

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Christopher

P.

Ricci

Saratoga

CA

US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention

FUNCTIONAL SPECIFICATION FOR A NEXT GENERATION AUTOMOBILE

Attorney Docket Number (if applicable)

6583-474-PROV

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number

☐ Firm or Individual Name

Customer Number

111285

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the invention was made by an agency of the United States Government. The U.S. Government agency name is:

☐ Yes, the invention was under a contract with an agency of the United States Government. The name of the U.S. Government agency and Government contract number are:

Entity Status

Applicant asserts small entity status under 37 CFR 1.27 or applicant certifies micro entity status under 37 CFR 1.29

- ☐ Applicant asserts small entity status under 37 CFR 1.27
- ☐ Applicant certifies micro entity status under 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
- ☒ No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Douglas W. Swartz/			Date (YYYY-MM-DD)	2013-04-15
First Name	Douglas W.	Last Name	Swartz	Registration Number (If appropriate)	37739

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DUPLICATED PROCESSING IN VEHICLES

CROSS REFERENCE TO RELATED APPLICATION

The present application is a continuation-in-part of U.S. Patent Application Serial No. 13/679,476, filed November 16, 2012, entitled "Vehicle Middleware", which claims the benefits of U.S. Provisional Application Serial Nos. 61/560,509, filed November 16, 2011; 61/637,164, filed April 23, 2012; and 61/663,335, filed June 22, 2012, all entitled "Complete Vehicle Ecosystem"; 61/646,747, filed on May 14, 2012, entitled "Branding of Electrically Propelled Vehicles Via the Generation of Specific Operating Sounds"; 61/653,275, filed on May 30, 2012, entitled "Vehicle Application Store for Console"; 61/653,264, filed on May 30, 2012, entitled "Control of Device Features Based on Vehicle State"; 61/653,563, filed on May 31, 2012, entitled "Complete Vehicle Ecosystem"; 61/672,483, filed on July 17, 2012, entitled "Vehicle Climate Control"; 61/714,016, filed on October 15, 2012, entitled "Vehicle Middleware"; and 61/715,699, filed October 18, 2012, entitled "Vehicle Middleware"; each of which is incorporated herein by this reference in its entirety.

Cross reference is made to U.S. Patent Application Nos. 13/420,236, filed on March 14, 2012, entitled, "Configurable Vehicle Console"; 13/420,240, filed on March 14, 2012, entitled "Removable, Configurable Vehicle Console"; 13/462,593, filed on May 2, 2012, entitled "Configurable Dash Display"; 13/679,459, filed on November 16, 2012, entitled "Vehicle Comprising Multi-Operating System"; 13/679,234, filed on November 16, 2012, entitled "Gesture Recognition for On-Board Display"; 13/679,412, filed on November 16, 2012, entitled "Vehicle Application Store for Console"; 13/679,857, filed on November 16, 2012, entitled "Sharing Applications/Media Between Car and Phone (Hydroid)"; 13/679,878, filed on November 16, 2012, entitled "In-Cloud Connection for Car Multimedia"; 13/679,875, filed on November 16, 2012, entitled "Music Streaming"; 13/679,676, filed on November 16, 2012, entitled "Control of Device Features Based on Vehicle State"; 13/678,673, filed on November 16, 2012, entitled "Insurance Tracking"; 13/678,691, filed on November 16, 2012, entitled "Law Breaking/Behavior Sensor"; 13/678,699, filed on November 16, 2012, entitled "Etiquette Suggestion"; 13/678,710, filed on November 16, 2012, entitled "Parking Space Finder Based on Parking Meter Data"; 13/678,722, filed on November 16, 2012, entitled "Parking Meter Expired Alert"; 13/678,726, filed on November

16, 2012, entitled “Object Sensing (Pedestrian Avoidance/Accident Avoidance)”;
13/678,735, filed on November 16, 2012, entitled “Proximity Warning Relative to Other
Cars”; 13/678,745, filed on November 16, 2012, entitled “Street Side Sensors”; 13/678,753,
filed on November 16, 2012, entitled “Car Location”; 13/679,441, filed on November 16,
5 2012, entitled “Universal Bus in the Car”; 13/679,864, filed on November 16, 2012, entitled
“Mobile Hot Spot/Router/Application Share Site or Network”; 13/679,815, filed on
November 16, 2012, entitled “Universal Console Chassis for the Car”; 13/679,476, filed on
November 16, 2012, entitled “Vehicle Middleware”; 13/679,306, filed on November 16,
2012, entitled “Method and System for Vehicle Data Collection Regarding Traffic”;
10 13/679,369, filed on November 16, 2012, entitled “Method and System for Vehicle Data
Collection”; 13/679,680, filed on November 16, 2012, entitled “Communications Based on
Vehicle Diagnostics and Indications”; 13/679,443, filed on November 16, 2012, entitled
“Method and System for Maintaining and Reporting Vehicle Occupant Information”;
13/678,762, filed on November 16, 2012, entitled “Behavioral Tracking and Vehicle
15 Applications”; 13/679,292, filed November 16, 2012, entitled “Branding of Electrically
Propelled Vehicles Via the Generation of Specific Operating Output”; 13/679,400, filed
November 16, 2012, entitled “Vehicle Climate Control”; __/ __, __, filed on ____,
2013, entitled “Improvements to Controller Area Network Bus”; 13/678,773, filed on
November 16, 2012, entitled “Location Information Exchange Between Vehicle and
20 Device”; 13/679,887, filed on November 16, 2012, entitled “In Car Communication Between
Devices”; 13/679,842, filed on November 16, 2012, entitled “Configurable Hardware Unit
for Car Systems”; 13/679,204, filed on November 16, 2012, entitled “Feature Recognition for
Configuring a Vehicle Console and Associated Devices”; 13/679,350, filed on November 16,
2012, entitled “Configurable Vehicle Console”; 13/679,358, filed on November 16, 2012,
25 entitled “Configurable Dash Display”; 13/679,363, filed on November 16, 2012, entitled
“Configurable Heads-Up Dash Display”; and 13/679,368, filed on November 16, 2012,
entitled “Removable, Configurable Vehicle Console”. The entire disclosures of the
applications listed above are hereby incorporated by reference, in their entirety, for all that
they teach and for all purposes.

FIELD

The disclosure relates generally to vehicle middleware systems and particularly to vehicle middleware systems for drivers and third-parties.

BACKGROUND

5 Modern vehicles use a number of communication systems and/or networks. Each of these communication systems and/or networks may have a bus structure that is open or proprietary. Each of these buses may also be specifically designed to work in a vehicle or may be available as a general communication protocol. These communication systems and/or networks connect the various individual components of the vehicles through their respective
10 buses. Examples of proprietary vehicle bus architecture include Controller Area Network (CAN) Bus, Local Interconnect Network (LIN) Bus, and the various Original Equipment manufacturer (OEM) Bus among others. Examples of open and general bus architecture include wired or wireless Ethernet and Low-Voltage Differential Signaling (LVDS) among others.

15 Taking the CAN bus for example, the CAN bus is a serial network developed primarily for use with automotive applications. CAN bus allows devices and microcontrollers in a vehicle to communicate with each other without a host computer.

The CAN protocol allows various devices and microcontrollers to be connected to a single CAN bus. According to the protocol, communication along the CAN bus is message-
20 based to allow messages and data to be sent from one connected device to another.

To facilitate communication on the CAN bus without the need of a host computer, CAN features an arbitration-free transmission mechanism. A CAN transmission includes an arbitration field (message ID) representing the priority of the message being transmitted. A dominant bit ('0') indicates a higher priority than a recessive bit ('1'). For example, in a
25 hypothetical two-bit ID CAN network, a device sending a '10' ID will have priority over a device sending a '11' ID on the CAN bus. In this example, both devices have a recessive bit in the first bit; however, the first device has a dominant second bit which could be used to arbitrate against a recessive second bit in the second device. The second device will back-off from transmitting over the bus upon this determination in favor of the second device and will
30 attempt to retransmit a few clock cycles after the first device has finished transmitting. It is recognized that each message ID transmitted must be unique over the CAN bus for this

arbitration-free transmission mechanism. According to the CAN specification, standard CAN (version 2.0A) uses 11-bit IDs, and extended CAN (version 2.0B) uses 29-bit IDs.

5 The CAN specification (ISO 11898) further described two types of CAN buses, the high-speed CAN bus (ISO 11898-2) (such as for engine, suspension, and transmission controllers and safety equipment) and the low-speed CAN bus (ISO 11898-3) (such as for
10 less critical components including non-safety sensors). The high-speed CAN bus is designed to carry data at high speed (up to 1Mbit/s in some implementation). The low-speed CAN bus is designed to carry data at a lower speed (up to 125Kbit/s in some implementation) but is more fault tolerant than the high-speed CAN bus. Further, the low-speed CAN bus can serve
15 as a back-up for the high-speed CAN bus in case there is a failure to the high-speed CAN bus.

As usage of the CAN standard evolves, many vehicles and systems implementing CAN are using both a high-speed and a low-speed CAN bus in parallel. The high-speed CAN bus carries information that is vital for vehicle operation or safety and is delivered to various
15 part of the vehicle or system in substantially real time. For example, the high-speed CAN bus would be used in a situation where an airbag deploys. When sensors in the bumper or at the front of the vehicle indicate that the vehicle has been involved in a frontal collision, the sensors can send priority information via the high-speed CAN bus to the airbag deployment unit to deploy the airbag. The low-speed CAN bus would be used for other less critical
20 applications.

A number of extensions have been proposed and used to extend the capabilities of the various bus architectures. For example, On-Board Diagnostics (OBD) adds support for requesting data from vehicle components for diagnostics purposes using Parameter Identifiers (PIDs). While OBD is designed to work with CAN bus, OBD can be implemented
25 to work with other general and/or OEM specific buses. Further, specific vehicle components such as the Engine Control Unit (ECU), Transmission Control Unit (TCU), Anti-lock Braking System (ABS), and generally Body Control Modules (BCMs) can have specific protocol extensions to work with the various bus architectures. Further, extensions to the bus architectures are needed to support carrying information regarding various environmental
30 type issues such as emissions information to comply with various government regulation mandates.

Vehicles, particularly passenger vehicles, are evolving rapidly with emerging safety, entertainment, and communication technologies. Existing vehicle bus protocols, which are largely designed for safety, are generally unsuitable for other non-safety communications, due to low bus bandwidth and transmission speed. There are therefore various needs in the art including improving information flow between vehicle components, leveraging the various communication systems and/or networks in the art to enhance vehicle safety, data security, and/or data processing, and providing remote authorized third party (*i.e.* peace officers, vehicle manufacturers, vehicle security services, and owners) access to a vehicle's functions and state information while maintaining security against unauthorized parties and components.

SUMMARY

These and other needs are addressed by the various aspects, embodiments, and/or configurations of the present disclosure. The present disclosure is directed to a vehicle having a variety of networking and other capabilities.

The vehicle can include:

(a) a plurality of processing modules to control a plurality of automated vehicle tasks, functions and/or operations, a first processing module being in an active mode whereby the first processing module is in primary control of at least most automated vehicle functions and/or operations and a second processing module being in a standby mode whereby the second processing module is ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

A non-transient, tangible computer readable medium can include microprocessor executable instructions that, when executed, designate a first processing module as being in an active mode whereby the first processing module is in primary control of at least most automated vehicle tasks, functions and/or operations and a second processing module as being in a standby mode whereby the second processing module is ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

A method can include the step of:

designating, by an arbitration module, a first processing module as being in an active mode, whereby the first processing module is in primary control of at least most automated vehicle tasks, functions and/or operations, and a second processing module as being in a

standby mode, whereby the second processing module is ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

The plurality of automated vehicle tasks, functions and/or operations can include monitoring, controlling and/or operating a plurality of the following: an engine and/or power
5 control unit, transmission control unit (TCU), a door setting, a window setting, a blind spot monitor, an airbag deployment control unit, a collision sensor, a nearby object sensing system, a seat belt control unit, a sensor for a seat belt setting, a power source controller, an energy output sensor, an engine temperature sensor, oil pressure, hydraulic pressure, a headlight, an emergency light, a brake light, a parking light, a fog light, an interior and/or
10 passenger compartment light, a tail light, a vehicle control system sensor, a wireless network, a cellular data sensor, a steering sensor, a torque sensor, an engine, power steering, a display panel, switch state control unit, and a brake control unit.

The plurality of automated vehicle tasks, functions and/or operations can include monitoring, controlling and/or operating a plurality of the following: an emissions system, a
15 seating system controller and/or sensor, an entertainment system, monitoring an ambient (outdoor) weather sensor, an odometer reading sensor, a trip mileage reading sensor, a road condition sensor, a radar transmitter/receiver output, a brake wear sensor, an oxygen sensor, an ambient lighting sensor, a vision system sensor, a ranging sensor, a parking sensor, a heating, venting, and air conditioning (HVAC) system and/or sensor, a water sensor, a air-
20 fuel ratio meter, a hall effect sensor, a microphone, a radio frequency (RF) sensor, and/or an infrared (IR) sensor.

For a first set of tasks, functions, and/or operations, the first processing module can be in primary control and the second processing module is in standby mode and, for a different second set of tasks, functions, and/or operations, the second processing module can
25 be in primary control and the first processing module is in standby mode.

In the standby mode, the second processing module can at least one of (a) perform shadow processing of the at least most automated vehicle tasks, functions and/or operations and (b) synchronize stored time-stamped processing state information with time-stamped processing state information regarding the at least most automated vehicle tasks, functions
30 and/or operations.

The first and second processing modules can be in wireless communication with one another, such that a state of the second processing module is maintained substantially in synchronicity with a state of the first processing module to enable a stateful failover from the first processing module to the second processing module.

5 The vehicle can include an arbitration module to arbitrate hand-off conflicts between duplicated first and second processing modules.

The arbitration module can select one of the first and second processing modules to currently possess and/or own a token, the token indicating which processing module is an active processing module and/or which processing module is a standby processing module.

10 The vehicle can include a health check module to determine a corresponding state of health of each of the duplicated first and second processing modules to perform at least one of critical and non-critical tasks, functions, and operations.

The health check module can perform a check and/or test, in response to an internally generated interrupt and/or request to determine a selected processing module's ability to
15 perform critical and/or non-critical vehicle tasks, functions, and/or operations, assign a score to the selected processing module based on the check and/or test results, and compare the score to one or more thresholds and/or to a score of a different processing module to determine a state of health to determine a state of health of the selected processing module.

The arbitration module, based on the relative and/or absolute state of health of each of
20 the first and second processing modules can select one of the first and second processing modules as a primary processing module in primary control of the at least most automated vehicle tasks, functions and/or operations and the other of the first and second processing modules as a secondary processing module in standby mode.

A hand-off procedure, initiated by the health check and/or arbitration modules, can be
25 activated whereby primary control is passed from the first processing module to the secondary processing module and the first processing module enters the standby mode. The relative weighting of at least some tasks, functions and/or operations in assigning the score can be a function of geographic location of the vehicle.

The vehicle described in the present disclosure can provide a number of advantages.
30 For example, the vehicle can provide for improved control of data stream management and integration to accommodate the ever-increasing sophistication of each data segment and

enable data sharing amongst all segments. It can enable interoperability amongst diverse systems. It can provide an open architecture, thereby obviating existing constraints on design changes due to locked-in technology. It can enable drivers freely and conveniently to integrate his or her digital lifestyle into a vehicle while enabling voice and fingertip
5 activation. It can implement a dynamic software environment and on board vehicle network that does not need to change over technology generations. Car manufacturers can have the freedom to specify any type of processor, memory or storage technology and to make appropriate changes at any time. The architecture can integrate presentation functions, sensor/control functions and infotainment functions in a highly modular extensible way
10 ensuring that the system design can scale up or down easily and evolve over many model years without battling technological obsolescence. For example, the architecture can allow the vehicle owner and/or manufacturer to upgrade and/or add application engines, upgrade the in-vehicle networking capabilities, upgrade Internet connectivity, upgrade display capabilities, and migrate to high availability capabilities, all without radical changes to the
15 software environment and/or for inter- and intra-model line differentiation. The vehicle can support multiple processing and expansion modules that anchor specific functions to a selected processor. It can support a variety of embedded Electronic Control Unit (“ECU”) data sources, such as those provided by LIN, CAN, and FlexRay, and IPv6 connectivity that enables seamless migration to Ethernet-based sensor technology and new bus architectures
20 supported by the AutoStar initiative. It can employ a single data management hub, providing improved vehicle safety in the face of security threats posed by connectivity to the Ethernet. It can enable vehicle manufacturers to manage multiple display subsystems that are unique to the subsystem location in the vehicle and deliver vehicle occupants a personalized experience. The subsystems can include, for example, a console display (providing
25 information and input/output control), a configurable dashboard display, a configurable heads-up display, and passenger display units. Configurable displays allow drivers to add/change gauges for non-vehicle operation information that is displayed on the dashboard and heads-up display to suit user preferences and needs. Direct video can be delivered through display controllers and/or an interactive touch screen, optionally equipped with
30 proximity sensors, all implemented with Ethernet-based intelligent display subsystems. Handheld devices, such as personal digital assistants, cellular phones, and tablet and laptop

computers, can interface wirelessly, via one or more tethered networks, with the vehicle's processing module(s) and be integrated into the processing resources available to perform vehicle-related tasks, operations, and functions. Assignment of an IPv6 address or other electronic address on a network to the vehicle can provide an address to locate the vehicle on the Internet (or other network), simplify implementing cyber security, enable applications that support safety and data collection for predictive analytics, enable voice-over-IP calls from the vehicle, and furnish reliable presence information to a presence service or server.

These and other advantages will be apparent from the disclosure.

The phrases "at least one", "one or more", and "and/or" are open-ended expressions that are both conjunctive and disjunctive in operation. For example, each of the expressions "at least one of A, B and C", "at least one of A, B, or C", "one or more of A, B, and C", "one or more of A, B, or C" and "A, B, and/or C" means A alone, B alone, C alone, A and B together, A and C together, B and C together, or A, B and C together.

The term "a" or "an" entity refers to one or more of that entity. As such, the terms "a" (or "an"), "one or more" and "at least one" can be used interchangeably herein. It is also to be noted that the terms "comprising", "including", and "having" can be used interchangeably.

The term "automatic" and variations thereof, as used herein, refers to any process or operation done without material human input when the process or operation is performed. However, a process or operation can be automatic, even though performance of the process or operation uses material or immaterial human input, if the input is received before performance of the process or operation. Human input is deemed to be material if such input influences how the process or operation will be performed. Human input that consents to the performance of the process or operation is not deemed to be "material".

The term "automotive navigation system" is a satellite navigation system designed for use in automobiles. It typically uses a GPS navigation device to acquire position data to locate the user on a road in the unit's map database. Using the road database, the unit can give directions to other locations along roads also in its database. Dead reckoning using distance data from sensors attached to the drivetrain, a gyroscope and an accelerometer can be used for greater reliability, as GPS signal loss and/or multipath can occur due to urban canyons or tunnels.

The term “bus” and variations thereof, as used herein, refers to a subsystem that transfers information and/or data between various components. A bus generally refers to the collection communication hardware interface, interconnects, bus architecture, and/or protocol defining the communication scheme for a communication system and/or communication network. A bus may also be specifically refer to a part of a communication hardware that interfaces the communication hardware with the interconnects that connect to other components of the corresponding communication network. The bus may be for a wired network, such as a physical bus, or wireless network, such as part of an antenna or hardware that couples the communication hardware with the antenna. A bus architecture supports a defined format in which information and/or data is arranged when sent and received through a communication network. A protocol may define the format and rules of communication of a bus architecture.

