure*” while claim [17e] recites “*the instance of a breach of the security measure.*”

543. As the differences between claim limitations [17e] and [1e] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

[17f] 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 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:

544. Claim limitation [17f] is substantially similar to limitation [1f] of claim 1, however, claim [1f] requires “*the instance of a breach of a security measure*” while claim [17f] requires “*the instance of breach of the security measure.*”

545. As the differences between claim limitations [17f] and [1f] are not substantial and do not change the meaning of claim, I refer back to my analysis of claim 1 to establish that this limitation is met by the combination of Spaur and Peirce.

13. Rationale to Combine

546. It would have been obvious to a PHOSITA at the time of the alleged invention to combine the vehicle network system disclosed in Spaur with the filtering system disclosed in Peirce to provide additional functionality, e.g., to improve safety and security. A PHOSITA would have understood that Spaur and Peirce are complementary technologies that are combinable, for example, Spaur discloses that:

The foregoing discussion of the invention has been presented for purposes of illustration and description. Further, the description is not intended to limit the invention to the form disclosed herein. Consequently, variations and modifications commensurate with the above teachings, within the skill and knowledge of the relevant art, are within the scope of the present invention. The embodiments described hereinabove are further intended to explain the best modes presently known of practicing the invention and to enable others skilled in the art to utilize the invention in such, or in other embodiments, and with the various modifications required by their particular application or uses. It is intended that the appended claims be construed to include alternative embodiments to the extent permitted by the prior art.

(Spaur, Ex. 1020, [0233].)

547. Spaur and Peirce are from the same field—vehicle network security:

A telematics system that includes a security controller is provided. The security controller is responsible for ensuring secure access to and controlled use of resources in the vehicle. The security measures relied on by the security controller can be based on digital certificates that grant rights to certificate holders, e.g., application developers. In the case in which applications are to be used with vehicle resources, procedures are implemented to make sure that certified applications do not jeopardize vehicle resource's [sic] security and vehicle users' safety. Relationships among interested entities are established to promote and support secure vehicle resource access and usage. The entities can include vehicle makers, communication service providers, communication apparatus vendors, vehicle subsystem suppliers, application developers, as well as vehicle owners/users. At least some of the entities can be members of a federation established to enhance and facilitate secure access and usage of vehicle resources.

(Spaur, Ex. 1020, Abstract.)

The present invention relates to telematics and in particular to securing communications involving uses of proprietary resources in a vehicle.

(Spaur, Ex. 1020, [0001].)

A message filtering system for a communications system in a vehicle enabling communication between various systems and subsystems via a vehicle bus. Electronic devices may be coupled to the bus. Electronic control units (ECUs) may be located therebetween. The ECU may regulate or control the flow of messages between the bus and the

electronic devices. Message filters may apply a filter policy to incoming and outgoing messages. In addition, the message filtering system may have an alert policy for violations of the filter policy. In one embodiment, the source identity of outgoing messages may be overwritten by a message filter dedicated to outgoing messages; this message filter may be an application specific integrated circuit.

(Peirce, Ex. 1021, Abstract.)

The present invention relates generally to a communication system within a vehicle and more specifically to filtering messages over a vehicle network within the vehicle.

(Peirce, Ex. 1021, 1:5-7.)

548. Spaur discloses a vehicle security architecture built around a centralized security controller that “ensur[es] secure access to and control[s] [the] use of resources in the vehicle.” (Spaur, Ex. 1020, Abstract.) Spaur discloses that the security controller also monitors common bus activity and discontinues secure channel connection if an invalid request is detected:

The security controller essentially acts as a switch in the system and can act as a proxy for other resources or services. All traffic between or among entities and/or resources is routed by or initiation is mediated by the security controller. After a secure session has been established, the security controller need only be involved as necessary to monitor traffic. Monitoring can relate to verifying that the traffic conforms to the predetermined profile, for example, of one or more particular

applications. In one embodiment, the security controller is not integrated into the common bus as a hub or switch, but communicates with the common bus and monitors activities related to security in order to effect its control in connection with assuring that conditions associated with the established relationships are met.