A “communication channel” refers to an analog and/or digital physical transmission medium such as cable (twisted-pair wire, cable, and fiber-optic cable) and/or other wireline transmission medium, and/or a logical and/or virtual connection over a multiplexed medium, such microwave, satellite, radio, infrared, or other wireless transmission medium. A channel is used to convey an information signal, for example a digital bit stream, from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second. Channel performance measures that can be employed in determining a quality or grade of service of a selected channel include spectral bandwidth in Hertz, symbol rate in baud, pulses/s or symbols/s, digital bandwidth bit/s measures (e.g., gross bit rate (signaling rate), net bit rate (information rate), channel capacity, and maximum throughput), channel utilization, link spectral efficiency, signal-to-noise ratio measures (e.g., signal-to-interference ratio, Eb/No, and carrier-to-interference ratio in decibel), bit-error rate (BER), packet-error rate (PER), latency in seconds, propagation time, transmission time, and delay jitter.

The terms “communication device,” “smartphone,” and “mobile device,” and variations thereof, as used herein, are used interchangeably and include any type of device capable of communicating with one or more of another device and/or across a communications network, via a communications protocol, and the like. Exemplary communication devices may include but are not limited to smartphones, handheld computers,

laptops, netbooks, notebook computers, subnotebooks, tablet computers, scanners, portable gaming devices, phones, pagers, GPS modules, portable music players, and other Internet-enabled and/or network-connected devices.

5 A “communication modality” refers to a protocol- or standard defined or specific communication session or interaction, such as Voice-Over-Internet-Protocol (“VoIP”), cellular communications (e.g., IS-95, 1G, 2G, 3G, 3.5G, 4G, 4G/IMT-Advanced standards, 3GPP, WIMAX™, GSM, CDMA, CDMA2000, EDGE, 1xEVDO, iDEN, GPRS, HSPDA, TDMA, UMA, UMTS, ITU-R, and 5G), Bluetooth™, text or instant messaging (e.g., AIM, Blauk, eBuddy, Gadu-Gadu, IBM Lotus Sametime, ICQ, iMessage, IMVU, Lync, MXit, Paltalk, 10 Skype, Tencent QQ, Windows Live Messenger™ or MSN Messenger™, Wireclub, Xfire, and Yahoo! Messenger™), email, Twitter (e.g., tweeting), Digital Service Protocol (DSP), and the like.

The term “communication system” or “communication network” and variations thereof, as used herein, refers to a collection of communication components capable of one or 15 more of transmission, relay, interconnect, control, or otherwise manipulate information or data from at least one transmitter to at least one receiver. As such, the communication may include a range of systems supporting point-to-point to broadcasting of the information or data. A communication system may refer to the collection individual communication hardware as well as the interconnects associated with and connecting the individual 20 communication hardware. Communication hardware may refer to dedicated communication hardware or may refer a processor coupled with a communication means (*i.e.*, an antenna) and running software capable of using the communication means to send a signal within the communication system. Interconnect refers some type of wired or wireless communication link that connects various components, such as communication hardware, within a 25 communication system. A communication network may refer to a specific setup of a communication system with the collection of individual communication hardware and interconnects having some definable network topography. A communication network may include wired and/or wireless network having a pre-set to an ad hoc network structure.

30 The term “computer-readable medium” as used herein refers to any tangible storage and/or transmission medium that participate in providing instructions to a processor for execution. Such a medium may take many forms, including but not limited to, non-volatile

media, volatile media, and transmission media. Non-volatile media includes, for example, NVRAM, or magnetic or optical disks. Volatile media includes dynamic memory, such as main memory. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, magneto-
5 optical medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, a solid state medium like a memory card, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. A digital file attachment to e-mail or other self-contained information archive or set of archives is
10 considered a distribution medium equivalent to a tangible storage medium. When the computer-readable media is configured as a database, it is to be understood that the database may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Accordingly, the disclosure is considered to include a tangible storage medium or distribution medium and prior art-recognized equivalents and successor media, in which the
15 software implementations of the present disclosure are stored.

The terms “dash” and “dashboard” and variations thereof, as used herein, are used interchangeably and include any panel and/or area of a vehicle disposed adjacent to an operator, user, and/or passenger. Typical dashboards may include but are not limited to one or more control panel, instrument housing, head unit, indicator, gauge, meter, light, audio
20 equipment, computer, screen, display, HUD unit, and graphical user interface.

The terms “determine”, “calculate” and “compute,” and variations thereof, as used herein, are used interchangeably and include any type of methodology, process, mathematical operation or technique.

The term “display” refers to a portion of a screen used to display the output of a
25 computer to a user.

The term “displayed image” or “displayed object” refers to an image produced on the display. A typical displayed image is a window or desktop or portion thereof, such as an icon. The displayed image may occupy all or a portion of the display.

The term “electronic address” refers to any contactable address, including a telephone
30 number, instant message handle, e-mail address, Universal Resource Locator (“URL”),

Universal Resource Identifier (“URI”), Address of Record (“AOR”), electronic alias in a database, like addresses, and combinations thereof.

5 The term “means” as used herein shall be given its broadest possible interpretation in accordance with 35 U.S.C., Section 112, Paragraph 6. Accordingly, a claim incorporating the term “means” shall cover all structures, materials, or acts set forth herein, and all of the equivalents thereof. Further, the structures, materials or acts and the equivalents thereof shall include all those described in the summary of the invention, brief description of the drawings, detailed description, abstract, and claims themselves.

10 The term “module” as used herein refers to any known or later developed hardware, software, firmware, artificial intelligence, fuzzy logic, or combination of hardware and software that is capable of performing the functionality associated with that element. Also, while the disclosure is presented in terms of exemplary embodiments, it should be appreciated that individual aspects of the disclosure can be separately claimed.

15 The terms “online community”, “e-community”, or “virtual community” mean a group of people that primarily interact via a computer network, rather than face to face, for social, professional, educational or other purposes. The interaction can use a variety of media formats, including wikis, blogs, chat rooms, Internet forums, instant messaging, email, and other forms of electronic media. Many media formats are used in social software separately or in combination, including text-based chat rooms and forums that use voice, 20 video text or avatars.

The term “presence” is a status indicator that conveys ability and willingness of a potential communication partner—for example a user—to communicate. A user’s client provides presence information (presence state) via a network connection to a presence service, which is stored in what constitutes his personal availability record (called a 25 presentity) and can be made available for distribution to other users (called watchers) to convey his availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging or recent implementations of voice over IP clients. A user client may publish a presence state to indicate its current communication status. This published state informs 30 others that wish to contact the user of his availability and willingness to communicate. The most common use of presence today is to display an indicator icon on instant messaging

clients, typically from a choice of graphic symbols with easy-to-convey meanings, and a list of corresponding text descriptions of each of the states. Even when technically not the same, the “on-hook” or “off-hook” state of called telephone is an analogy, as long as the caller receives a distinctive tone indicating unavailability or availability.

5 The term “satellite positioning system receiver” refers to a wireless receiver or transceiver to receive and/or send location signals from and/or to a satellite positioning system, such as the Global Positioning System (“GPS”) (US), GLONASS (Russia), Galileo positioning system (EU), Compass navigation system (China), and Regional Navigational Satellite System (India).

10 The term “social network service” is a service provider that builds online communities of people, who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web-based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.

15 The term “social network” refers to a web-based social network.

 The term “screen,” “touch screen,” or “touchscreen” refers to a physical structure that enables the user to interact with the computer by touching areas on the screen and provides information to a user through a display. The touch screen may sense user contact in a number of different ways, such as by a change in an electrical parameter (e.g., resistance or capacitance), acoustic wave variations, infrared radiation proximity detection, light variation
20 detection, and the like. In a resistive touch screen, for example, normally separated conductive and resistive metallic layers in the screen pass an electrical current. When a user touches the screen, the two layers make contact in the contacted location, whereby a change in electrical field is noted and the coordinates of the contacted location calculated. In a
25 capacitive touch screen, a capacitive layer stores electrical charge, which is discharged to the user upon contact with the touch screen, causing a decrease in the charge of the capacitive layer. The decrease is measured, and the contacted location coordinates determined. In a surface acoustic wave touch screen, an acoustic wave is transmitted through the screen, and the acoustic wave is disturbed by user contact. A receiving transducer detects the user
30 contact instance and determines the contacted location coordinates. The touch screen may or

may not include a proximity sensor to sense a nearness of object, such as a user digit, to the screen.

The term “vehicle” refers to a device or structure for transporting animate and/or inanimate or tangible objects (e.g., persons and/or things), such as a self-propelled conveyance. The term “vehicle” as used herein includes any conveyance, or model of a conveyance, where the conveyance was originally designed for the purpose of moving one or more tangible objects, such as people, animals, cargo, and the like. The term “vehicle” does not require that a conveyance moves or is capable of movement. Typical vehicles may include but are in no way limited to cars, trucks, motorcycles, busses, automobiles, trains, railed conveyances, boats, ships, marine conveyances, submarine conveyances, aircraft, space craft, flying machines, human-powered conveyances, and the like.

The preceding is a simplified summary of the disclosure to provide an understanding of some aspects of the disclosure. This summary is neither an extensive nor exhaustive overview of the disclosure and its various aspects, embodiments, and/or configurations. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure but to present selected concepts of the disclosure in a simplified form as an introduction to the more detailed description presented below. As will be appreciated, other aspects, embodiments, and/or configurations of the disclosure are possible utilizing, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts a vehicle configured in accordance with an embodiment;

Fig. 2 is a block diagram of a processing module according to an embodiment;

Fig. 3 depicts a vehicle implementing processing modules configured in accordance with an embodiment;

Fig. 4 depicts a flow diagram of a health-check method according to an embodiment;

Fig. 5 depicts a flow diagram of a hand-off procedure method according to an embodiment;

Fig. 6 depicts a flow diagram of a system stand-by method according to an embodiment;

Fig. 7 depicts a flow diagram of a processor off-load method according to an embodiment;

Fig. 8 depicts a flow diagram according to an embodiment;

Fig. 9 depicts a flow diagram according to an embodiment;

5 Fig. 10 depicts a flow diagram according to an embodiment;

Fig. 11 depicts a flow diagram according to an embodiment;

Fig. 12 depicts a flow diagram according to an embodiment;

Fig. 13 depicts a flow diagram according to an embodiment;

Fig. 14 depicts a flow diagram according to an embodiment;

10 Fig. 15 is a block diagram of a computational system according to an embodiment;

Fig. 16 is a block diagram of an input/output system according to an embodiment;

Fig. 17 depicts a flow diagram according to an embodiment;

Fig. 18 depicts a flow diagram according to an embodiment;

Fig. 19 depicts a flow diagram according to an embodiment;

15 Fig. 20 is a block diagram of a vehicle computational system according to an embodiment;

Fig. 21 depicts a flow diagram according to an embodiment;

Figs. 22A-B depict configurations of input/output systems according to an embodiment;

20 Fig. 23 depicts a flow diagram according to an embodiment;

Fig. 24 depicts a flow diagram according to an embodiment;

Fig. 25 depicts a flow diagram according to an embodiment;

Fig. 26 depicts a flow diagram according to an embodiment;

Fig. 27 depicts a communication system according to an embodiment;

25 Fig. 28 depicts a flow diagram according to an embodiment;

Fig. 29 depicts a flow diagram according to an embodiment;

Fig. 30 depicts a flow diagram according to an embodiment; and

Fig. 31 depicts a flow diagram according to an embodiment.

DETAILED DESCRIPTION

30 Overview

The present disclosure describes a vehicle implementing one or more processing modules. These modules are configured to connect and interface with the various buses in the vehicle, where the various buses are connected with the various components of the vehicle to facilitate information transfer among the vehicle components. Each processing module is further modularized with the ability to add and replace other functional modules now or in the future. These functional modules can themselves act as distinct vehicle components. Each processing module may hand-off processing to other modules depending on its health, processing load, or by third-party control. Thus, the plurality of processing modules help to implement a middleware point of control to the vehicle with redundancy in processing and safety and security awareness in their applications.

Exemplary processing modules include one or more of:

(a) an active-active or active-standby duplicated processing module configurations in fully or partially wirelessly networked vehicles;

(b) an arbitration module to handle hand-off conflicts in duplicated processing module configurations;

(c) a health check module which checks critical and non-critical tasks, functions, and operations of each processing module to determine which to designate as the active or primary processing module;

(d) a displayed object movement module to move displayed objects from a source input/output system to a target or destination input/output system ;

(e) a media filter which filters and/or processes (e.g., formats, configures, changes a presentation mode of, and/or otherwise causes at least part of the signal to be altered from the signal as received) third party sourced signals, particularly multimedia signals, in a manner consistent with a vehicle universal or occupant-specific whitelist, blacklist, or other user preference, sensed occupant context, and/or a governing federal, state, provincial, and/or local law or regulation;

(f) in a vehicle equipped with an internal wireless network and optionally bus-type network, a network selector which selects a network for signal transmission based on network/node status, signal/noise ratio, type of signal, available and/or unavailable bandwidth, network performance parameter(s) (e.g., availability, packet drop or loss, jitter,

latency, buffer capacity, throughput, and the like) quality of service, and/or other parameters and configures the signal for transmission over the selected network;

(g) a diagnostic module handles warning/error signals in a predetermined manner;

(h) a remote control module which receives a request from a remote source or
5 third party to command a vehicle function (which function may be identified by a suitable function-specific code), authenticates the requestor, and if successfully authenticated and if privileged to request the performance of the vehicle function, executes the request notwithstanding a contrary command from the vehicle operator;

(i) a media controller, which receives a media stream from a remote node,
10 identifies which input/output systems are disabled (and/or restricted) due to operator command and/or as a result of governing law, and provides the media stream to an input/output system associated with the associated occupant;

(j) an installation supervisor which, for a newly installed software and/or hardware and/or other device (such as an on-board sensor, processing module or component
15 thereof, software application, circuit board, expansion module or component thereof (which expansion module may be hardware, software, or a combination thereof), critical or non-critical device (such as those discussed above with respect to the critical or non-critical system controller(s)), cellular upgrade module (e.g., 2G, 3G, 4G, 5G, LTE, or other cellular standard upgrade or Subscriber Identity Module (“SIM”) card, board, or other upgrade
20 module, and the like), determines whether the newly installed component satisfies defined functional and/or source or reuse requirements and/or restrictions for the component, license restrictions, and other criteria, and, if satisfied, creates data structures in the component (if it has a resident memory) and the vehicle memory to bind the component to the current vehicle;

(k) a computational module selector to perform processing load balancing over
25 multiple processing modules;

(l) network security which isolates a component encountering a security breach event and/or isolates the primary processing module from other components in the local network if the former is not possible;

(m) a “cone of silence” capability by the media controller for external
30 computational devices;

(n) an automated caching, potentially by individual input/output systems, by the media controller of media based on various factors;

(o) a presence reporting module considering local laws in determining whether an individual is present (e.g., for unified communications) and, if so, by what communication channel(s) and/or modalities; and

(p) a networking module to enable processing modules of different vehicles to wirelessly connect for to exchange vehicle information.

~~(p)~~ These and other features are discussed in this disclosure and in the attached Exhibit "A", which is incorporated herein by this reference.

The Vehicle

Figs. 1, 3, and 15 collectively illustrate a vehicle 100 incorporating various features.

Referring to Fig. 1, the vehicle 100 includes, among many components common to vehicles, wheels 104, a power source 108 (such as an engine, motor, or energy storage system (e.g., battery or capacitive energy storage system)), a manual or automatic transmission 112, a manual or automatic transmission gear controller 116, a power controller 120 (such as a throttle), a braking system 136, a steering wheel 140, a display panel 144 (e.g., a dashboard displaying information regarding components in vehicle 100), and an occupant seating system 148.

Other components in vehicle 100 include communication components such as a wireless signal receiver 152 to receive wireless signals from signal sources such as roadside beacons and other electronic roadside devices, and a satellite positioning system receiver 156 (e.g., a Global Positioning System ("GPS") (US), GLONASS (Russia), Galileo positioning system (EU), Compass navigation system (China), and Regional Navigational Satellite System (India) receiver).

The vehicle 100 also includes a number of control units and sensors for the various components of vehicle 100. Exemplary control units and sensors therefore include wheel state sensor 160 to sense one or more of vehicle speed, acceleration, deceleration, wheel rotation, wheel speed (e.g., wheel revolutions-per-minute), wheel slip, and the like. Power source controller and energy output sensor 164 controls the power source and to senses a power output of the power source 108. Example aspects of power source controller and energy output sensor 165 include balancing the mixture of fuel (e.g. gasoline, natural gas, or

other sources of fuel) and other elements (e.g. air for combustion) and measuring one or more of current engine speed (e.g., revolutions-per-minute), energy input and/or output (e.g., voltage, current, fuel consumption, and torque), and the like. Switch state control unit 168 activates or deactivates the power source (e.g. the ignition). Transmission control unit 5 (“TCU”) 170 sets the current state the transmission (e.g., gear selection or setting) based on the state of gear controller 116. Power control unit 174 sets the throttle for power source 108 given the state of power controller 120. Brake control unit 176 operates the current state (braking or non-braking) of braking system 136 based on the state of the brake controller (which could be linked to power controller 120).

10 Vehicle 100 also includes other control units and sensors for safety purposes. An airbag deployment system includes an airbag deployment control unit 133 and a collision sensor 132. When a collision is detected by collision sensor 132, data is sent to airbag release control unit 133 which determines whether to deploy the airbag based on the data received (e.g., the speed of the collision and the area of impact to determine whether an 15 airbag deployment can promote safety). Other safety components include seat belt control unit and sensors for setting the seat belt (e.g. engaging or disengaging the seat belt during hard breaking), head light control unit and sensors for headlight 128 and other lights (e.g. emergency light, brake light, parking light, fog light, interior or passenger compartment light, and/or tail light state (on or off)), door settings (locking and unlocking), window settings 20 (opening or closing), one or cameras or other imaging sensors (which commonly convert an optical image into an electronic signal but may include other devices for detection objects such as an electromagnetic radiation emitter/receiver that emits electromagnetic radiation and receives electromagnetic waves reflected by the object) to sense objects, such as other vehicles and pedestrians and optionally determine the distance, trajectory and speed of such 25 objects, in the vicinity or path of the vehicle, and other components and sensors as known in the art.

Vehicle 100 further includes components for the convenience and enjoyment of the occupants or operators. Seating system controller and sensor 178 sets the position and other settings of a seat and measure various attributes of an occupant of the seat (e.g., the current 30 weight of seated occupant) in a selected seat of the seating system 148. Entertainment system

190, preferably located in the head unit of the passenger compartment, provides entertainment options such as music or video for occupants of vehicle 100.

Examples of other vehicle components include one or more cameras or other imaging sensors (which commonly convert an optical image into an electronic signal but may include
5 other devices for detection objects such as an electromagnetic radiation emitter/receiver that emits electromagnetic radiation and receives electromagnetic waves reflected by the object) to sense objects, such as other vehicles and pedestrians and optionally determine the distance, trajectory and speed of such objects, in the vicinity or path of the vehicle, odometer reading sensor, trip mileage reading sensor, wind speed sensor, radar transmitter/receiver output,
10 brake wear sensor, steering/torque sensor, oxygen sensor, ambient lighting sensor, vision system sensor, ranging sensor, parking sensor, heating, venting, and air conditioning (HVAC) sensor, water sensor, air-fuel ratio meter, blind spot monitor, hall effect sensor, microphone, radio frequency (RF) sensor, infrared (IR) sensor, vehicle control system sensors, wireless network sensor (e.g., Wi-Fi and/or Bluetooth sensor), cellular data sensor,
15 and other sensors known to those of skill in the vehicle art.

Vehicle 100 includes one or more vehicle buses 180 for connecting the various components and systems of vehicle 100 as described above. In modern vehicles, subsystems such as an anti-lock braking system (ABS), which may be used by brake control unit 176 and braking system 136, engine control unit (ECU), which may be used by power source control
20 164, transmission control unit (TCU), which may be used by transmission control unit 170 and gear controller 116, and supplemental restraint system (SRS), such as airbag deployment control unit 133 and collision sensor 132 and seating system controller and sensor 178, are frequently interconnected using a standardized bus. Standardized buses for use in vehicles include Controller Area Network (CAN), and Local Interconnect Network (LIN) and others,
25 as are known in the art. In particular, these components and subsystems may use the high-speed CAN bus for real-time information. Other components with lower priorities may use the low-speed CAN bus to transmit information. Vehicle bus 180 (which is optional) is illustrated as one bus in Fig. 1. However, vehicle 100 may include one or more of these standardized buses, such as a combination of the high-speed and low-speed CAN, LIN,
30 and/or other buses. Also, vehicle bus 180 may further include and support extensions to standardized buses, such as the FlexCAN extension to the CAN bus. Further, vehicle bus 180

may include standardized communication networks that can be implemented vehicle 100. Well known networks include Ethernet, Wi-Fi, USB, I²C, RS232, RS485 and FireWire.

Vehicle 100 also includes processing module 124. Preferably, processing module 124 is placed in the trunk, hood (not shown), behind the head unit (not shown), and/or other
5 accessible but unseen locations. Processing module 124 is coupled to vehicle bus 180 and provides processing for data related to vehicle bus 180 and other vehicle components.

Processing modules, for example, can perform, monitor, and/or control critical and non-critical tasks, functions, and operations, such as interaction with and/or monitoring and/or control of critical and non-critical on board sensors and vehicle operations (e.g.,
10 engine, transmission, throttle, brake power assist/ brake lock-up, electronic suspension, traction and stability control, parallel parking assistance, occupant protection systems, power steering assistance, self-diagnostics, event data recorders, steer-by-wire and/or brake-by-wire operations, vehicle-to-vehicle interactions, vehicle-to-infrastructure interactions, partial and/or full automation, telematics, navigation/SPS, multimedia systems, audio systems, rear
15 seat entertainment systems, game consoles, tuners (SDR), heads-up display, night vision, lane departure warning, adaptive cruise control, adaptive headlights, collision warning, blind spot sensors, park/reverse assistance, tire pressure monitoring, traffic signal recognition, vehicle tracking (e.g., LoJackTM), dashboard/instrument cluster, lights, seats, climate control, voice recognition, remote keyless entry, security alarm systems, and wiper/window control).
20 Processing modules can be enclosed in an advanced EMI-shielded enclosure containing multiple expansion modules. Processing modules can have a “black box” or flight data recorder technology, containing an event (or driving history) recorder (containing operational information collected from vehicle on board sensors and provided by nearby or roadside signal transmitters), a crash survivable memory unit, an integrated controller and circuitry
25 board, and network interfaces. Processing module 124 is further disclosed with reference to Fig. 2.

As set forth below and as shown in Fig. 3, multiple processing modules 124a-c may be located at various locations in a common vehicle. The disparate, spaced apart locations of the processing modules 124a-c provide redundancy in the event of a collision or other
30 catastrophic event. For example, a collision with the rear of the vehicle 100 may damage the processing module 124c but not the processing modules 124a,b.

As will be appreciated, the multiple processing modules 124a-c may be configured to operate in an active/active and/or active/standby mode. These operating modes describe the manner in which first and second (redundant) devices operate under normal conditions. In active/standby implementations, only the primary device in a pair processes information and issues commands. The standby device sits idle, ready to assume the active role should the primary device fail. The standby device may receive, from the primary device, processing, command, and primary device state information to facilitate stateful failover, but it does not itself commonly perform meaningful work until the primary device fails. In active/active implementations, both devices are online and collaboratively process information and issue commands under normal conditions. When one device fails, all processing is handled by the remaining device.

A user can be an occupant of a vehicle 100 that implements the system of Fig. 1. A user can further be an assembler, technician, or mechanic working on the vehicle to configure the system of Fig. 1 for use by an end-user of the vehicle.

Fig. 2 illustrates an exemplary block diagram for a (primary and/or secondary) processing module 124a-c.

Processing module 124 may include processor 210, memory 220, storage 230, and interfaces for one or more buses 240-270. Among the interfaces 240-270 include high-speed CAN bus 240, low-speed CAN bus 250, LIN bus 260, network interface 270, and/or wireless interface 280. One skilled in the art will recognize that processing module 124 may take other configurations and with other buses as known in the art, and interfaces 240-290 may be implemented with more or fewer buses than those shown.

The operations of processing module 124 will now be described with respect to the high-speed CAN bus interface 240 and low-speed CAN bus interface 250 as an exemplary configuration in one embodiment of the invention. In one implementation, processing module 124 receives data transmitted over vehicle bus 180 through high-speed CAN bus interface 240 and/or low-speed CAN bus interface 250. Data transmitted over the high-speed CAN bus includes priority data from subsystems such as anti-lock braking system (ABS), which may be used by brake control unit 176 and braking system 136, engine control unit (ECU), which may be used by power source control 164, transmission control unit (TCU), which may be used by transmission control unit 170 and gear controller 116, and

supplemental restraint system (SRS), such as airbag deployment control unit 133 and collision sensor 132 and seating system controller and sensor 178, as described above. Data transmitted over the low-speed CAN bus includes other noncritical data, such as engine temperature and oil pressure sensor readings.

5 Wireless interface 280, by contrast, can be a transceiver for one or more long, intermediate, or short range wireless networks, such as a radio (e.g., cellular such as CDMA, GSM, or IS-95 network), 802.X, a WiFi™ network, a Bluetooth™ network, and the like, sending and receiving a wide variety of information, including lower priority information, such as data for the convenience and enjoyment of the occupants in entertainment system 190
10 or seating system 148. The wireless interface 280 can access information over one or more wireless networks using an appropriate protocol, such as the Wireless Application Protocol, Wireless Internet Protocol, Wireless Session Protocol, Bluetooth Wireless Protocol, Wireless Datagram Protocol, Wireless HART Protocol, Wired Equivalent Privacy (WEP), MiWi and MiWi P2P, RuBee (IEEE standard 1902.1), Wireless USB, Wireless Transport Layer
15 Security (WTLS), and the like. 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.

 Local network interface 270 is a transceiver for signals exchanged with other on
20 board components of the vehicle (including the components discussed above with respect to Fig. 1). The signals may be sent over a wired or wireless (or combination thereof) network. In one configuration, the local network interface is a wireless access point. Any suitable local area network protocol may be used, with the Ethernet protocol and the short-range protocols mentioned above being examples.

25 The processor 210 may comprise a general purpose programmable (micro) processor or controller for executing application programming or instructions. In accordance with at least some embodiments, the processor 210 may include multiple processor cores, and/or implement multiple virtual processors. In accordance with still other embodiments, the processor 210 may include multiple physical processors. As a particular example, the
30 processor 304 may comprise a specially configured application specific integrated circuit (ASIC) or other integrated circuit, a digital signal processor, a controller, a hardwired

electronic or logic circuit, a programmable logic device or gate array, a special purpose computer, or the like. The processor 210 generally functions to run programming code or instructions implementing various functions of the device 200.

Memory 220 for use in connection with the execution of application programming or instructions by the processor 210, and for the temporary or long term storage of program instructions and/or data. As examples, the memory 220 may comprise RAM, DRAM, SDRAM, or other solid state memory. Alternatively or in addition, data storage 230 may be provided. Like the memory 220, the data storage 230 may comprise a solid state memory device or devices. Alternatively or in addition, the data storage 230 may comprise a hard disk drive or other random access memory.

Fig. 3 depicts a vehicle 300 with multiple processing modules according to an embodiment. Vehicle 300 includes bus 180, vehicle component 310, and processing modules 124A-C.

Vehicle component 310 is an exemplary vehicle component for illustration purposes that is connected to bus 380. Vehicle component 310 may represent any of the vehicle components discussed in connection with vehicle 100 (Fig. 1).

Each of the processing modules 124A-C is coupled to bus 180. Processing module 124A is located in the engine compartment of vehicle 300; processing module 124B is located in the passenger compartment of vehicle 300; and processing module 124C is located in the truck of vehicle 300.

In one configuration, some of the processing modules 124A-C may have limited processing functions as compared to the others. For example, processing module 124A may act as the default processing module for vehicle 300 normally because of its location being close to most critical vehicle components in the engine compartment (*i.e.*, ECU, TCU). If the other processing modules 124B-C are only needed for redundancy, they may be implemented to only have limited capabilities (*i.e.*, these processing modules would not be required to have processing all critical and non-critical functions). This implementation has the advantage of reduced costs and/or space as compared to fitting processing module with full capabilities. The processing modules 124A-C may also have cascading levels of capabilities. For example, processing module 124B is fitted in the passenger compartment and is deemed to most likely survive a collision; it may be required to have capabilities critical to vehicle

operation but no other capabilities to save space in the passenger compartment. Processing module 124C may have additional capabilities such as a cellular module so that emergency calls may be automatically placed if the default processing module 124A fails.

5 In another configuration, each of the processing modules 124A-C may have different capabilities. For example, processing module 124A may have capabilities only for critical vehicle functions; processing module 124C may have capabilities only for non-critical vehicle functions; and processing module 124B may be reserved for back-up processing of both critical and non-critical vehicle functions. In one implementation, processing may be off-loaded to another processing module if one module becomes overloaded. This
10 configuration has the advantage of a further reduction in costs and space because processing power is not wasted due to redundancy. In the case where one processing module malfunctions, the other processing modules may pick up processing duties via a processor off-load procedure. If there is not enough processing power for all wanted functionalities, the processing modules may work together to prioritize critical vehicle functions ahead of
15 non-critical functions.

Fig. 20 depicts computational modules and data structures in memory 220 according to an embodiment.

An arbitration module 2000 selects a processing module to currently possess or own token 2004 (which is used to designate the processing module 124, in an active-standby
20 configuration, being the active or standby processing module or, in an active-active configuration, having the responsibility for certain tasks, functions, or operations, such as critical tasks, operations, or functions, while the other processing module has responsibility for other different tasks, operations, or functions, such as non-critical tasks, operations, or functions.

25 A health check module 2008 performs checks or tests, in response to internally generated interrupts or requests from the other processing module, its ability to perform both critical and non-critical tasks, functions, and operations. Individual scores and composite or cumulative scores for the tasks, functions, and operations can be determined and compared to thresholds to determine an absolute state of health and/or to the individual and/or cumulative
30 scores of the other processing module to determine a relative state of health.

Critical system controller(s) control, monitor, and/or operate critical systems.

Critical systems can include one or more of (depending on the particular vehicle) monitoring, controlling, and/or operating the ECU, TCU, door settings, window settings, and/or blind spot monitor, monitoring, controlling, and/or operating the safety equipment (e.g., airbag deployment control unit 133, collision sensor 132, nearby object sensing system, seat belt control unit, sensors for setting the seat belt, *etc.*), monitoring and/or controlling certain critical sensors such as the power source controller and energy output sensor 164, engine temperature, oil pressure sensing, hydraulic pressure sensors, sensors for headlight 128 and other lights (e.g., emergency light, brake light, parking light, fog light, interior or passenger compartment light, and/or tail light state (on or off)), vehicle control system sensors, wireless network sensor (e.g., Wi-Fi and/or Bluetooth sensor), cellular data sensor, and/or steering/torque sensor, controlling the operation of the engine (e.g., ignition), head light control unit, power steering, display panel, switch state control unit 168, power control unit 174, and/or brake control unit 176, and/or issuing alerts to a user and/or remote monitoring entity of potential problems with a vehicle operation.

Non-critical system controller(s) 2016 control, monitor, and/or operate non-critical systems. Non-critical systems can include one or more of (depending on the particular vehicle) monitoring, controlling, and/or operating a non-critical system, emissions control, seating system controller and sensor 178, entertainment system 190, monitoring certain non-critical sensors such as ambient (outdoor) weather readings (e.g., temperature, precipitation, wind speed, and the like), odometer reading sensor, trip mileage reading sensor, road condition sensors (e.g., wet, icy, *etc.*), radar transmitter/receiver output, brake wear sensor, oxygen sensor, ambient lighting sensor, vision system sensor, ranging sensor, parking sensor, heating, venting, and air conditioning (HVAC) system and sensor, water sensor, air-fuel ratio meter, hall effect sensor, microphone, radio frequency (RF) sensor, and/or infrared (IR) sensor.

On board sensor monitor(s) 2020 include interfaces to receive signals from and transmit signals to a corresponding on-board sensor, including the on-board sensors discussed above, and the logic to monitor sensor operation and readings.

The displayed object movement module 2024 monitors display input received from occupants for commands to move a displayed object from a first display to a different second display in the vehicle for viewing by, for instance, a different occupant. The display input

may include, for example, a sensed gesture, an icon selection, or other input indicative to a desire or request to move a displayed object from the first display to the second display. The moved object may or may not be retained for view on the first display after movement.

5 The diagnostic module 2028 handles warning/error signals in a predetermined manner. The signals, for instance, can be presented to a third party and/or occupant and/or cause the performance of on board diagnostics.

10 The media filter 2032 filters third party sourced signals, particularly multimedia signals, in a manner consistent with a vehicle universal or occupant-specific whitelist, blacklist, or other user preference, sensed occupant context, and/or a governing federal, state, provincial, or local law or regulation.

15 The network selector 2036 selects a network for signal transmission based on network/node status, signal/noise ratio, type of signal, available and/or unavailable bandwidth, network performance parameter(s) (e.g., availability, packet drop or loss, jitter, latency, buffer capacity, throughput, and the like) quality of service, and/or other parameters and configures the signal for transmission over the selected network.

20 The remote control module 2040 receives a request from a remote source or third party to command a vehicle function (which function may be identified by a suitable function-specific code), authenticates the requestor, and if successfully authenticated and if privileged to request the performance of the vehicle function, executes the request notwithstanding a contrary command from the vehicle operator. The requestor can, for example, be a vehicle owner, a law enforcement authority, a vehicle manufacturer, a lender having a loan collateralized by the vehicle, and the like.

25 The installation supervisor 2044, for a newly installed software and/or hardware and/or other device (such as an on-board sensor, processing module 124 or component thereof, software application, circuit board, expansion module 290 or component thereof (which expansion module 290 may be hardware, software, or a combination thereof), critical or non-critical device (such as those discussed above with respect to the critical or non-critical system controller(s) 2012 and 2016), cellular upgrade module (e.g., 2G, 3G, 4G, 5G, LTE, or other cellular standard upgrade or Subscriber Identity Module (“SIM”) card, board, 30 or other upgrade module, and the like), determines whether the newly installed component satisfies defined functional and/or source or reuse requirements and/or restrictions for the

component, license restrictions, and other criteria, and, if satisfied, creates data structures in the component (if it has a resident memory) and the vehicle memory 220 to bind the component to the current vehicle.

5 The media controller 1524 receives a media stream from a remote node, identifies which input/output systems are disabled due to operator command and/or as a result of governing law, and provides the media stream to an input/output system associated with the associated occupant.

10 The computational module selector 2052 identifies the computational modules, particularly software applications, currently available within the local area network of the vehicle, the identification including not only the type (*e.g.*, game, multimedia, music, utility, and the like), source or vendor (*e.g.*, Apple, Microsoft, and the like), capabilities and requirements (*e.g.*, operating system, processing, memory, display, and other requirements) but also the version of the computational module, and records this information in memory 220. The selector 2052 can select not only, for duplicated computational modules, a most
15 current version of the duplicated module to execute and a computational platform (*e.g.*, first, second, . . . processing module or external computational device 1532) for the execution.

The presence reporting module 2056 considers local laws, individual (contactee) context, and other factors in determining whether an individual (contactee) is present (*e.g.*, for unified communications) and, if so, by what communication channel(s).

20 The social networking module 2070 creates, manages, and/or maintains a social networking session with one or more other vehicles. The social networking module 2070 can identify operational vehicles having an occupant in a social networking relationship with an occupant of the selected vehicle, notify one or both occupants of the capability of instantiating a social networking session, and effectuate and maintain such a session.

25 In one application, processing module 124 is configured to process information sent over the CAN buses. As priority data is received by processing module 124 from high-speed CAN bus interface 240 and/or low-speed CAN bus 250, processing module 124 may determine the nature of the received data and independently do further processing on the received data. In a preferred embodiment, processor 210 executes instructions stored in
30 memory 220 to perform these functions. Further, memory 220 serves as stores and retrieves for data by processor 210.

In one configuration, processing module 124 only receives data over high-speed CAN bus 240 and may send the data back over low-speed CAN bus 250. As the CAN bus provides arbitration-free transmission, processing module 124 may passively listen to information traffic, which includes priority data from the various components as discussed, sent over high-speed CAN bus 240. Processing module 124 then determines if a piece of received information may need further processing and should be sent to devices via low-speed CAN bus 250.

For example, collision sensor 132 may have detected a frontal collision. In one data path, collision sensor 132 may send a signal with details to the collision (*i.e.*, areas of impact and/or force and/or velocity of impact) over high-speed CAN bus 240 with specific target to airbag release control unit 133 to potentially deploy the airbags once airbag release control unit 133 determines that it is suitable to do so upon the receipt of the sent data. Since the CAN bus is arbitration-free, processing module 124 also receives the collision information from collision sensor 132. Processing module 124 then processes the information received to determine to relay the information to an information display (*i.e.*, display console of entertainment system 190) via the low speed CAN bus 250.

It is noted that the data rate is limited in the current implementations of the CAN bus. However, future implementations may allow for higher speeds such that the CAN bus may support data rate suitable for multimedia application. In these implementations, processing module 200 may be configured to leverage the CAN bus for multimedia use. For example, real-time multimedia information (*i.e.*, analog/digital radio or television signal) may be received by an antenna and transmitted through a CAN bus via processing unit 200 to entertainment system 190. At some point in time, one component of vehicle 100 may have suffered a malfunction that requires information the driver. In the default implementation of the CAN bus, the higher priority signal from the malfunctioning component will have priority over the multimedia information. With the leveraged CAN bus by processing module 200, the high priority signal from the malfunctioning component can be further processed by processor 210. If processor 210 determines that the malfunction is minor, processor 210 may relay the malfunction information to the low speed CAN bus 250 but being mixed in with the multimedia information such that there is little disruption to playing backing the multimedia information. Further, processor 210 may also consider if the

malfunction requires further processing such as notification to a repair facility or emergency services.

In another configuration, processing module 200 may leverage other buses such as the network interface 270 and/or wireless interface 280 that have more bandwidth for the data. For example, while the present implementation of the CAN bus would not support multimedia information with any substantial bit rate, the network interface 270 may be leveraged such that while CAN bus information is received via the high speed CAN bus 240, multimedia information is relayed separately via the network interface 270. This enables the processing module 200 to implement the previous example discussed involving relaying information regarding malfunctioning component without waiting for a future implementation of the CAN bus.

In another application, a processing module 124 may add further expansion modules 290A-N for further capabilities. For example, expansion modules 290A-N may contain a cellular telephony module. The cellular telephony module can comprise a GSM, CDMA, FDMA, or other digital cellular telephony transceiver and/or analog cellular telephony transceiver capable of supporting voice, multimedia and/or data transfers over a cellular network. Additionally, expansion modules 290A-N can include other cellular telephony modules from different providers or modes for other wireless communications protocols. As examples, the modules for other wireless communications protocols can include a Wi-Fi, BLUETOOTH TM, WiMax, infrared, or other wireless communications link. The cellular telephony module and the other wireless communications module can each be associated with a shared or a dedicated antenna. Further, expansion modules 290A-N may also include other wired bus modules that may connect to additional essential and nonessential vehicle components that may be installed or upgraded in the future. Processing modules 290A-N may contain functions critical to the operation of the vehicle such as engine control (ECU), transmission control (TCU), airbag control, various sensors, or other operational or safety related components. Further, processing modules 290 may take on more processing duties from a vehicle component 310 connected to bus 380. Thus, processing modules 124A-C benefits from redundancy in the case that one of modules malfunctions. Further, in a vehicle collision, it is expected that at least some of the processing modules may totally malfunction.