(Spaur, Ex. 1020, [0010].)

Security monitoring—the security controller 100 monitors common bus 96 activity and vehicle bus 84 activity between or among resources to ensure that the security conditions established during configuration or authentication continue to be met over time. For example, if there were a time condition related to bus activity, the security controller 100 could dynamically discontinue the secure channel connection after a predetermined time event.

(Spaur, Ex. 1020, [0042], *see also* [0048], [0051]-[0052].)

549. However, Spaur does not disclose how to isolate an individual component once a security breach or violation is detected.

550. Peirce discloses a vehicle communication system that includes a filtering system to “filter[] messages over a vehicle network” to provide increased security. (Peirce, Ex. 1021, 1:5-7.)

551. Peirce discloses that its filtering system includes receive filters and transmit filters, each of which are coupled to an ECU:

Turning to FIG. 2, there is shown an exemplary vehicle network. The vehicle network may be CAN, MOST, LIN, LAN or other suitable

protocol, standard, etc. The illustrated vehicle network includes a plurality of electronic control units (ECUs) 214, 215, 216, 217, a plurality of transmit filters 210, 211, 212, 213, a plurality of receive filters 218, 219, 220, 221, the telematics unit 30, and a plurality of VSMs 38, 40, 42. FIG. 2 illustrates that the transmit filters 210, 211, 212, 213 and the receive filters 218, 219, 220, 221 are coupled to each of the ECUs 214, 215, 216, 217, respectively. The ECUs 214, 215, 216, 217 are coupled via VSM interfaces 231, 235, 239, 243 to the telematics unit 30 and each of the VSMs 38, 40, 42, respectively. Each of the ECUs 214, 215, 216, 217 (e.g., via the transmit filters and receive filters) may be coupled to an exemplary bus (e.g., bus 44) via primary interfaces 230, 234, 238, and 242 at nodes 205, 206, 207, 208. Thus, the bus 44 may indirectly connect the telematics unit 30 and VSMs 38, 40, 42 to one another.

(Peirce, Ex. 1021, 6:63-7:13.)

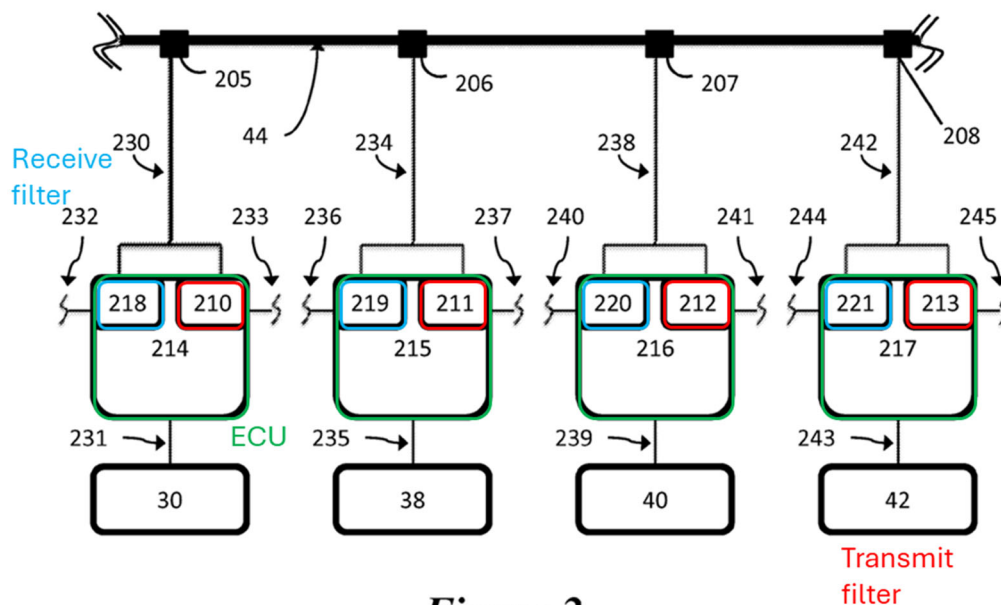


Figure 2

Peirce, Ex. 1021, Figure 2 (Annotated)