In these cases, the remaining processing modules may take over limited or full processing duties of the malfunctioning vehicle components 310 or processing modules 390A-C.

In one configuration, processor 210, memory 220, storage 230, and the bus interfaces 240-280 may also be expansion modules similar to 290A-N. For example, processor 210
 5 may be initially implemented as an OMAP 4 processor. In the future, OMAP 5 processors may be developed and processor 210 may be upgraded as a modular component.

In another application, processing module 124 is able to support additional vehicle hardware and/or software components that are added to the vehicle and is connected to processing module 124 via a bus. For example, vehicle 100 may have installed an additional
 10 entertainment system. In one configuration, processing module 124 can treat the additional component that is connected to processing module 200 via a bus as an expansion module 290A-N.

In another configuration, the additional hardware and/or software component may require further processing for it to work with processing module 124. For example, the bus
 15 protocol may need to be modified to support communicating with the additional component because the additional component has capabilities beyond the existing protocol (*i.e.*, an extension to an existing bus architecture). In one implementation, processing module 124 must first check to ensure that the additional component complies with OEM defined standards such that rogue components not recognized for a particular vehicle would not be
 20 supported.

Fig. 15 depicts the vehicle 100 in communication, via first, second, . . . networks 1504 a, b, . . . , with a remote node 1500, such as a computational device, *e.g.*, a server, mobile phone, tablet computer, laptop computer, personal computer, and the like, of the vehicle owner, law enforcement authority, insurance company, vehicle or parts
 25 manufacturer/vendor (*e.g.*, to provide vehicle diagnostics, maintenance alerts, vehicle or part recall notifications, and/or predictive analytics), a service provider (*e.g.*, a convenience service provider such as a service to connect the vehicle operator with a dealer, a service to locate the vehicle, a service to provide vehicle information and/or feature assistance, an automotive navigation system service and a service to start a vehicle (OnStar™ being an
 30 example), a location-based service provider (*e.g.*, traffic and/or weather reporting and/or adviser on gas, accommodations, navigation, parking assistance, and/or food), Internet

content provider, software vendor, concierge service provider, a processing module of another vehicle, a roadside monitor, sign, beacon, and the like, to name a few.

The first, second, . . . networks 1504a,b, . . . can be any wireless network, such as a radio or cellular network (e.g., CDMA, CDMA2000, AMPS, D-AMPS, TACS, ETACS,
5 CSK, CDMAOne, GSM, EDGE, GPRS, HSCSD, UMTS, WCDMA, HSPA, WIMAX, WIMAX ADVANCED, LTE ADVANCED, or FDMA in accordance with the 1G, 2G, 2G transitional, 3G, 3G transitional, 4G or 5G cellular network standards), a Wi Fi network, a Bluetooth network, and the like.

The vehicle 100 includes a transceiver 1508 to send and receive signals over a
10 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 1504a, b, . . ., primary and secondary processing modules 124a 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
15 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
20 computers, and the like. As will be appreciated, the logic for the gateway/firewall 1512, media controller 1524 and network controller 1528 can be contained within memory/storage 220, 330. The various components are connected by a bus, wireless network, or combination thereof (denoted by reference 1536).

The gateway/firewall can be any suitable module that can maintain secure
25 connectivity. The need for the gateway/firewall is necessitated by the assignment of a wireless data network address, such as defined by IPv6 (Internet Protocol version 6), with the corresponding processing module 124. As will be appreciated, IPv6 addresses, as commonly displayed to users, consist of eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:0000:8a2e:0370:7334.

30 Each processing module 124 can have an independent network address or use a common network address. The gateway can be any module equipped for interfacing with

another network that uses one or more different communication protocols. The firewall can use any technique to maintain security, including network address translation, network layer or packet filtration, application-layer firewall, and the like.

Fig. 16 depicts an exemplary input/output architecture for the vehicle 100. The architecture includes first, second, . . . nth input/output systems 1600a-n, the media controller 1524, display controller(s) 1604 to receive user input via the input/output system(s) and configure the output presented by the input/output system(s) to the user, audio controller(s) 1608 to control audio output to the user, and rule sets 1612 (stored in memory/storage 220, 230) to regulate corresponding features/functions of the vehicle 100, particularly the information and/or other output provided to each occupant by a respective input/output system. Generally, each of the multiple occupants has a separate and corresponding input/output system 1600. For example, each seat 148 can have a corresponding input/output system 1600.

As can be appreciated, the functionality disclosed herein may be affected by the geographical location and/or movement of a vehicle. A vehicle may cross a jurisdictional line where different laws exist that concern behavior in or about vehicles. These laws may be stored, as one or more rule set(s) 1612, in a database on-board and/or remotely accessible by the vehicle. A vehicle may use its location-based features to determine the appropriate applicable laws and enable or disable certain features to a user. For example, in the event that an individual crosses a state line where the local laws prohibit texting while driving, the vehicle may disable texting for the vehicle operator. This blocking would not prevent others in a vehicle from texting, and if allowed may provide for the operator to continue to send voice-activated texts, etc. Movement and location of the vehicle may be determined using location-based features as described herein. Moreover, to prevent false blocking of features, a specific user device position may be determined by sensors on the device, sensors in the vehicle, and/or combinations thereof. Although described with reference to blocking the texting ability of a specific user, it can be appreciated that the ability to surf the Internet, view photos, access streaming content, and other predetermined distractions may also be disabled.

For an additional external computational device 1532 that connects to processing module 124 via wireless interface 280, a secured connection protocol is needed. Unlike a

wired bus connection, which is generally electronically confined to vehicle 100, a wireless connection via wireless interface 280 may be broadcast to other communication systems within the vicinity of vehicle 100. Thus, other wireless communication hardware, systems, and networks might be able to communicate with the communication system of the vehicle 100. This ability is potentially a security hazard.

To resolve this issue, wireless security rules should be used to ensure that only trusted devices, such as the external computational device 1532, communicate wirelessly, via the wireless interface 280, with the on board vehicle components through the wireless interface 280. Such security is provided by the gateway/firewall 1512 applying known security algorithms. In one implementation, wireless security may be implemented by the gateway/firewall 1512 using the current security setup in the 802.11 standard such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) or other security systems as known in the art. OEMs may also choose to implement security by using a propriety security system and/or wireless protocol to work with the in-vehicle wireless communication network.

Upgrading the vehicle 100 using different processing modules and/or other on board components, such as on board sensors 1516, can be done securely and seamlessly. A limit may be imposed on the place and manner in which an additional component communicating via the in-vehicle wireless network may be added to the vehicle 100. For example, installation of the additional component may only be available at an automobile shop or may even more limited to only in OEM approved shops or dealership to ensure that the newly installed component is fully tested to communicate only with vehicle 100 and not with other adjacent vehicles.

To facilitate this process, a handshake procedure may be used during the initial installation of the component. In one implementation, an OEM approved shop may have codes that will allow the new component to accept a link with vehicle 100. During this handshake procedure, vehicle 100 and its relevant components, such as processing module 200, may negotiate a protocol and/or security settings to communicate with the new component. For example, a symmetric or asymmetric code or key pair may be developed for encrypting communications. Alternatively, codes for WEP, WPA, or other security systems as known in the art may be developed for secured communication. After this initial

handshake procedure, the new component and vehicle 100 will not have to do any further security setup in the future to prevent leaking the secured codes. In a further implementation, the new component is considered married or bound to vehicle 100 and may not communicate with any other vehicles unless unmarried or unbound when the component is removed at an approved shop. The dedication of the component to the vehicle may be done by using a unique code, such as a serial number of the component or vehicle, to enable a type of routine licensing compliance check when the car is activated. This can be done, for example, by comparing a unique code received by the installed component from another vehicle component or by the other vehicle component from the installed component. The licensing check is successful when the received code matches a code stored in memory of the receiving device.

In another configuration, the additional, or installed, component may also communicate wirelessly with other vehicle components of vehicle 100 without needed processing module 200 to relay any communication. This may be done by sharing a vehicle encryption scheme and code for the wireless use. This may be useful for emergency purposes (*i.e.*, the police may have a need to control certain components in a vehicle).

Operation of Arbitration and Health Check Modules 2000 and 2008

The processing modules 124 can use any of a variety of techniques to determine relative status and/or processing role of each. For example, under one technique a token is passed to signify the active or passive processing module or the processing module performing a specified set of processing operations. The processing module in possession of the token at any one time has the status and/or is responsible for the set of processing operations associated with the token. Rules may be used to arbitrate between the processing modules when each asserts ownership and/or non-ownership of the token.

By way of illustration, the processing modules 124 can determine which module is active and which is standby by employing the following rules. Upon detection of a selected stimulus (e.g., at vehicle start-up, processing module power-up, and/or periodically during vehicle or processing module operation), the health check module 2008 in each processing module 124 runs self-tests or queries the health check module 2008 other processing module 124 to perform selected computational tasks and provide the result. The processing modules 124 thus exchange messages with each other. Based on the results of its self-test (or queried

tests), each processing module 124 decides whether it can become active. If so, the processing module 124 asserts an available signal to an arbitration module 2000, which propagates the signal to the other processing module 124. The arbitration module 2000, applying rules, chooses the active processing module 124 and forwards the token to the
5 selected processing module 124, along with an interrupt. Rules may include a default selection, an ordered, random or pseudorandom periodic change in which processing module 124 is active and which is standby, which processing module 124 is healthier (or has a higher state of health score, the relative capabilities of the processing modules 124 (with the more capable processing module being active), and the like. The arbitration module 2000
10 propagates a token non-ownership signal to the other processing module 124, along with an interrupt. Each processing module 124, in response, sets its status in memory to “primary” or “standby”. If the active processing module 124 is removed, powered down, or voluntarily de-asserts ownership or possession of the token, the standby processing module immediately receives the available token 2004, along with an interrupt. It then assumes, and records in
15 memory, the primary state.

In one variation, arbitration is performed by the arbitration module 2000 using a health check procedure 400 shown in Fig. 4.

Health check procedure 400 by the health check module 2008 is one way in which each processing modules 124A-C may self-check to determine a respective state of health
20 (e.g., if the processing modules remains fully functional or is only partially functional). Health check procedure 400 may be activated by each processing module 124 or one of the other processing modules 124 at a certain time interval or may be manually activated by user (i.e., a user directly activating the module or whenever the ignition is started). Health check procedure 400 may also be continuously running while the vehicle 300 is running to ensure
25 the fastest response time in case a collision occurs resulting in an immediate loss of processing functions.

In step 410, the health check module 2008 in each processing module 124 performs a health check on its critical tasks, functions or operations of which losing one would result in a potentially critical loss to vehicle operation. As discussed previously, the critical tasks,
30 functions or operations may include, for example (depending on the particular vehicle), monitoring, controlling, and/or operating a critical system. Health check 410 may involve

procedures such as testing or monitoring that each critical function or operation is operating within predetermined or selected operating parameters and/or causing each critical component (safety equipment, selected sensors, engine, power steering, and/or brakes) to operate within selected operating parameters. In some configurations, a critical system, such as the ECU, may include both critical (i.e., engine failure) and non-critical tasks or functions (i.e., minor oil leak). Health check 410 may be configured to check only the critical tasks or functions.

In pass test check 411, if any malfunction to a critical task, function or operation is detected, the procedure activates hand-off procedure in step 440, which will be discussed with reference to Fig. 5. In one variation, a cumulative score is computed for all critical tasks, functions, and operations. The individual scores of the tasks, functions, and operations and cumulative score for the processing module is provided to the arbitration module 2000, which compares both sets of scores for the two processing modules 124 and selects and designates the healthier of the two processing modules 124 as the primary or active processing module 124.

If the processing module 124 passes test check 411, health check on non-critical tasks, functions or operations 420 is performed. Non-critical tasks, functions or operations may include, for example (depending on the particular vehicle) monitoring, controlling, and/or operating a non-critical system. In step 420, health check is done on various functions of the non-critical system, with each function having a score for passing the health check. The score may be adjusted according to the level non-criticality of the system. For example, an emissions control unit, while it may be non-critical to vehicle operation, may nonetheless be fairly important so as to comply with environmental regulations; therefore an emissions control unit could be weighted a comparatively high score for passing. In contrast, an entertainment system's failure may not be deemed to be important (except for operator/occupant inconvenience) and may be weighted with a relatively low score for passing.

In step 421, the score is tabulated for all non-critical systems and compared to see if it is above a certain threshold. If the score is below the threshold, a hand-off procedure is activated in step 450. For example, if emissions control by the processing module 124 is detected to be failing, causing or potentially causing harmful gas emissions to rise

significantly above the legal limit, health check 421 may give a very low score to this non-critical system. Therefore, even if the entertainment system is working perfectly, health check may still give a score that is below the threshold and hand-off procedure will be activated.

5 In one configuration, the score weight for each non-critical system may be defined dynamically according to the location of the vehicle or other factors. For example, vehicle-use laws may affect how a non-critical system should be weighted (i.e., the stringency of emissions law, noise control law, or other laws in one area). Thus, vehicle -use laws may be provided by an organization, governmental entity, group, individual, and/or combinations
10 thereof. The laws may be stored locally or retrieved from a remotely located storage. The vehicle-in-use laws may be statutes and/or regulations that are enforced by a government entity, such as a city, municipality, county, province, state, country, and the like. These laws may define vehicle, traffic, transportation, and/or safety rules associated with a given geographical region. An exemplary vehicle-in-use law governs texting, cellular phone use,
15 and video availability to the operator when the car is in motion and the like). The laws may be updated from time to time to, among other things, account for changes in the laws. Thus, a first task, operation, or function may be critical in a first geographic location but noncritical in a different second geographic location. Likewise, a first task, operation, or function may be non-critical and have a first score (if operating properly) in a first geographic location but
20 be non-critical and have a lower second score (if operating properly) in a second geographic location.

 In step 430, if the score for non-critical systems is above the threshold, the active processing module 124 may be continued to be used as the active processor. In one variation, a cumulative score is computed for all non-critical tasks, functions, and operations.
25 The individual scores of the tasks, functions, and operations and cumulative score for the processing module is provided to the arbitration module, which compares both sets of scores for the two processing modules and selects and designates the healthier of the two processing modules as the primary or active processing module.

 The operation of a an arbitration module 2000 procedure 500 for a processing module
30 will now be discussed with reference to Fig. 5.

The arbitration module 2000 can activate a token arbitration procedure 500 by steps 440 and 450 (Fig. 4) where either (a) the one or more critical tasks, functions, and operations has failed health check or (b) where one or more non-critical tasks, functions, and operations has not tabulated enough score to represent that the selected processing module is healthy enough for processing. Arbitration may be based on an absolute and/or relative state-of-health.

In step 510, a health check is performed, by a respective health check module 2008, on each processing module 124 and the pass/fail results and scoring information reported to the other processing modules 124 and/or the arbitration module 2000.

In step 514, the arbitration module 2000 selects a next processing module 124 (until all are considered) and proceeds to decision diamond 518.

In decision diamond 518, the arbitration module 2000 determines whether the selected processing module 124 passes the health test on set of critical tasks, functions, and operations. If so, the arbitration module 2000 proceeds to decision diamond 524.

In decision diamond 524, the arbitration module 2000 determines whether the selected processing module 124 passes the health test on set of non-critical tasks, functions, and operations. If so, the arbitration module 2000 proceeds to step 528.

In step 528, the arbitration module 2000 creates or updates data structures indicating that the selected processing module 124 is healthy and recording the selected processing module's respective scoring information. Optionally, the arbitration module 2000 can determine and record the relative state-of-health of the selected processing module 124 relative to other processing modules.

When the selected processing module 124 fails to pass one or more sets of critical tasks, functions, and operations (decision diamond 518) or non-critical tasks, functions, and operations (decision diamond 524), the arbitration module 2000 proceeds to step 532 and creates or updates data structures indicating that the selected processing module 124 is unhealthy and recording the selected processing module's respective scoring information. Optionally, the arbitration module 2000 can determine and record the relative state-of-health of the selected processing module 124 relative to other processing modules.

After performing steps 528 or 532, as appropriate, and when no processing module 124 remains to be analyzed, the arbitration module 2000 proceeds to decision diamond 536.

In decision diamond 536, the arbitration module 2000 determines whether a healthy processing module 124 is available and, when available, designates, in step 540, the healthiest (based on absolute or relative state-of-health or both) processing module 124 as the active processing module 124 (or, in an active-active configuration, as being primarily responsible for handling critical tasks, functions, and operations).

When no healthy processing module 124 is available, the arbitration module 2000 implements emergency measures, activates an alarm indicating that there is currently no available healthy processing module 124, and reports the alarm to the user and/or a remote node 1500, such as the vendor, manufacturer, servicing entity, roadside service, and the like.

The emergency measures implemented can vary by application. In one application, the emergency measure is to identify which processing module 124 is healthy to perform each set of critical and optionally non-critical tasks, functions and operations. If a healthy processing module exists for each set of critical and optionally non-critical tasks, functions and operations, the arbitration module 2000 assigns each set of critical and optionally non-critical tasks, functions, and operations to a processing module 124 having a sufficiently high health score (e.g., above a selected threshold) to perform the selected set of critical and optionally non-critical tasks, functions and operations. Where multiple processing modules are healthy enough to perform the selected set of critical and optionally non-critical tasks, functions and operations, the arbitration module 2000 can select the processing module having the highest health score for the selected set of critical and optionally non-critical tasks, functions and operations and/or having the highest available or unused processing units or resources to perform the selected set of critical and optionally non-critical tasks, functions and operations. Where no processing module 124 is healthy to perform a selected set of critical and optionally non-critical tasks, functions and operations, the selected set of critical and optionally non-critical tasks, functions, and operations can be performed by a remote node, via first, second, . . . network 1504a, b, The remote node 1500 can be, for example, the vendor, manufacturer, servicing entity, roadside service, and the like. In one application, the critical and optionally non-critical tasks, functions, and operations are performed by a remote node 1500, via first, second, . . . network 1504a, b, . . . , rather than by a local or on board processing module 124.

An important aspect of an active-standby configuration can be how to maintain synchronicity between the active and standby processing modules to enable “hot” hand-offs, which can be particularly important for automotive applications, without loss of memory as to the current operational state of the vehicle and its component tasks, functions, and operations. One technique is to have the standby processing module 124 perform “shadow” processing in which it receives all input received by the active processing module 124 and performs the same processing tasks, functions, and operations as the active processing module 124. The assumption is that the two processing modules 124 have identical processing rates and therefore, at any one time, precisely duplicate the other as to processing state of completion as to any task, function, and/or operation. Due to varying processing loads on the processing modules, delays in signal transmissions, and other factors, this assumption may or may not be true. Another technique is to have the standby processing module 124 receive, and store in memory 220, time-stamped processing state information from the active processing module 124. The time-stamped processing state information relates to any processing task, function or operation currently being performed by the active processing module 124 and the results thereof. A potential issue with this approach is latency between the current and reported states of the active processing module 124. Another technique is a combination of the foregoing techniques. In this technique, the standby processing module 124 performs “shadow processing” but periodically checks its processing state information against the time-stamped processing state information received from the active processing module 124 and resets, alters, or updates its state information to reflect the received processing state information. Where a processing string is being performed correctly, it does not typically need to be revised to reflect a potentially earlier point reflected in the received and time stamped state information (which may be delayed). A reset to an earlier point in the processing string may be appropriate where the standby processing module 124 is too far ahead of the active processing module 124. The primary purpose of this combined approach is to confirm processing accuracy by the standby processing module 124 and to keep the standby processing module 124 from getting too far in advance of the active processing module 124 in processing information.

Operation of Remote Control Module 2040

Fig. 27 depicts a particular configuration of a remote node 1500. The remote node 1500, configured as a central repository for vehicle information, includes a server 2700 and associated database 2704. The remote node 1500 is in wireless communication, via network 1504, with first, second, . . . nth vehicles 100a-n. Currently, car drivers have the option to sign up for a service like General Motors OnStar® to remotely unlock cars, and provide other features such as remote start, tracking vehicles, and/or locking cars, etc.

In some embodiments, the present disclosure is directed to a central repository 2704 that can be used in conjunction with an individual vehicle. The central repository may be stored remotely (as shown) or on-board the vehicle. In the event that the central repository is stored remotely, it may be supervised by a law enforcement agency, or secure administrative agency. It is anticipated that strong security procedures may be employed to avoid hacker attacks, especially if stored at a remote central repository like the Department of Motor Vehicles (DMV), or other security-approved location. In the event that a vehicle is stolen, the true owner of a vehicle may prove ownership to the central repository and locate, lock, shutdown, etc. the vehicle.

Commonly, the requested vehicle function is one or more of accelerate, decelerate, activate, deactivate, provide current vehicle location, broadcast audible and/or visual message to vehicle operator, brake, set a maximum, vehicle velocity, and lock doors. The requested vehicle function can be identified by a function-specific code. The remote control module can map the function-specific code in a look up table indexing function-specific codes with corresponding vehicle functions to determine the requested vehicle function to be performed.

In another embodiment, a police device may communicate to another vehicle to slowly reduce that vehicle's speed, shutdown the engine, cut power, etc. The communication can be securely effected using unique codes or other cryptographic techniques. Moreover, the communication may be through a server associated with a central repository. It is anticipated that the module controlling these functions is securely guarded and designed to prevent hacking attempts.

The operation of a system stand-by procedure 600 implemented by a remote control module 2040 and/or other component of a processing module 124 will now be discussed with reference to Fig. 6. Stand-by procedure 600 may be activated when the selected processing

module 124 transitions from active to standby or standby to active or in response to a command from the operator or the remote node 1500. In one configuration, stand-by procedure 600 may also be activated manually by the driver of the vehicle or by another third party. For example, the driver or another third party may wish to disable certain aspects of vehicle 300 (*i.e.*, the driver may wish to disable certain functions, either critical or non-critical, of the vehicle to prevent another user of the vehicle, such as a valet, from accessing them, a third party, which may be the police or a theft prevention service such as On-Star, may wish to disable a stolen vehicle or a vehicle which is otherwise in violation of the law).

Manual activation of stand-by procedure 600 may be done locally or remotely. For local activation, an additional component in the form of a switch may be added and connected to the processing module via a bus or as an expansion module 290A-N. The driver may then manually activate the switch as needed.

Most likely, manual activation of stand-by procedure 600 is done remotely (*i.e.*, by the police, theft prevention service, or the owner of the vehicle at a remote location). As such, in one implementation, the corresponding processing module may be accessed via a non-physical bus such as by wireless interface 280. However, this is not the preferred method. As discussed previously, vehicle components communicating with a processing module wirelessly should only work with a secured scheme. The in-vehicle wireless network should not be accessible to third parties for further security purposes. A direct access to the in-vehicle wireless bus would defeat these principles. The wireless interface 280 may have a limited range such that connection and control can only be effected within the vicinity of the vehicle. Nevertheless, this implementation may be useful in cases where there is an emergency that is within the vicinity of the vehicle (*i.e.*, emergency road closure) that requires a third party such as the police to disable passing vehicles for safety reasons. In such cases, the authorized third party may activate codes that bypasses securities of the in-vehicle wireless network that is normally off-limit and directly access the processing module.

In another implementation, the vehicle may have a cellular or satellite communication component that has the capability of accessing an outside cellular or other communication network. Alternatively, this communication component may be installed as an additional expansion module 290A-N as discussed previously. Access to processing module is granted through a valid security verification within this component. Therefore, access to the

processing module using this implementation does not require open access to the in-vehicle wireless bus.

5 In another configuration, stand-by procedure 600 may also be activated by a control system within the vehicle when some automated condition is met. For example, a leased or rental car company may wish to limit the geographical location where the vehicle can be driven. The vehicle may be automatically disabled if it is detected that the vehicle has left the allowed zone of operation (*i.e.*, detected via a GPS).

10 In step 601, the method confirms if any critical subsystem would be unavailable. As discussed above, a critical subsystem may be unavailable because it did not pass the health check, because it was disabled by the driver or a third party, or because some automated condition has been met.

15 If critical subsystems are unavailable, step 610 performs general vehicle stand-by. In one configuration, general vehicle stand-by disables all components of the vehicle rendering the vehicle unusable. However, this may lead to safety issues where a sudden shut-down of the vehicle while operating on the road may be hazardous to both the driver of the vehicle and other vehicle on the road. In another configuration, general vehicle stand-by performs a shut-down of non-critical systems while placing a limit on critical system designed to bring the vehicle to stop. For example, a speed limiter may limit the speed of the vehicle to a minimal speed so that the vehicle can be brought to a safe stop subsequently but cannot
20 operate effectively. After the vehicle is brought to a stop, general shut-down that disables all components of the vehicle may be performed.

25 In step 620, an alarm is activated to inform about the status of a general stand-by. Here, similar to step 540, an alarm is normally sent to at least components like display 144 or entertainment system 190 of vehicle 100 via a reliable bus such as the high speed CAN bus to inform the driver of the generally stand-by. In one implementation, an alarm may also be sent to a remote node 1500, such as a service or maintenance provider, e.g., a nearby or a default car repair facility with possible system diagnosis information, emergency services if it is detected that a emergency affecting road safety has occurred, and/or to car manufacturers for data collection and other purposes..

If critical subsystems are not unavailable in step 601, the method further confirms if any non-critical subsystem is unavailable 602. If any of the non-critical subsystem is indeed unavailable, the method performs specific stand-by on the specific subsystem 630.

Specific stand-by 630 involves performing stand-by only for a specific non-critical subsystem. For example, if entertainment system 190 malfunctions, entertainment system 190 can be safely turned off without affecting the operation of the vehicle. However, some non-critical functions may be affected such as an alarm function announcing certain information that is pre-disposed to be announced by entertainment system 190. In this case, specific stand-by 630 may include rerouting the information to display 144, perhaps with the information to be presented in abbreviated form to ensure the information will be presentable on display 144. Specific stand-by 630 for entertainment system 190 may also involve rerouting information to other perceptible methods such as by light or sound.

In step 640, the method activates an alarm to information driver and third-party services of specific subsystem stand-by similar to step 620.

Fig. 9 depicts a method of operation of the remote control module 2040. There are a number of examples of operation by a remote control module 2040.

In one example, a police officer or other law enforcement authority and/or rule trap sensor can “ping” an automobile for information relating to its speed and driving conditions. By comparing this received data from the automobile to known data relating to stop signs, speed limits, and the like, a decision can be made on whether the law has been broken. For example, the sensor itself may not necessarily determine the speed of a vehicle. The sensor asks the vehicle to respond to the sensor with the vehicle’s speed and possibly other information. Therefore, the speed detection is achieved through responding to a sensor’s question and the vehicle’s answer. It is anticipated that a specific sensor may use alternate detection methods to verify the accuracy of a received signal. For instance, if a vehicle is asked to respond with a current speed value, and does so, the sensor may send a radar signal to verify the response. If the response does not match the verification signal, a note is made of the anomaly and the data is recorded. This data may be used by law enforcement to later identify vehicles that are malfunctioning and/or have been compromised. The identity of the car, including serial number, owner identity (e.g., name, home address, and contact information), driver’s license number, insurance information (e.g., name and address of

insurance company, owner's insurance policy identification, and coverage limits), and the like), and/or licensing information (e.g., license plate number) can be provided by the vehicle to the requestor.

5 In another example, a law enforcement authority, owner, or other privileged entity may request a critical or non-critical task, function or operation to be disabled or behave in a selected manner. For instance, a law enforcement officer can cause the vehicle to decelerate in a high speed pursuit or, for a high speed pursuit or stolen car, can disable the engine.

10 In another example, a remote node 1500, such as a law enforcement authority, an insurance company, an intelligent sign or traffic signal, a roadside monitor, or the owner himself or herself requests historic or current vehicle operating information, such as speed, and/or information received by the vehicle from an external source, such as a stop light, speed limit sign, yield or stop sign, and the like. This information can be compared to identify poor driving practices and/or breaking of the law. It can also be used in accident reconstruction to determine who is at fault in an automobile accident where vehicle operators
15 frequently dishonestly represent who is at fault. Currently, responsible drivers pay inflated insurance premiums because the insurance industry cannot guaranty a particular driver's adherence to the law or general driving behavior. To address this concern, current insurance companies may allow a driver to install a device in a vehicle to randomly monitor behavior. This device can only monitor certain functions and requires the installation of a device
20 separate from the vehicle's ecosystem. The present disclosure is directed to using various data compiled by the system to analyze factors contributing to an individual's driving behavior and/or habits. In the event that an individual wishes to receive better insurance rates for responsible driving, a lower quantity of driving, or other good driving indicators, the driver may agree to provide insurance tracking information. The insurance tracking system
25 may consider GPS and other location-based information (to compare actual speed with speed limit data), g-force sensors (to detect rapid acceleration, hard turns, etc.), perimeter sensors (to detect close-calls, inattention while changing lanes, etc), in order to determine conformance with the good-driving terms established by an insurance company. Because the device may be integrated, and/or associated, with the vehicle's ecosystem total behavioral
30 data may be recorded and sent in real-time to a receiving module. Moreover, the system may detect the user and provide accurate information for each user of a vehicle.

Referring to Fig. 9, the remote control module 2040, in step 900, receives a request to command a vehicle task, function and/or operation and/or to transmit specified information to the requestor.

In step 904, the remote control module 2040 attempts to authenticate the requestor.

5 User authentication is a way of identifying a user and verifying that the user is allowed to access some restricted service. Authentication can be performed by, for example, by encrypted symmetric or asymmetric key exchange, public and private key cryptography, a secure remote password, multi-factor authentication (e.g., three major factors include verification by something a user knows (such as a password or PIN), something the user has
10 (such as a smart card, ATM card, or a security token), and something the user is (such as the use of biometrics, such as a fingerprint or retina scan)), time-based authentication, a unique digital identity, closed-loop authentication, access control service, and the like.

Control then passes to decision diamond 908 where the remote control module determines whether authentication was successful. When authentication is successful, the
15 remote control module, in decision diamond 912, determines whether the requestor is privileged to make the request. In other words, a first requestor is entitled to a first set of privileges with respect to access to vehicle information and/or control of vehicle tasks, functions, and operations while a second requestor is entitled to a different second set of privileges with respect to access to vehicle information and/or control of vehicle tasks,
20 functions, and operations. A law enforcement entity or vehicle owner, for example, will generally have a highest level of privilege (enabling broad access to vehicle information and/or control of vehicle tasks, functions, and operations) while an insurance company or servicing entity will not have the highest level of privilege.

When the requestor is entitled to make the request, the remote control module, in step
25 916, executes or causes execution of the request in accordance with rules governing what the privilege accorded the requestor, which may override operator and/or other occupant commands.

When the requestor is not entitled to make the request, the remote control module, in step 920, ignores the request and logs in memory 220 the information surrounding the
30 request, e.g., the identity of the requestor, the time stamp of the request, and the request itself.

The remote control module 2040 can perform other functions at the request of the vehicle owner and/or a vehicle family member. The remote control module 2040 can receive vehicle configuration commands from a remote node 1500 that cause the remote control module 2040 to implement the configuration commands. The configuration commands
5 respect the configuration of any vehicle component, including on board input/output system display appearance and/or content and/or icon configuration, programmable hard button function mapping, on board cached media selection, alteration of vehicle performance parameters, and vehicle status.

A number of examples will be described to illustrate these remote control module
10 functions. In a first example, a vehicle owner or family member, via a remote node 1500, such as a home computer, tablet or laptop computer, smart phone, and the like, can customize his or her input/output system display settings, appearance, sounds, wall paper, icon selection and location, and the like. Manufacturer or after market defined templates may be provided to assist the user in configuring the input/output system. The user, for instance, could move
15 graphical objects, such as icons, around to where he or she wants them to be. He or she could put in or remove graphics. He or she could add a digital tachometer or navigation application, such as one downloaded from an application store over the Internet. He or she could rearrange preferences. For instance, he or she may cause the default configuration on the infotainment or entertainment system to be the radio presets or the navigation. Because
20 the vehicle is web-based, the user can download third party displays from a commercial entity, such as an on line application store, or even trade with friends. He or she could configure programmable hard buttons, such as stereo or radio buttons, so that a selected button that currently causes the radio to scan can be made to trigger the on board navigation application. Users can apply software-based skins, such as wall paper, that are decorative
25 ways to add personal style to the vehicle. Users can add functionality to the vehicle. For example, he or she can download, over the Internet, media, such as digital movies from an on line rental service, such as Netflix, and digital games to the vehicle memory. He or she can customize vehicle performance, such as by tuning the vehicle through the remote connection. For instance, if the user moves the vehicle to a sport mode, shifting points would be altered
30 and, if the user moves the vehicle into economy mode, cylinders could be disabled at different speeds. He or she can connect to obtain and/or run diagnostics of a selected vehicle

component. He or she could use the diagnostics to obtain quotes for and/or schedule repair or maintenance operations by selected service personnel. He or she could check states of selected vehicle operations, including whether cabin lights are on or off, whether headlights are on or off, whether windows are up or down, whether the on board alarm is on or off, whether the on board alarm has been triggered, and whether the sun roof is open or closed. The remote node 1500 could then be used to reset the state as desired, e.g., turn cabin lights off, turn headlights off, close windows and/or sunroof, activate alarm, and the like. The user could also set up communication paths and/or modalities for vehicle-generated alarms. Exemplary communication paths and/or modalities, including phone call, instant messaging, emails, and the like.

A hard reset could be performed to reset all vehicle components to factory default settings.

This operation of the remote control module 2040 will be discussed with reference to Fig. 31.

Referring to Fig. 31, the remote control module 2040, in step 3100, receives a request, via a remote node 1500 and from an owner or family member of the owner, to configure a selected component of the vehicle, such as an on board input/output system, and/or to access vehicle state information.

In step 3104, the remote control module 2040 attempts to authenticate the requestor.

User authentication is a way of identifying a user and verifying that the user is allowed to access some restricted service. Authentication can be performed by, for example, by encrypted symmetric or asymmetric key exchange, public and private key cryptography, a secure remote password, multi-factor authentication (e.g., three major factors include verification by something a user knows (such as a password or PIN), something the user has (such as a smart card, ATM card, or a security token), and something the user is (such as the use of biometrics, such as a fingerprint or retina scan)), time-based authentication, a unique digital identity, closed-loop authentication, access control service, and the like.

Control then passes to decision diamond 3108 where the remote control module determines whether authentication was successful. When authentication is successful, the remote control module, in decision diamond 3112, determines whether the requestor is privileged to make the request. In other words, a first requestor is entitled to a first set of

privileges with respect to access to vehicle information and/or control of vehicle tasks, functions, and operations while a second requestor is entitled to a different second set of privileges with respect to access to vehicle information and/or control of vehicle tasks, functions, and operations.

5 When the requestor is entitled to make the request, the remote control module, in step 3116, executes or causes execution of the request in accordance with rules governing what the privilege accorded the requestor, which may override operator and/or other occupant commands.

10 When the requestor is not entitled to make the request, the remote control module, in step 1320, ignores the request and logs in memory 220 the information surrounding the request, *e.g.*, the identity of the requestor, the time stamp of the request, and the request itself.

15 This functionality can enable a vehicle to have multiple configurations for a selected vehicle component, such as an input/output system, that is indexed or associated with a specific occupant. Techniques can be used to determine where each occupant is seated in the vehicle, map the identified occupant to the set of data structures correlating each occupant with selected vehicle component configuration and configuring the respective input/output system accordingly. Thus, the vehicle can have plural differently configured input/output systems at any one time. When the selected component is a component other than an
20 input/output system, the particular configuration of the selected component to be employed is dependent on who the identified operator of the vehicle is.

25 In addition to the techniques described elsewhere for identifying a vehicle occupant, other techniques that may be employed include ignition keys that are identified uniquely to an occupant, user input such as selection of one or more keys, entry of an identification code or other identity, or biometric data, such as a fingerprint or retinal scan, and login. When the occupant is identified and associated with a particular seating position, the selected component will autoconfigure.

Operation of Computational Module Selector 2052

30 The operation of a processor off-load procedure 700 by computational module selector 2052 one or more processing module(s) will now be discussed with reference to Fig. 7. This operation is particularly beneficial in an active-active configuration but may be used

in an active-standby configuration. As discussed with respect to vehicle 300 of Fig. 3, some configurations of expansion modules 290A-C may require processor off-load to share processing functions of tasks among a number of expansion modules in a common host processing module 124 or across different processing modules 124. For example, a first expansion module 290A and/or host processing module 124 may be specialized for critical functions while a different second expansion module 290B and/or host processing module 124 is specialized for non-critical functions. In an event where the first expansion module 290A and/or its host processing module 124 loses some processing power, the first expansion module 290A and/or its host processing module 124 may be able to off-load some critical function to second expansion module 290B and/or its host processing module 124.

In step 701, the method continuously checks if a next processing module, expansion module, and/or external computational device(s) 1532 (in wireless communication with the network controller 1528 via the gateway/firewall 1512) is available with excess processing power. If a next processing module, expansion module, and/or external computational device(s) 1532 is not available, the method will check at some time interval later to see if a new processing module, expansion module, and/or external computational device(s) 1532 would have a change in a number of available and/or unavailable processing power units and/or bandwidth. Other stimuli for this step 701 include a user request to initiate execution of an application, notification of a processing resource having unused bandwidth below a selected threshold, notification of a processing resource having used bandwidth above a selected threshold, a power level of a processing resource falling below a selected threshold, notification of a processing resource having an operational error, malfunction, or outage, and the like.

If a next processing module, expansion module, and/or external computational device(s) 1532 is available, the method confirms with the next processing module, expansion module, and/or external computational device(s) 1532 on its available processing power units and/or bandwidth for a task 710. Other factors considered in determining whether a selected processing module, expansion module, and/or external computational device is available include not only the processing resources available but also the application and operating system requirements as compared to the capabilities of the selected processing module,

expansion module, and/or external computational device and power level in the selected processing module, expansion module, and/or external computational device.

In one configuration, processing module, expansion module, and/or external computational device(s) 1532 may be distinguished depending on the type of processing
5 needed. For example, a critical function might not be suitable for a processing module that deals only with non-critical functions and vice versa due to safety, security, or other concerns. In other configurations, a critical function might look for a processing module that is tasked with a disproportionately high non-critical function load to balance the processing load.

10 If the selected processing module, expansion module, and/or external computational device(s) 1532 is available to process a given task, function or operation 710, the task is off-loaded to the selected processing module, expansion module, and/or external computational device(s) 1532.

If the selected processing module, expansion module, and/or external computational
15 device(s) 1532 is not available to process a given task, function or operation 710, the procedure continues to check if any other processing module, expansion module, and/or external computational device(s) 1532 is available 702. If there is a different processing module, expansion module, and/or external computational device(s) 1532 available, the method returns to step 701.