552. Peirce discloses that the transmit filters 210-213 and the receive filters 218-221 can be located outside of the ECU 214-217:

Turning to FIG. 5, there is shown another embodiment of the bus 44, the ECU 217, and the VSM 42 that is generally similar to that of FIG. 4; however, in FIG. 5, both the transmit filter 213 and the receive filter 221 are shown physically and/or logically isolated from the ECU 217 and/or the protocol controller 265—thus, mitigating the possibility of corruption of both.

(Peirce, Ex. 1021, 9:29-35.)

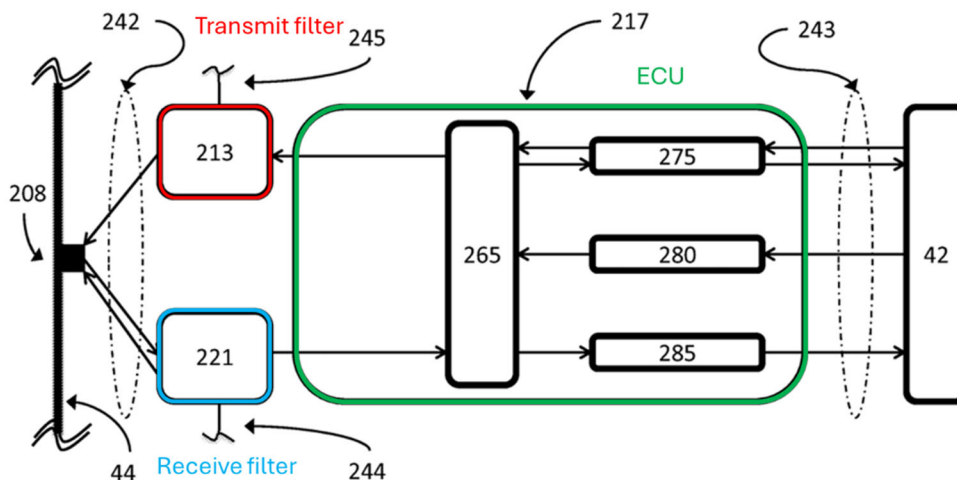


Figure 5

Peirce, Ex. 1021, Figure 5 (Annotated)

553. Peirce further discloses that the transmit filters 210-213 and the receive filters 218-221 are subject to filter policies that validate and/or verify the authenticity of transmitted messages:

The transmit filters 210, 211, 212, 213 and/or the receive filters 218, 219, 220, 221 may be subject to a filter policy (e.g., one or more rules). The filter policy may include executable instructions for implementing logical functions which may include validating or verifying the authenticity of the message contents. Executable instructions of the policy include software or firmware and is not limited to routines, modules, objects, components, data structures, and/or the like, for performing particular tasks and/or implementing particular abstract data types.

(Peirce, Ex. 1021, 7:38-47.)

The filter policy may minimize or eliminate the transmission of corrupt messages over the bus 44. Corrupt messages include any undesirable or invalid or improper message. They may be generated by a malicious third party (e.g., a hacker) or simply by a corrupted or damaged bus, ECU, VSM, or other subsystem. When the corrupted message is sent over the bus (e.g., 44), other subsystems (including VSMs) may reply and/or take action resulting in an inaccurate, improper, and even harmful effect on the vehicle and its occupants. For example, a hacked or damaged infotainment system may send a corrupt message onto the bus 44 which it might not normally send—for instance a corrupt message regarding the vehicle's wheel speed. This corrupt message may then be received by a traction control system within the vehicle resulting in below-normal traction-control performance.

(Peirce, Ex. 1021, 7:60-8:8.)