20 If there is no other processing module, expansion module, and/or external computational device(s) 1532 available, the method informs the active processing module, expansion module, and/or external computational device(s) 1532 of no available offload capacity 730. In one configuration, the active processing module may decide to drop the task that it is unable to handle. The active processing module, expansion module, and/or external
25 computational device(s) 1532 may also decide to return to step 701 to continue to check for a next available processing module, expansion module, and/or external computational device(s) 1532.

A further set of operations for the computational module selector 2052 will now be discussed with reference to Fig. 23. This set of operations identifies, for a selected
30 computational module, such as an expansion module, software application, or other computational module, which processing modules or external computational device(s) 1532

contain the selected computational module for purposes of computational module selection. While the prior flow chart depicts a method to balance processing load amongst plural processing devices, the present flow chart selects which duplicative computational module should perform a request by a user.

5 In step 2300, the computational module selector 2052 detects a stimulus. Exemplary stimuli include a user or operator request to initiate a computational module and/or perform a selected task, function, or operation, an interrupt based on a passage of a predetermined time, installation of a computational module, a request by a different user to use a platform currently executing the computational module, notification of a processing resource having
10 unused bandwidth below a selected threshold, notification of a processing resource having used bandwidth above a selected threshold, a power level of a processing resource falling below a selected threshold, notification of a processing resource having an operational error, malfunction, or outage, and the like.

In step 2304, the computational module selector 2052, in step 2308, determines
15 duplicated computational modules and the host processing platform(s) therefore. Host processing platforms can include a processing module, expansion module, and/or external computational device(s) 1532. Duplication may be for a specific computational device (e.g., from a common vendor and commonly named) or for a common type of computational device. For example, duplication may be determined for the differing versions of automotive
20 navigation system applications GPS Drive™ by MotionX™, Garmin GPS™, Magellan GPS™, Tomtom GPS™, and other SPS systems or for all navigation applications generally regardless of vendor, application identity, or version.

In step 2312, the computational module selector 2052 selects a computational module and platform to execute each duplicated computational module. For example, if an occupant
25 requests, by an input/output system of the vehicle, a game or multimedia application and if different versions of the game or multimedia application are on a processing module 124 and external computational device(s) 1532, the computational module selector 2052 can select the most recent version of the game or multimedia application and host platform containing same, regardless of whether the host platform is a processing module or external
30 computational device 1532 currently in communication with a processing module and by what device, whether an input/output system or user interface of the external computational

device 1532 receiving the request. If the request were to be received by an input/output system 1600 to initiate a game and the most recent version of the game were located on a processing module, the processing module would be selected to execute the game and output would be provided to an occupant by the corresponding input/output system 1600. If the request were to be received by an input/output system 1600 to initiate a game and the most recent version of the game were located on an external computational device 1532, the external computational device 1532 would be selected to execute the game and output would be provided to processing module for presentation to an occupant by the occupant's input/output system 1600. If the request were to be received by an external computational device 1532 to initiate a game and the most recent version of the game were located on a processing module, the processing module would be selected to execute the game and output would be provided to an occupant by the external computational device 1532. If the request were to be received by external computational device 1532 to initiate a game and the most recent version of the game were located on the external computational device 1532, the external computational device 1532 would be selected to execute the game and output would be provided to processing module for presentation to an occupant by the external computational device 1532.

In decision diamond 2316, the processing module, or external computational device 1532, by the user interface receiving the stimulus, whether an input/output system or the user interface of the external computational device 1532, queries the user whether or not the older versions of the computational module should be updated to the newer locally available or newest remotely available version.

If no or a negative response is received, the computational module selector 2352 proceeds to decision diamond 2324.

If a positive response is received, the computational module selector 2052, in step 2320, requests the host platform to upgrade the computational module.

In decision diamond 2324, the computational module selector 2052 determines whether the selected platform is currently available to execute the computational module. The selected platform may currently be executing other computational modules and have insufficient available processing resources for execution. The computational module selector 2052, in that event, would attempt to off load some of the processing to another platform to

free up sufficient processing resources for execution. In other words, the computational module selector 2052 would perform processing load balancing to more optimally use processing resources. A user may currently be using the selected platform, such as engaged in a call if the selected platform is a cellular phone or watching multimedia content. The computational module selector 2052 would determine if the platform can request the user for permission to use the platform for processing the computational module. When the user is on a call, such a request cannot be made. If a request can be made, the user is requested. The platform is only deemed to be available when the user provides input indicating availability.

When the platform is not available, the computational module selector 2052 in step 2328 selects a next available platform even though the platform may contain an older version of the computational module.

When the selected module is currently available or when the computational module selector 2052 selects a different platform in step 2328, the computational module selector in step 2328, initiates execution, by the selected platform, of the computational module.

Operation of Network Controller 1528

Fig. 24 depicts another operation of the network controller 1528. As noted, 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 event data recording. Due to the potentially dire consequences of a security breach event 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 gateway, 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, end-to-end encryption (in one or more of 2, 3, and/or application layer), and RF shielding substantially surrounding the interior 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.

5 In step 2400, the network controller 1528 detects a stimulus, such as 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
10 resource. The stimulus may be a warning signal received by the network controller 1528 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 potential
15 security breach event. 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. The security breach event details,
20 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 event can be
25 isolated from other vehicular network components or whether the active processing module 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
30 network, that contains and exposes the network's external-facing services to a larger 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, 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 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 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 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 (in one or more of 2, 3, and/or application layer(s))).

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 event 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 event and details regarding it. The critical security mechanism may be activated to protect the critical components and active processing module.

5 Operation of Network Selector 2036

The operation of the network selector 2036, a subcomponent of the network controller 1528, will now be discussed with reference to Figs. 8 and 10-11.

Referring to Fig. 8, an active processing module 124, in step 800, receives a signal to transmit to a separate vehicle component. The signal can be, for example, from any on board computational component, including an on board sensor 1516 (including those discussed
10 above), a critical or non-critical system controller 2012 or 2016, an on board sensor monitor 2020, the displayed object movement module 2024, the diagnostic module 2028, the media filter 2032, the remote control module 2040, the installation supervisor 2044, the multimedia control module 2048, the computational module selector 2052, the media controller 1524, the
15 gateway/firewall 1512, another processing module 124, the transceiver 1508, an input/output system 1520, a network controller 1528, and/or an external computational device 1532.

The network selector 2036, in step 804, selects a network compatible with the type and/or required format of the signal, such as one or more of local wired network 808, local wireless network 812, and/or the internet 816, to deliver the signal to a selected local or
20 remote endpoint, including those set forth in the prior paragraph. The selection is based on one or more factors, including a type, urgency, importance and/or requirements of the signal (e.g., whether the signal contains an urgent flag or other urgency indicator, a source of the signal (such as from an on-board sensor or sensor monitor, a critical component, a non-critical component, and the like), a type of signal payload (such as whether the signal
25 contains multimedia), transmission and/or bandwidth requirements for the signal (e.g., requisite maximum latency, packet loss, jitter, and/or transmission rate, transport protocol, quality of service, and the like)), an operational status (e.g., operational or nonoperational) of each of the compatible networks, an operational status of an intermediate node on the compatible networks, a signal/noise ratio over each of the compatible networks, available
30 and/or unavailable bandwidth for each of the compatible networks, current compatible network performance parameters (e.g., packet drop, latency, jitter, throughput, quality of

service, availability, bandwidth utilization, error rate, delay, and the like), and other factors influencing signal quality, reliability, and/or transmission speed.

Network and node performance parameters and characteristics can be collected by any number of techniques. One technique uses the Simple Network Management Protocol (SNMP), which is a protocol for sending and transmitting network performance information. Network performance monitoring tools vary from simple one device applications to a complex hierarchical system. These systems employ a variety of monitoring techniques. Some systems use passive monitoring to gather information about network traffic while others actively poll network devices to gather network performance data. Exemplary network performance monitoring tools include packet sniffers, flow monitors, and application monitors. Flow monitoring aggregates network traffic based on individual connections, users, protocols, or applications. The network selector can obtain information regarding network and node performance by accessing a node's management information base (MIB). A MIB is a database used to store management information in networks. MIBs are used by network management systems to identify network data objects that are stored, retrieved and set by the system. A MIB uses a hierarchical tree structure to store an extensible collection of data. A subset of Abstract Syntax Notation One (ASN.1) is used to specify an object. The network selector can be configured as a network management system, which includes a centralized network management station and management agents running on network devices. Using a management protocol, the management station polls agents distributed throughout the network, such as in network nodes, for information about the network devices. Agents return requested information ranging from bandwidth usage to CPU load. Using this information, the network management system provides performance and error reporting information.

Generally, the network selector determines the type, urgency, importance and/or requirements of the signal and one or more of the above parameters for each of the compatible networks, compares the signal parameters with the compatible network parameters and selects the compatible network able to currently best satisfy the requisite signal parameters. For example, a signal from a critical component generally is transmitted by a local wired network 808, such as a bus, due to the high signal quality, reliability and/or transmission speed required for the signal. A multimedia signal would generally not be

transmitted by a local wired network as it is not commonly incompatible with the signal payload. Such a signal would more typically be transmitted by a local wireless network 812 (e.g., by Bluetooth™ or WiFi™ or a “hot spot”) or, if the signal recipient (whether or not an on board component or remote node) has a corresponding IP address, by the internet 816.

5 In one configuration, the network selector 2036 determines, for each of the plural communication networks, a corresponding one or more of a network status, a node status, a signal/noise ratio, an available and/or unavailable bandwidth, a current performance parameter(s), and a quality of service and selects the selected network based on one or more relative values associated with the corresponding value(s). The network selector can, for
10 example, determine a composite value for each of the plural networks. The composite value is based on one or more of the corresponding one or more of a network status, a node status, a signal/noise ratio, an available and/or unavailable bandwidth, a current performance parameter(s), and a quality of service. The composite value computational algorithm can weight (or hierarchically rank) some of the individual values of network status, node status,
15 signal/noise ratio, available and/or unavailable bandwidth, current performance parameter(s), and quality of service more or higher than others. The composite is used, rather than multiple values, in selecting the selected network.

 By way of example, a signal relating to a critical task, function, and/or operation is deemed to have a higher level of importance than a signal relating to a non-critical task,
20 function, and/or operation. The former signal may be transmitted by a low error-rate and low latency network, such as a bus-type network, while the latter signal may be transmitted over a wireless network or even the Internet.

 Once the compatible network is selected for signal transmission, the network selector 2036, in step 820, configures or causes to be configured the signal in accordance with the
25 selected network’s transmission protocol. For example, when the signal is to be transmitted over a local wireless network 812, the signal payload and/or signal itself would generally be packaged (such as by a protocol stack) in a header and trailer in accordance with an appropriate one of the WiFi™ or Bluetooth™ protocols. By way of further example, when the signal is to be transmitted over the Internet 816, the signal payload and/or signal itself
30 would generally be packaged (such as by a protocol stack) in a header and trailer in accordance with TCP/IP suite of protocols.

The properly configured or formatted signal is then transmitted over the selected compatible network.

A further operation of the network selector 2036 will now be discussed with reference to Fig. 10. In this operation, the network selector 2036 receives a media stream from a remote node 1500, such as a radio or television station or other Web site, and selects an intermediate local network to carry the media stream to an input/output system for presentation to an occupant of the vehicle.

In step 1000, a processing module 124 receives the media stream from the remote node 1500. The media stream packets contain destination information associating the media stream with one or more input/output systems of the vehicle.

In step 1004, the network selector 2036 determines the transmission mode and/or network based on various parameters, including network status, intermediate node status, signal/noise ratio of the network, type and/or source of media, available and/or unavailable bandwidth, network performance parameters (e.g., availability, packet drop, latency, jitter, throughput, etc.), quality of service, and the like. The network selector 2036 selects which of the local on board wireless network 812 (e.g., generated by a on board or portable component within the vehicle), local wired network 808, and nearby independent wireless network 1008 (e.g., generated by a component external to the vehicle) is to carry the media to the destination input/output system(s) of the vehicle.

In step 1012, the media is provided, over the selected network, to the destination input/output system(s).

Operation of Media Controller 1524

A further operation of the network selector 2036 and operations of the media controller 1524 will now be discussed with reference to Fig. 11. In this operation, the network selector 2036 receives a signal, which typically includes a media payload, from a local or remote node and selects an intermediate local compatible network to carry the media stream to an input/output system for presentation to an occupant of the vehicle. Depending on an input/output system mode, the signal is directed by the media controller 1524 only to a subset or to all of the input/output systems. In a dependent mode, common content is provided synchronously to each of the input/output systems while in an independent mode different content is provided to different ones of the input/output systems. While each

occupant controls his or her input/output system in independent mode, the operator controls all input/output systems in the dependent mode. This is particularly beneficial for young children as occupants. The operator typically selects which of the modes is in effect in the vehicle at any one time.

5 In step 1100, the processing module 124 receives a signal for graphical presentation to one or more occupants. The signal typically comprises media as a payload.

In step 1104, the network selector 2036 determines the transmission mode and/or compatible network based on various parameters, including network status, intermediate node status, signal/noise ratio of the network, type and/or source of media, available and/or
10 unavailable bandwidth, network performance parameters (e.g., availability, packet drop, latency, jitter, throughput, etc.), quality of service, and the like. The network selector 2036 selects which of the local on board wireless network 812 (e.g., generated by a on board or portable component within the vehicle), local wired network 808, and Internet 818 is to carry the media to the destination input/output system(s) of the vehicle.

15 In step 1108, the media controller 1524 determines which of the input/output systems are to receive the media. There are a number of factors that can influence this decision. The first is whether the input/output systems are in dependent or independent mode. The second is whether an applicable law, whether federal, state, provincial, or local, limits the operation of one or more of the input/output systems. The satellite positioning system receiver on
20 board the vehicle can provide, at any time, the precise vehicle position to a processing module. The processing module can use the position coordinates to determine a set of applicable laws and, from the set of applicable laws, determine one or more restrictions on input/output systems of vehicles within that jurisdiction. Restrictions may also be configured by the operator of the vehicle. These legal and operator restrictions are collectively referred
25 to as rule set(s) 1612. For example, exemplary restrictions, or rule sets 1612, include not providing videos to the operator when the vehicle is in gear or moving, banning texting in the vehicle when the vehicle is in gear or moving, and banning cellular calls when the vehicle is in gear or moving. Restrictions may, alternatively, require the media to be presented to the operator and/or occupant in a specific manner. For example, the audio channel of a video
30 may be permitted to be played in the absence of the video channel of the video. A cellular call may be permitted using a hands-free mode but not using a handheld phone.

In step 1112, the media controller 1524 configures and transmits the signal in accordance with the selected network and the restrictions, if any, determined in step 1108. Configuration refers not only to formatting and including the addresses of the input/output systems to receive the signal but also to changing the media payload, such as, for instance,
5 removing video content while leaving audio content.

Upon receipt, the signal is processed by the display and/or audio controllers 1604 and 1608 and presented, by the recipient input/output system and over the corresponding input/output system to the occupant.

Fig. 17 depicts another operation of the media controller 1524.

10 In step 1700, the media controller 1524 detects a stimulus, such as an occupant request to change the operational mode of an input/output system.

In step 1704, the media controller 1524 determines a current operational mode of the input/output system associated with each of the occupants (e.g., independent or dependent operation) and whether the occupant has authority or is privileged to request the change. The
15 mode is changed only when the occupant is authorized or privileged to make the change.

In step 1708, the media controller 1524 determines when the requestor is authorized or privileged to request the operational mode change, the input/output system preferences of each of the occupant user(s) including the requestor.

In step 1712, the media controller 1524 determines when the requestor is authorized
20 or privileged to request the operational mode change, the pertinent rule set(s) 1612. As noted, the rule set(s) 1612 include rules set by the owner or operator of the vehicle, manufacturer of the vehicle, and as a matter of applicable law.

In step 1716, the media controller 1524 determines, when the requestor is authorized or privileged to request the operational mode change, a current state of each of the
25 input/output system(s). The current state includes not only the on/off status and settings but also the content being displayed and operations currently being performed by the occupant for each of the input/output systems.

In step 1720, the media controller 1524 determines when the requestor is authorized or privileged to request the operational mode change, a current display configuration of each
30 of the input/output systems.

In step 1724 and when the requestor is authorized or privileged to request the operational mode change, the media controller 1524 configures or reconfigures each of the input/output systems and the corresponding displays as required by the new operational mode. For example, when the current operational mode is independent and the new operational mode is dependent, the media controller 1524 blocks content currently being provided to each of the subservient input/output displays in favor of providing to each of the subservient input/output displays the content provided to the master input/output display controlled by the requestor or to display content selected by the requestor. When the current operational mode is dependent and the new operational mode is independent, the media controller 1524 continues to provide the content formerly provided to all of the input/output systems to the requestor's input/output system but returns each of the other input/output systems to a default display. From the default display, the respective user can select customized content, which may be the same as or different from the content being provided to the requestor's input/output system.

Fig. 18 depicts another operation of the media controller 1524.

In step 1800, the media controller 1524 receives a signal from a local or remote node 1500. The signal includes, for example, media from a web site or server or communication from a third party.

In optional step 1804, the media controller 1524 unpacketizes the signal and analyzes the payload. This is done, for example, when the destination for the signal and/or type of payload is not clear from the packet header and/or trailer.

In step 1808, the media controller 1524 selects an input/output system to receive the packet payload. This can be based, for example, on the destination information in the header and/or results of the analysis of optional step 1804.

In step 1812, the media controller 1524 determines the applicable rule set 1612 (or set of restrictions), if any, governing the destination input/output system and/or payload type or content.

In step 1816, the media controller 1524 determines a current input/output system configuration(s). The current configuration includes not only settings and capabilities but also whether the input/output system is in the dependent or independent operational mode.

Based on the above information, the media controller 1524 determines whether the payload can be provided to each of the destination input/output systems and, if so, generates a command incorporating the payload and including commands to the input/output system on how to render and display the content. As noted, the payload cannot be provided to a
5 subservient input/output system when in the dependent operational mode and the content differs from that provided to the master input/output system. It cannot be provided when an applicable rule set 1612 prohibits such presentation. It may need to be filtered to remove some of the payload to comply with the applicable rule set 1612.

10 In step 1824, the command is forwarded to each of the destination input/output systems.

Fig. 19 depicts another operation of the media controller 1524.

In step 1900, the media controller 1524 determines a location of each external computational device 1532 by a suitable technique. In one example, a signal receiver or transceiver or other connectivity access point, such as a wireless access point, WiFi™
15 antenna, and the like is placed at each input/output system and/or near each occupant seating location and/or at the operator's seat. The network interface on the network controller can force external computational devices to connect via a specified communication protocol, such as by Bluetooth™ or WiFi™.

In step 1904, the media controller 1524 determines a spatial location of each of the
20 external computational devices relative to one or more selected connectivity access points. Continuing the example of the prior paragraph, the media controller 1524 measures, at each connectivity access point, a signal strength for each detected external computational device and, using the measured signal strengths and a suitable algorithm such as triangulation, determines a spatial location of each external computational device and, in step 1908 for each
25 located external computational device, a nearest input/output system and/or occupant seat.

In step 1912, the media controller 1524 determines a pertinent rule set 1612 for the determined location of each external computational device.

In decision diamond 1916, the media controller 1524, based on the pertinent rule set 1612, determines whether or not to accept connectivity access by each of the external
30 computational devices or what limitations to place on such access. In the latter case, specific tasks, functions, and/or operations may be permitted by the pertinent rule set but not others.

For example, a cellular phone may be forced into hands free calling mode or prevented from texting or using an instant messaging application or protocol when located at the operator's seat. The rule set 1612 may be configured as a table listing, by vehicle location, an applicable set of legal restrictions and/or permissions and the restrictions or permissions on specific tasks, functions, and/or operations.

When unlimited or limited access is permitted by the rule set 1612, such access is provided by the media controller.