554. Peirce further discloses that the receive filters 218-221 validate/verify “the message contents of incoming messages (i.e., those received from the bus 44).” (Peirce, Ex. 1021, 8:43-45.) Peirce explains that the receive filters 218-221 “store known message IDs in accordance with the filter policy” and “then compare the message ID of an incoming message with the known message IDs in its storage to validate whether the incoming message should be accepted or not” by vehicle system modules (VSMs). (Peirce, Ex. 1021, 8:45-50.) Peirce further explains that if “the incoming message ID matches one of the known message IDs, then the incoming message may be validated and may be sent to the VSM 42[,]” however, if the

message IDs do not match, “the message may be corrupt and the transmission of the incoming message may be terminated never reaching the VSM 42.” (Peirce, Ex. 1021, 8:50-55.)

555. Similarly, Peirce discloses that the transmit filter 210-213 validate/verify “the message contents of outgoing messages (i.e., those being sent to the bus 44).” (Peirce, Ex. 1021, 8:56-58.) Peirce explains that the transmit filter 210-213 stores “the source ID of the VSM 42 (and/or the ECU 217) in accordance with the filter policy.” (Peirce, Ex. 1021, 8:58-60.) The transmit filter 210-213 “may compare the source ID of an outgoing message with the source ID of the VSM 42 to validate whether the outgoing message should be sent or not.” (Peirce, Ex. 1021, 8:61-64.) Peirce states that if “the source ID of the outgoing message matches the source ID of the VSM 42, then the outgoing message may be validated and may be sent to the bus 44[,]” however, if the sourced IDs do not match “the message may be corrupt and the transmission of the outgoing message may be terminated never reaching the bus 44.” (Peirce, Ex. 1021, 8:65-9:3.)

556. Peirce also explains that the VSM 42 represents a variety of components, including “an engine control module,” “a powertrain control module,” “a body control module,” as well as “numerous other[]” modules within the vehicle that exchange data and commands. (Peirce, Ex. 1021, 4:36-62.)

557. A PHOSITA would have understood that by filtering incoming/outgoing messages and blocking transmission of the message if it fails the filter policy, Peirce's filtering system prevents the message from reaching other VSMs or ECUs in the vehicle network, which effectively isolates the compromised or malfunctioning VSM/ECU from affecting other components on the vehicle network.

558. Additionally, as shown in Figure 5 above, Peirce further discloses that its filters (e.g., receive filters 210-213, transmit filters 218-221) can be “physically and/or logically isolated from the ECU [or VSM] . . . thus, mitigating the possibility of corruption of both[,]” allowing the filtering logic to continue blocking or terminating communications originating from an affected ECU even when that ECU is itself compromised. (Peirce, Ex. 1021, 9:29-35.) A PHOSITA would have understood that by terminating communications from corrupted or unauthorized sources—such as a “malicious third party” or a “corrupted or damaged ECU”—Peirce's filters isolate the affected computational component from the remainder of the network because the compromised component cannot place messages on the bus or receive messages not authorized by the filter policy. (Peirce, Ex. 1021, 7:60-8:7.)

559. A PHOSITA would have further understood that Peirce's externally located filtering system provides a greater level of security than systems in which a controller merely instructs an ECU to ignore certain messages. In such controller-

directed systems, if the ECU itself is compromised, it may not follow the instruction or may continue generating harmful traffic. Peirce avoids this vulnerability by placing the filtering logic outside the ECU and directly in the communication path, where it independently evaluates message validity and terminates improper transmissions before they can “reach[] the bus 44.” (Peirce, Ex. 1021, 8:54-9:3.) Because the filtering occurs upstream of the network bus and does not rely on the proper operation of the ECU, an attacker cannot use a compromised ECU to inject messages or execute interference-based denial-of-service attacks.

560. A PHOSITA at the time of the alleged invention would have been motivated to combine the vehicle network system disclosed in Spaur with the filtering system techniques disclosed in Peirce to yield predictable results, e.g., to increase the vehicle communication network security, by being able to detect and isolate affected/compromised components from the rest of the vehicle network. The ability to isolate specific vehicle components based on the detection of a breach (e.g., harmful, improper messages), improves control over inter-component communications and enhances safety by ensuring that compromised or malfunctioning components cannot affect critical vehicle systems, while allowing uncompromised components to continue operating normally.