In decision diamond 1920, the media controller 1524 monitors each of the external computational devices for a change in spatial location. In other words, the media controller detects movement of any external computational device from a first connectivity access point or input/output system or seat governed by a first rule set to a second different connectivity access point or input/output system or seat governed by a different rule set. This is so because each connectivity access point or input/output system or seat has a corresponding rule set. When no change detected, decision diamond 1920 is repeated by the media controller substantially continuously or periodically.

When limited or unlimited access is not accepted (decision diamond 1916) or a location change is detected (decision diamond 1920), the media controller returns to step 1904.

Fig. 25 depicts a further operation of the media controller 1524. Currently, a particular vehicle radio may have access to XM, AM, FM, and in some cases "streaming audio" capabilities through separate sources (remote node(s) 1500). However, it is necessary to change the input on a console to receive the information and music from a specific source.

It is an aspect of the present disclosure to provide a console capable of compiling and playing music and multimedia information (such as a streaming video) by a general and/or specific category. It is anticipated that the console may adaptively select the source providing the content according to specific rules, such as music type. For example, the console may select the strongest signal, or highest quality of channel. Furthermore the data is collected regardless of the source and represented by icons (independent of source) on the console. These icons may be selected by the user to access content. In one configuration, the icon corresponds to a type of music. The music is band and/or communication mode

independent. For example, a “classical music” icon indexes and/or links to all classical music channels, whether AM, FM, streaming, XM, etc.

In some cases, a user may be listening to one station/source while media information is being received and cached from another station/source. In the event that the first signal is lost, the cached media signal or stream may play. Additionally, the system may adaptively “signal surf,” for a given category, to determine the best channel to receive the highest or best quality signal (e.g., S/N ratio, stream or radio wave). Moreover, the system may be able to determine that a reception limit is being neared (by pilot signal back or satellite positioning system receiver location) and may push delayed broadcast media information or other content to a vehicle computer to be cached and listened to after coverage is lost.

In step 2500, the media controller 1524 detects a stimulus indicating that caching of media content is to be performed. This may be a request by a user, a media signal falling below a specified signal-noise ratio, the vehicle nearing an estimated broadcast limit or range of the media source (or remote node 1500), a request by a remote node 1500 (or signal source) to forward content to the vehicle for caching for later presentation to the user, a user action requiring the media not to be presented by the vehicle (e.g., the vehicle operation moves from being “parked” to being in gear (or in “drive” or “reverse”), and the like. As will be appreciated, many jurisdictions’ laws prohibit displaying media to a driver while a vehicle is in operation.

In decision diamond 2504, the media controller 1524 determines whether or not to cache media. Depending on the stimulus, rules configured by the user or default rules, may cause the stimulus to be ignored. For example, when the request is from a remote node 1500 the media controller 1524 may have a rule denying such SPAM-like requests, may determine that insufficient memory resources are available to cache the content, may determine that the media content or remote node 1500 constitutes a potential security breach event, or may have the remote node 1500 address, identity, or other identifier on a blacklist. When the media is a video, the video may be cached for one input/output system, namely that of the driver, but not for another input/output system, namely that of a passenger.

In step 2508, when caching is to be performed the media controller 1524 commences caching the streaming media for delayed presentation to the user. As will be appreciated, the media controller 1524 can continue normal buffering of streaming media packets.

In step 2512, when caching is not to be performed, the media controller 1524 can continue normal buffering of streaming media packets but does not perform media caching.

Fig. 26 depicts a further operation of the media controller 1524. The operation involves conforming media presentation, by input/output system, in a manner comply with a
5 pertinent rule set 1612. For example, instant messages, RSS feeds, Twitter messages, can, in response to a vehicle moving from a parked (non-operational) to an operational (in motion) state, cease displaying this content to the driver and, instead, audibly present the content and message source identifier to the driver, such as reading the source name or address and RSS feeds or Twitter or instant messages or enabling the audio channel for streaming multimedia
10 while disabling the video channel.

In step 2600, the media controller 1524 detects a stimulus indicating that media presentation is to be altered for one or more input/output systems. This may be a request by a user or a change in vehicle state from operational to non-operational or from non-operational to operational (e.g., a user action requiring the media not to be presented by the
15 vehicle (e.g., the vehicle operation moves from being “parked” or a non-operational state to being in gear (or in “drive” or “reverse” or in motion), or an operational state). As will be appreciated, many jurisdictions’ laws prohibit displaying media to a driver while a vehicle is in operation.

In decision diamond 2604, the media controller 1524 determines whether or not to
20 alter the media presentation for a selected input/output system. When, for example, the vehicle moves from an operational to a non-operational state, the media presentation for the selected input/output system can revert automatically to a more functional format. For instance, multimedia can have all channels, both audio and video, enabled for presentation, by the selected input/output system to the user. An RSS feed or Twitter or instant message,
25 among others, can revert to text presentation, with automated reading being disabled.

In step 2608, the media presentation is altered, as determined, for one or more selected input/output systems.

In step 2612, media continues to be presented, in an unchanged format, on the selected input/output system.

30 Operation of Installation Supervisor 2044

An operation of the installation supervisor 2044 will now be discussed with reference to Fig. 12. The operation can provide a plug-and-play functionality for automotive components, whether device, hardware and/or software.

5 In step 1200, the installation supervisor 2044 detects an attempt to install a new computational component in the vehicle. The attempt can be detected by receipt of an installation notification or request from a user or the computational component itself. The computational component can be software, hardware, or a combination thereof. Exemplary computational components include an on board sensor 1516, a media controller 1524, a gateway/firewall 1512, a processing module 124, a network controller 1528, an input/output
10 system 1520, a display and/or audio controller 1604 and/or 1608, an arbitration module 2000, a health check module 2008, a critical system controller 2012, a non-critical system controller 2016, an on board sensor monitor 2020, a displayed object movement module 2024, a diagnostic module 2028, a media filter 2032, a network selector 2036, a remote control module 2040, a computational module selector 2052, an expansion module 290, an
15 application, a plug-in module, and the like.

In step 1204, the installation supervisor 2044 determines the characteristics of the computational component. Exemplary characteristics include manufacturer, model number, serial number, date of manufacturer, and capabilities.

20 In decision diamond 1208, the installation supervisor 2044 determines whether the component is already linked to another vehicle. This can be done by accessing the memory of the installation component itself to check for a prior installation or accessing the records of the manufacturer via remote node 1500.

When the component has not yet been linked to another vehicle, the installation supervisor 2044, in decision diamond 1212, determines whether the installation is in
25 compliance with licensing restrictions on the use of the computational component. Licensing conditions and/or restrictions can include payment of funds to vendor, use restrictions (e.g., user-based license restrictions (e.g., authorized user, concurrent user, floating user, and user value unit restrictions), capacity-based license restrictions (e.g., install, processor value unit, server and virtual server restrictions), territorial restrictions (e.g.,
30 use permitted only in certain countries, states, provinces, and the like), and other license

restrictions (e.g., client device (or host vehicle-based restrictions) and resource value unit restrictions)), and other conditions and/or restrictions.

When the component installation is in compliance with applicable license restrictions, the installation supervisor 2044, in decision diamond 1216, determines whether the
5 computational component is eligible for use in the current vehicle. Eligibility is based not only on specifications and capabilities of the computational component but also vehicle manufacturer approval or disapproval of the computational component for vehicles having this particular make, model and year of manufacture.

When the computational component is eligible for use in the current vehicle, the
10 installation supervisor 2044, in step 1220, creates data structures in the memories of the computational component and computational module binding the computational component to the vehicle. This can be done, for example, by creating data structures in the memory of the computational component containing a serial number or vehicle identification number of the vehicle and in the memory 220 of the processing module containing a serial number or
15 other unique identifier for the computational component and a description of the type, make, model, year of manufacture, and date of installation of the computational component.

When any of the following is true, namely the computational component is already linked to another vehicle (decision diamond 1208), the license does not permit the installation of the computational component (decision diamond 1212), and/or the component
20 is ineligible for use with the current vehicle (decision diamond 1216), the installation supervisor 2044, in step 1224, ignores the computational component, and therefore refuses installation of same, logs the attempted installation (including a description of the computational component and time stamp associated with the attempted installation) and/or notifies a remote node 1500 (such as a manufacturer for purposes of warranty invalidation)
25 and/or the operator of the invalid attempt.

Operation of Media Filter 2032

An operation of the media filter 2032 will be discussed with reference to Fig. 13.

In step 1300, a processing module 124 receives a signal from a third party source, such as a web site or server (in response to web browsing) or a communication from a third
30 party, such as email, text, cellular call, and the like, for presentation to an occupant.

In step 1304, the media filter 2032 determines preferences of the occupant and/or other restrictions. Preferences include, for example, a white or black list (of approved or disapproved message sources respectively), presence of the destination occupant as received from a presence server or service associated with the destination occupant, preferences of or
5 rules relating to the destination occupant as determined by another occupant having privileges to control content presented to the destination occupant (e.g., parental control of content and/or communications presented to a child), context of the destination occupant (e.g., driving the vehicle, engaging in an unrelated higher priority activity on the input/output system associated therewith, etc.), and governing laws (or an applicable rule set 1612).

10 In decision diamond 1308, the media filter 2032 determines, based on the determined preferences and/or restrictions from step 1304, whether or not to block the signal or alter the payload of the signal to conform with the preferences and/or restrictions.

When the signal is not to be blocked, the media filter 2032 proceeds to step 1312 and presents the signal or its payload to the destination occupant. The signal may be blocked, for
15 example, when it is a call to an operator while the vehicle is in motion (to comply with a state or local law). Electronic SPAM may be blocked.

When the signal is to be blocked, the media filter 2032 proceeds to step 1316 and blocks the signal. The signal may be blocked, for example, when it is a call to an operator while the vehicle is in motion (to comply with a state or local law). Electronic SPAM may
20 be blocked.

Operation of Diagnostic Module 2028

The diagnostic module 2028 queries on board sensors 1516 and/or on board sensor monitor(s) 2020, and/or critical and/or non-critical system controller(s) 2012 and 2016 to determine states of various parts, components, subsystems, tasks, functions, and/or
25 operations of the vehicle. The diagnostic module 2028 can then perform diagnostics using locally stored or remotely stored (at remote node 1500) pre-determined logic to identify faults, malfunctions, or other problems and, optionally, generate repair advice and/or warnings and/or instructions and/or recommendations to the vehicle operator. This diagnosis can also locate and/or determine and/or identify any parts or components required to repair
30 the vehicle, the source and/or source(s) for replacement parts and/or components, identify a nearest and/or preferred service or repair facility or service, provide an estimate of the repair

cost at a selected facility and/or comparative estimates at different facilities in proximity to the vehicle's current location, and/or obtain any manufacturer's and/or vendor's update information required to repair or resolve the identified fault, malfunction, or other problem. The diagnostic module 2028 can provide any repair instructions and/or recommendations to the operator, pre-order the replacement parts and/or components, contact the nearest and/or preferred service facility for a repair estimate, contact the nearest and/or preferred service facility to schedule an appointment for the repair or service, and/or forward, optionally at the owner's and/or operator's instructions, the collected information regarding the fault, malfunction, or other problem to a remote node 1500 (specified by the operator and/or owner) for monitoring and/or evaluation. The owner and/or operator can have a default location or select a location for fault, malfunction, or other problem analysis assistance.

Fig. 14 depicts an operation of the diagnostic module 2028.

In step 1400, the diagnostic module 2028 receives, from a local or remote source (such as the remote node 1500), a signal warning of an actual or potential malfunction of an on board component, including any of the components discussed above.

In step 1404, the diagnostic module 2028, in step 1404, determines user and/or default preferences regarding treatment of the signal. The various options include one or more of present the signal to a third party such as a manufacturer or servicing entity (option 1408), presenting the signal to an occupant of the vehicle (option 1412), contacting an emergency service provider or first responder (e.g., request tow truck or roadside service provider, contact police, and/or request dispatch of an ambulance), a service facility located in proximity to a current vehicle location, a manufacturer, a replacement part source, and a remotely located diagnostic service to diagnose a cause of the warning and/or error signal and performing on board diagnostics (option 1416) to obtain more diagnostic information regarding the actual or potential malfunction followed by option 1408 or 1412. In one application, the signal is forwarded to a manufacturer or repair service vendor that compares the reported fault and vehicle-specific parameters (e.g., mileage, date of last service, and/or environmental conditions) to the maintenance and/or fault history for the vehicle model and provides, to the vehicle operator, the result of the comparison along with a probability of the diagnosis being correct. The signal can include, for example, a current (SPS or map) location of the vehicle, an identity of the vehicle and/or vehicle owner or occupant, and diagnostic

information and/or diagnosed cause of the warning signal. The manufacturer or service vendor also updates its database for the particular model of the vehicle to reflect the reported fault. The manufacturer or service vendor can dispatch an emergency service provider or first responder to the location reported by the vehicle SPS, and/or schedules the workload for the repair shop and pre-orders the required part(s) for the repair shop. The diagnostic module
5 can recommend a source of conduct or action (including those discussed above) for the vehicle operator and, if accepted, execute or cause execution of same.

In step 1420, the diagnostic module 2028 determines a further treatment of the warning or error signal. The determination may be based, for instance, on a command or
10 request received from the third party or occupant or an applicable set of rules and/or policies.

Fig. 28 depicts another operation of the diagnostic module 2028.

Fig. 28 depicts a vehicle ecosystem capable of providing accurate indications for purposes of service and maintenance in accordance with embodiments of the present disclosure. Currently, vehicles may offer a warning light and/or series of lights to provide
15 information to a user regarding vehicle condition. These lights may have a multitude of meanings that may require further inspection by a mechanic or other qualified individual. In order to interpret and decode the meanings behind a light combination, the user is routinely required to consult the owner's manual, the Internet, or to call the dealer. In some cases, these lights are only maintenance reminders and need not be immediately addressed.
20 However, in other cases, the lights are urgent and require immediate attention.

The present disclosure can provide an Internet enabled car that is capable of transmitting vehicle codes, error code readings, and to remotely diagnose and display these codes to a user and/or a mechanic. This diagnostic information may be performed on-board or remotely. It is anticipated that the information may be accessed according to chosen
25 preferences. Additionally, it is anticipated that based on the type of warning/error code, the system may suggest a recommended course of action. For example, if the error code indicates a severe or catastrophic failure the system may suggest to pull-over, stop the car, and proceed to a safe area away from the automobile.

In some embodiments, the system may provide "conversational" warnings to a user.
30 These warnings and associated codes may also be simultaneously transmitted to a selected garage and/or postponed for approval to transmit to the nearest garage (either wired or

wirelessly). In addition, the system may estimate an approximate time to fix (based on past garage fix times, garage inventory, severity of problem, combinations, etc.) and make appropriate suggestions. For example, the system may provide the conversational warning “Please do not be alarmed, your engine is running slightly low on oil; there are four garages
5 in the general area. You have time to get a cup of coffee while you wait; here are three coffee shops in the immediate location” and/or “It appears that the rear left suspension is malfunctioning and the upper strut will need to be replaced. It is noticed that you are greater than 80 miles from home, would you like to book a reservation at a local hotel? There are five hotels in the area rated three stars or above.”

10 Referring to Fig. 28, the diagnostic module 2028, in step 2800, receives and interprets a maintenance and/or system error and/or warning code. Such codes are known in the art of automotive design and generally depend on the automotive and/or component manufacturer. Accordingly, the diagnostic module 2028 will, generally, have a lookup table or other set of data structures to map the code not only to a corresponding condition and/or conversation
15 meaning but also behavioral rule in a rule set. In appropriate applications, the conversational meaning can be further determined based on the condition.

The diagnostic module 2028, in step 2808, provides the conversational meaning, such as audibly and/or visually, to the vehicle operator.

The diagnostic module 2028, in step 2812, determines other factors related to the
20 received code(s). The pertinent rule in the rule set, for example, can cause the diagnostic to query other components potentially impacted by the condition and/or having other data points relevant to the condition. The diagnostic module 2028, in accordance with the pertinent rule, may contact a remote node for additional information relevant to the code, including the conversational advice to be provided to the vehicle operator.

25 In step 2816, the diagnostic module 2028 provides the conversational advice to the operator. The advice may be interactive in which event the operator would query the diagnostic module 2028 for information not clear from the initially provided conversation meaning and/or advice. A menu-type structure can be used by the diagnostic module to respond to the operator request for further information. Such further information may require
30 the diagnostic module to initiate a contact, on behalf of the operator, with a remote node 1500.

In step 2820, the diagnostic module logs codes, internally and/or provides the codes to a remote node 1500 for logging, and provides for transfer of the operator to a selected entity or entities, such as one or more remote nodes 1500.

In step 2824, the diagnostic module 2028 optionally transfers the codes, on a
5 predetermined stimulus, to a remote node 1500.

Operation of Displayed Object Movement Module 2024

An operation of the displayed object movement module 2024 will now be discussed with reference to Figs. 21 and 22. The displayed object movement module 2024 enables a user to share displayed content or other image, in substantial real time and not via a message
10 transmitted by a component located physically outside of the vehicle, with one or more other input/output systems. Typically, the displayed content is simply directed by the media controller to the target display (and/or a computational device associated with the target occupant as discussed in more detail below). The displayed object can be any displayed image, including streaming video, a web page, an icon, a window, an application, other
15 content, and the like.

In step 2100, the displayed object movement module 2024 detects a stimulus. The stimulus can be, for example, receipt of a gesture by a touchscreen display of an input/output system, user selection on a first input/output system of a different second input/output system to which the displayed object is to be moved, and the like.

20 In step 2104, the displayed object movement module 2024 determines, based on the stimulus, to which input/output system display to move the displayed object.

Fig. 22A depicts one technique to determine the destination input/output system(s). Each of the dashed lines 2208a-connecting to the displayed object 2204 in the display 2200 indicates a direction, or vector, along which the displayed object 2204 is to be moved. The
25 displayed object movement module 2024 projects the direction to determine an input/output display intersected by or nearest the projection of the vector. By way of illustration, the first gesture 2208a (if received by an input/output system in a back seat) will cause the displayed object 2204 to move to the driver's input/output system (which corresponds to position "1"), the second gesture 2208b (if received by an input/output system in a back seat) will cause the
30 displayed object 2204 to move to the input/output system positioned in the middle front seating position (which corresponds to position "2"), the third gesture 2208c (if received by

an input/output system in a back seat) will cause the displayed object 2204 to move to the input/output system positioned in the right (facing the front of the vehicle) front seating position (which corresponds to position “3”), the fourth gesture 2208d (if received by an input/output system in either a front or back seat) will cause the displayed object 2204 to

5 move to the left adjacent input/output system (relative to the gesture receiving input/output system) (which corresponds to position “4”), the fifth gesture 2208e (if received by an input/output system in either a front or back seat) will cause the displayed object 2204 to move to the right adjacent input/output system (relative to the gesture receiving input/output system) (which corresponds to position “5”), the sixth gesture 2208f (if received by an

10 input/output system in a front seat) will cause the displayed object 2204 to move to the input/output system positioned in the left rear seating position (which corresponds to position “6”), the seventh gesture 2208g (if received by an input/output system in a front seat) will cause the displayed object 2204 to move to the input/output system positioned in the middle rear seating position (which corresponds to position “7”), and finally the eighth gesture

15 2208h (if received by an input/output system in a front seat) will cause the displayed object 2204 to move to the input/output system positioned in the right rear seating position (which corresponds to position “8”).

Fig. 22B depicts one technique to determine the destination input/output system(s). The display 2200 of the user’s input/output system displays a seating diagram of the vehicle.