561. A PHOSITA would have understood how to combine Spaur and Peirce with a reasonable expectation of success. In terms of hardware, a PHOSITA would

have modified the security controller 100 of Spaur's vehicle network system to include Peirce's filters 210-213, 218-221. As stated above, Peirce discloses that the filters 210-213, 218-221 can be "physically and/or logically isolated from the ECU" and implemented as separate hardware blocks, e.g., "application specific integrated circuit," rather than as an integrated ECU circuitry. (Peirce, Ex. 1021, 9:8-12, 9:29-35.) A PHOSITA would have understood that Peirce's disclosure indicates that the filters 210-213, 218-221 are modular, not ECU dependent, and can be positioned anywhere along the communication path between a component and the vehicle bus. Spaur's security controller 100 already sits in this communication path and is responsible for monitoring bus traffic, performing "firewall" and "bus arbitration" functions, and ensuring "secure access to and controlled use of resources" among all onboard components. (Spaur, Ex. 1020, [0010], [0042]-[0043], [0048], Abstract.) Since the security controller 100 is already the centralized gatekeeper through which vehicle communications pass, a PHOSITA would have recognized that relocating Peirce's message-validation filters into controller 100 simply shifts the filtering function from a distributed ECU-level location to a centralized location—without altering the function of the filters themselves.

562. In terms of software, a PHOSITA would have modified the security controller 100 disclosed in Spaur with Peirce's filter policy logic to enable isolation of a compromised component from the rest of the vehicle network. Spaur discloses

that the security controller 100 performs message monitoring, detection of “invalid, unwanted or malformed requests[,]” and enforcement of security rules governing “secure access to and controlled use of resources in the vehicle.” (Spaur, Ex. 1020, [0048], Abstract.) Peirce discloses that its filter policies consist of executable instructions for “validating or verifying the authenticity of the message contents” and for “terminat[ing] the transmission” of messages that violate those rules. (Peirce, Ex. 1021, 7:40-43, 8:41-9:3, 10:47-51.)

563. As Peirce states that its filters can be logically separated from the ECU and implemented as standalone logic or firmware modules, a PHOSITA would have understood that the same policy-evaluation code could be incorporated into the firmware running on Spaur’s security controller 100. (*See* Peirce, Ex. 1021, 9:8-12, 9:29-35.) Thus, integrating Peirce’s filter policy logic into Spaur’s security controller 100’s existing communication-processing loop would require only routine programming—e.g., inserting the filter-policy checks where controller 100 already processes bus traffic. This modification would have been a straightforward combination of known elements in the prior art, yielding the predictable result of, not only detect malformed or unauthorized communications, but also isolate compromised components by blocking or terminating their messages.

IX. Objective Indicia Does Not Support Patentability

564. Considering the information that I have reviewed, my general knowledge of the field of vehicle communication systems and limiting access to vehicle systems based on the location of a mobile device, and publications within that and related fields, I am not aware of any objective evidence that might support the patentability of the claims of the '100 Patent. Further, from my review of the file history (Ex. 1002) of the '100 Patent, I did not see that the applicant raised any secondary indicia of non-obviousness during prosecution. I am not otherwise aware of any publicly available evidence of secondary indicia of non-obviousness. Should any alleged secondary indicia of non-obviousness be presented, I reserve the right to provide an opinion thereon.

X. Conclusion

565. In my opinion, all the elements of the challenged claim limitations are disclosed by the references discussed above and that the claims are unpatentable in view of these prior art references.

566. I reserve the right to supplement my opinions to address any information obtained, or positions taken, based on any new information that comes to light throughout this proceeding.

I declare under penalty of perjury that the foregoing is true and accurate to the best of my ability.

Executed on December 8, 2025



Scott Andrews.