20 The first seat icon 2212a corresponds to the driver’s seating position, the second seat icon 2212b to the middle front seating position (if present), the third seat icon 2212c to the right front seating position, the fourth seat icon 2212d to the left rear seating position, the fifth seat icon 2212e to the middle rear seating position (if present), and the sixth seat icon 2212f to the right rear seating position. This display would typically be selected from the display

25 containing the displayed object to be moved and would be selected before or after selection of the displayed object for movement. Unlike the prior technique, which generally requires the displayed object to be moved to multiple input/output systems sequentially or entry of multiple gestures, which can be laborious, the seating diagram enables the displayed object to be moved substantially simultaneously to multiple input/output systems. Specifically,

30 selection of a seating position selects the input/output system servicing the seating position. Multiple seating positions can be selected from the display 2200, which, when a movement

command is received, causes the displayed object to be moved to each of the input/output system(s) servicing the seating position(s) selected.

Other modalities for sharing the displayed object or content are possible. The displayed object movement module 2024 can provide the user seeking to share content with a list of the sensed identities of the various vehicle occupants. The user can simply select the occupants, by his or her corresponding unique identifier, to receive the shared content. When selected, the vehicle processing module would have a corresponding seating position and display for each named occupant. The content is, upon receipt of a “share” or “send” command then shared with each selected occupant’s respective delay. The identity can be name, nickname, contact address (such as email address or instant message handle), and the like. The identity of each occupant can be sensed by any suitable technique, including parameters, such as weight, received by a seating sensor of the occupant’s seat, seat or other settings selected by the occupant and received by a processing module, a computational device, such as a cell phone, laptop, tablet computer, e-reader, personal digital assistant, and the like carried by the occupant (such information would be exchanged, such as by a handshake, by the vehicle’s processing module and the computational device), direct input from the occupant or user, sensed biometric information, and the like.

Returning to Fig. 21, the displayed object movement module 2024 moves the displayed object selected for movement to the display of each of the selected input/output systems and alters the current display of each of the selected input/output systems to include the moved displayed object. Alteration of the display can depend on the content currently being viewed at each of the targeted displays. For example, if a target display is displaying streaming video, the moved displayed object could be minimized, giving the user the option of opening the displayed object and interrupting the video display. If a target display is inactive for a specified time period and therefore in “sleep” or “power down” mode, the moved displayed object could be maximized and the display awakened from a “sleep” or “power down” mode to display the maximized displayed object. The format and other display parameters of the shared content or displayed object can also be based on default or preferences of the sharing user or selected recipient (or target occupant) or a further command received from the sharing user or target occupant.

In decision diamond 2112, the displayed object movement module 2024 determines whether to continue display of the displayed object on the source display which received the movement command for the displayed object. The determination can be based on default or preferences of the sharing user or target occupant or a further command received from the the sharing user or target occupant. When the source display is to be altered, the displayed object movement module 2024, in step 2116, alters the source display to remove the displayed object. When the source display is not to be altered, the displayed object movement module 2024, in step 2120, continues to display the displayed object.

Problems can arise when the display of the target occupant is not activated. The vehicle processing module can determine which of the displays are activated and not activated. The vehicle processing module can cause each of the targeted displays to be activated if not already activated. Alternatively, the processing module can simply ignore any share command for those targeted displays that are not activated but perform the command for those targeted displays that are activated.

One optional operating mode of the displayed object movement module 2024 is to share the displayed object or other selected content with a computational device such as a cell phone, laptop, tablet computer, e-reader, personal digital assistant, and the like, carried and/or associated with one or more selected occupants and currently present in the vehicle. In that event, the content can be shared with the targeted display if activated and/or with the computational device if activated. The sharing user could specify which of the display and computational device is to be the recipient of the shared content. Alternatively, an order of priority could govern the selection. For example, the display is selected if activated and, if not activated, any activated computational device associated with the recipient and currently physically present in the vehicle would be selected as the recipient.

Operation of Presence Reporting Module 2056

A presence reporting module considers local laws, individual (or contactee) context, and other factors in determining whether an individual is present (*e.g.*, for unified communications) and, if so, by what communication modalities and/or channel(s) (*e.g.*, Voice over IP, cellular call, email, texting, tweeting, instant messaging, short message service, audio and video enabled call, and the like. Local laws, for example, may prohibit cellular calls and/or texting and/or tweeting while the car is in motion. In that event, a

permissible communication channel, such as email or paging, is reported to the presence service 1500. The context could include, for example, the contactee is in the driver's seat (as determined by an on board sensor, such as a seating sensor), and the like), the vehicle is in motion, the vehicle is parked, the contactee is absent from vehicle (as determined by an on board sensor, such as a seating sensor, and the like), the contactee is currently using his or her corresponding input/output system and therefore is or is not available (depending on contactee preference), a current seating position of the contactee (e.g., whether the contactee is a driver or passenger), a current geographical and/or geopolitical location of the vehicle, and so on. Other factors include, for example, the on board communication system and/or external computational device(s) 1532 are currently out of cellular phone range, the on board communication system and/or external computational device(s) 1532 are currently roaming, the wireless connection, such as over a cellular network, with the on board communication system and/or external computational device(s) is currently unacceptable (e.g., unacceptably low signal-to-noise ratio or quality or grade of service), and the like.

In one exemplary application, the presence reporting module can determine, based on the vehicle occupant context, whether the vehicle occupant is present and available for receiving an inbound communication and/or by what communication channel and/or modality to contact the vehicle occupant. The vehicle occupant context can be one or more of whether the vehicle occupant is in the driver's seat, whether the vehicle is in motion and/or in gear, whether the vehicle is parked, whether the vehicle occupant is absent from vehicle, whether the vehicle occupant is currently using his or her corresponding on board input/output system, whether an on board vehicle transceiver to receive in bound communications is contactable, whether the on board vehicle transceiver is currently roaming, and whether a quality and/or grade of service of a wireless connection with the vehicle transceiver is unacceptable.

With reference to Fig. 29, the presence reporting module 2056, in step 2900, detects a stimulus, such as a passage of time, a query by the presence service 1500, an incoming or inbound contact, a change in user context, a change in the applicable local law due to a change in location of the vehicle, a change in contactee context, or a change in another factor.

In step 2904, the presence reporting module 2056 collects the context of the contactee, such as by querying on board sensors 1516, a input/output system 1520 corresponding to a seating location of the contactee to determine a current state of the input/output system (operational or non-operational) and/or activity of the contactee (e.g.,
5 web surfing, playing media, engaged in a phone call, etc.), an external computational device 1532 associated with the contactee, and/or the transceiver 1508 and/or network controller 1528 for information regarding the available networks for a communication and/or the quality of a connection over each network.

In decision diamond 2908, the presence reporting module 2056 determines whether
10 the previously reported presence information requires updating (e.g., the previously reported presence information is no longer valid due a sensed change). When no update is required, the presence reporting module 2056 returns to step 2900. When an update is required, the presence reporting module 2056 proceeds to step 2912.

In step 2912, the presence reporting module 2056 reports the update(s) (or changes to
15 the previously reported presence information) to the presence service 1500.

In step 2916, the presence service 1500 receives the update(s) and updates the current presence information for the associated contactee.

Operation of Networking Module 2070

An operation of the networking module 2070 will now be discussed with reference to
20 Fig. 30.

Networking, particularly social networking, among vehicles can add a new dimension to driving. For example, an operator can socially network with a friend driving in the next lane. Although this can be done with cell phones, it can be difficult to retrieve the number while driving let alone to dial it without increasing accident risk. Rather than fuming
25 silently, occupants of different vehicles can conduct a social round table as they sit in gridlock. If an operator wanted to communicate with another car, he or she could address it using the license plate number. When the networking session is a social networking session, the networking participants in each of the networked vehicles can be members of a preexisting online community, e-community, and/or virtual community.

30 There are a myriad of other examples of networked vehicles. Networked vehicles, for example, can enable multiple cars to connect while on car trips to share information about

how much gas is left in the fuel tanks, competing fuel economy between the cars, shared routes, and land marks and gas stations on the route ahead. Networked vehicles can record the real-time fuel economy of a vehicle and then compare that fuel economy to peers, thereby enabling the driver to see other drivers that have driven the same, or similar routes, and
5 receive suggestions from other drivers on the best route for the best fuel economy. A ride-sharing network can encourage ad hoc carpooling and provide a rating and recommendation system for its users. Networked vehicles can play games with one another. Since the game could have access to car metrics, games could incorporate actual car data, such as speed, fuel, *etc.* Games could simulate what would happen if an operator drove the way he or she wanted
10 to. Kids in socially networked vehicles can play games against one another.

With reference to Fig. 30, the processing module of a vehicle receives a stimulus in step 3000. The stimulus can be a request by a user to initiate a network with a vehicle identified by the user providing the license plate number, receipt of a request for initiating a networking session from another vehicle, the determination that a vehicle of a socially
15 networked contact is available to initiate a networking session, and the like.

In step 3004, the social networking module 2070 identifies the vehicles in wireless communication with the selected vehicle and having one or more occupants in a networking relationship with a current vehicle occupant. The networked vehicles are typically in spatial proximity to one another, with the networking messages being exchanged over a short-range
20 wireless technology forming a personal area network such that the information is not exchanged over the Internet. The networked vehicles can be in spatial proximity to one another, the networking messages can be exchanged using a short wavelength radio transmission having a limited range, and the radio transmission can use a frequency band ranging from about 2 to about 3 GHz.

25 In step 3008, the networking module 2070 determines whether or not to initiate a networking session. This can be determined by receiving user input, predetermined rules provided by the user, legal restrictions on the ability of the current or other vehicle to engage in a networking session, and the like.

When a networking session is to be initiated, the networking module 2070, in step
30 3012, initiates the session.

In optional step 3016, the networking module 2070 collects vehicle information and provides the information to the networked vehicle. The other vehicle, in return, can provide its collected vehicle information.

5 In step 3020, the networking module terminates or suspends the session when a vehicle occupant leaves one of the networked vehicles and/or at the request of a vehicle occupant.

After step 3020 or when no networking session is to be initiated (decision diamond 3008), the networking module 2070 returns to step 3000.

10 The exemplary systems and methods of this disclosure have been described in relation to vehicle processing modules. However, to avoid unnecessarily obscuring the present disclosure, the preceding description omits a number of known structures and devices. This omission is not to be construed as a limitation of the scopes of the claims. Specific details are set forth to provide an understanding of the present disclosure. It should however be appreciated that the present disclosure may be practiced in a variety of ways
15 beyond the specific detail set forth herein.

Furthermore, while the exemplary aspects, embodiments, and/or configurations illustrated herein show the various components of the system collocated, certain components of the system can be located remotely, at distant portions of a distributed network, such as a LAN and/or the Internet, or within a dedicated system. Thus, it should be appreciated, that
20 the components of the system can be combined in to one or more devices, such as a vehicle computer system, a Personal Computer (PC), laptop, netbook, smart phone, Personal Digital Assistant (PDA), tablet, *etc.*, or collocated on a particular node of a distributed network, such as an analog and/or digital communications network, a packet-switch network, or a circuit-switched network or collocated on a particular node of a distributed network, such as an
25 analog and/or digital communications network, a packet-switch network, or a circuit-switched network. It will be appreciated from the preceding description, and for reasons of computational efficiency, that the components of the system can be arranged at any location within a distributed network of components without affecting the operation of the system. For example, the various components can be located in a server. Similarly, one or more
30 functional portions of the system could be distributed between a communications device(s) and an associated computing device.

Furthermore, it should be appreciated that the various links connecting the elements can be wired or wireless links, or any combination thereof, or any other known or later developed element(s) that is capable of supplying and/or communicating data to and from the connected elements. These wired or wireless links can also be secure links and may be
5 capable of communicating encrypted information. Transmission media used as links, for example, can be any suitable carrier for electrical signals, including coaxial cables, copper wire and fiber optics, and may take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

Also, while the flowcharts have been discussed and illustrated in relation to a
10 particular sequence of events, it should be appreciated that changes, additions, and omissions to this sequence can occur without materially affecting the operation of the disclosed embodiments, configuration, and aspects.

A number of variations and modifications of the disclosure can be used. It would be possible to provide for some features of the disclosure without providing others.

15 For example in one alternative embodiment, the application store is applied in a vehicle other than a wheeled or tracked vehicle. For example, the application store can be implemented in an aircraft, boat, ship, and the like.

In another alternative embodiment, the application store can include not only media player software but also media itself. Media, for example, can involve one or more media
20 types (e.g., audio and/or video). Media can thus refer to music, movies, videos, audio books, pictures, screen savers, display wallpaper, and the like.

In yet another embodiment, the systems and methods of this disclosure can be implemented in conjunction with a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit element(s), an ASIC or other integrated
25 circuit, a digital signal processor, a hard-wired electronic or logic circuit such as discrete element circuit, a programmable logic device or gate array such as PLD, PLA, FPGA, PAL, special purpose computer, any comparable means, or the like. In general, any device(s) or means capable of implementing the methodology illustrated herein can be used to implement the various aspects of this disclosure. Exemplary hardware that can be used for the disclosed
30 embodiments, configurations and aspects includes computers, handheld devices, telephones (e.g., cellular, Internet enabled, digital, analog, hybrids, and others), and other hardware

known in the art. Some of these devices include processors (e.g., a single or multiple microprocessors), memory, nonvolatile storage, input devices, and output devices. Furthermore, alternative software implementations including, but not limited to, distributed processing or component/object distributed processing, parallel processing, or virtual machine processing can also be constructed to implement the methods described herein.

In yet another embodiment, the disclosed methods may be readily implemented in conjunction with software using object or object-oriented software development environments that provide portable source code that can be used on a variety of computer or workstation platforms. Alternatively, the disclosed system may be implemented partially or fully in hardware using standard logic circuits or VLSI design. Whether software or hardware is used to implement the systems in accordance with this disclosure is dependent on the speed and/or efficiency requirements of the system, the particular function, and the particular software or hardware systems or microprocessor or microcomputer systems being utilized.

In yet another embodiment, the disclosed methods may be partially implemented in software that can be stored on a storage medium, executed on programmed general-purpose computer with the cooperation of a controller and memory, a special purpose computer, a microprocessor, or the like. In these instances, the systems and methods of this disclosure can be implemented as program embedded on personal computer such as an applet, JAVA® or CGI script, as a resource residing on a server or computer workstation, as a routine embedded in a dedicated measurement system, system component, or the like. The system can also be implemented by physically incorporating the system and/or method into a software and/or hardware system.

Although the present disclosure describes components and functions implemented in the aspects, embodiments, and/or configurations with reference to particular standards and protocols, the aspects, embodiments, and/or configurations are not limited to such standards and protocols. Other similar standards and protocols not mentioned herein are in existence and are considered to be included in the present disclosure. Moreover, the standards and protocols mentioned herein and other similar standards and protocols not mentioned herein are periodically superseded by faster or more effective equivalents having essentially the same functions. Such replacement standards and protocols having

The present disclosure, in various aspects, embodiments, and/or configurations, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various aspects, embodiments, configurations embodiments, subcombinations, and/or subsets thereof. Those of skill in the art will understand how to
5 make and use the disclosed aspects, embodiments, and/or configurations after understanding the present disclosure. The present disclosure, in various aspects, embodiments, and/or configurations, includes providing devices and processes in the absence of items not depicted and/or described herein or in various aspects, embodiments, and/or configurations hereof, including in the absence of such items as may have been used in previous devices or
10 processes, e.g., for improving performance, achieving ease and/or reducing cost of implementation.

The foregoing discussion has been presented for purposes of illustration and description. The foregoing is not intended to limit the disclosure to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the
15 disclosure are grouped together in one or more aspects, embodiments, and/or configurations for the purpose of streamlining the disclosure. The features of the aspects, embodiments, and/or configurations of the disclosure may be combined in alternate aspects, embodiments, and/or configurations other than those discussed above. This method of disclosure is not to be interpreted as reflecting an intention that the claims require more features than are
20 expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed aspect, embodiment, and/or configuration. Thus, the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the disclosure.

Moreover, though the description has included description of one or more aspects, embodiments, and/or configurations and certain variations and modifications, other variations, combinations, and modifications are within the scope of the disclosure, e.g., as
25 may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative aspects, embodiments, and/or configurations to the extent permitted, including alternate, interchangeable and/or
30 equivalent structures, functions, ranges or steps to those claimed, whether or not such

alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

What is claimed is:

1. A vehicle, comprising:

a plurality of processing modules to control a plurality of automated vehicle tasks, functions and/or operations, wherein a first processing module is in an active mode whereby
5 the first processing module is in primary control of at least most automated vehicle tasks, functions and/or operations and a second processing module is in a standby mode whereby the second processing module is ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

2. The vehicle of claim 1, wherein the first and second processing modules are in
10 wireless communication with one another, and wherein a state of the second processing module is maintained substantially in synchronicity with a state of the first processing module to enable a stateful failover from the first processing module to the second processing module.

3. The vehicle of claim 1, wherein the plurality of automated vehicle tasks,
15 functions and/or operations comprise monitoring, controlling and/or operating a plurality of the following: an engine and/or power control unit, transmission control unit (TCU), a door setting, a window setting, a blind spot monitor, an airbag deployment control unit, a collision sensor, a nearby object sensing system, a seat belt control unit, a sensor for a seat belt setting, a power source controller, an energy output sensor, an engine temperature sensor, oil
20 pressure, hydraulic pressure, a headlight, an emergency light, a brake light, a parking light, a fog light, an interior and/or passenger compartment light, a tail light, a vehicle control system sensor, a wireless network, a cellular data sensor, a steering sensor, a torque sensor, an engine, power steering, a display panel, switch state control unit, and a brake control unit.

4. The vehicle of claim 1, wherein the plurality of automated vehicle tasks,
25 functions and/or operations comprise monitoring, controlling and/or operating a plurality of the following: an emissions system, a seating system controller and/or sensor, an entertainment system, monitoring an ambient (outdoor) weather sensor, an odometer reading sensor, a trip mileage reading sensor, a road condition sensor, a radar transmitter/receiver output, a brake wear sensor, an oxygen sensor, an ambient lighting sensor, a vision system
30 sensor, a ranging sensor, a parking sensor, a heating, venting, and air conditioning (HVAC)

system and/or sensor, a water sensor, a air-fuel ratio meter, a hall effect sensor, a microphone, a radio frequency (RF) sensor, and/or an infrared (IR) sensor.

5 5. The vehicle of claim 1, wherein the first and second processing modules are duplicated and further comprising an arbitration module to arbitrate hand-off conflicts
5 between the duplicated first and second processing modules.

6. The vehicle of claim 5, wherein the arbitration module selects one of the first and second processing modules to currently possess and/or own a token, the token indicating at least one of (i) which processing module is an active processing module and/or which processing module is a standby processing module and (ii) which processing module is
10 responsible for a selected set of processing tasks, functions, and/or operations associated with the token.

7. The vehicle of claim 1, wherein the first and second processing modules are duplicated and further comprising a health check module to determine a corresponding state of health of each of the duplicated first and second processing modules to perform at least
15 one of critical and non-critical tasks, functions, and operations.

8. The vehicle of claim 7, wherein the health check module performs a check and/or test, in response to an internally generated interrupt and/or request to determine a selected processing module's ability to perform critical and/or non-critical vehicle tasks, functions, and/or operations, assign a score to the selected processing module based on the
20 check and/or test results, and/or compare the score to one or more thresholds and/or to a score of a different processing module to determine a relative and/or absolute state of health of the selected processing module.

9. The vehicle of claim 8, wherein the arbitration module, based on the relative and/or absolute state of health of each of the first and second processing modules selects one
25 of the first and second processing modules as a primary processing module in primary control of the at least most automated vehicle tasks, functions and/or operations and the other of the first and second processing modules as a secondary processing module in standby mode.

10. The vehicle of claim 9, wherein a hand-off procedure is activated whereby
30 primary control is passed from the first processing module to the secondary processing module and the first processing module enters the standby mode.

11. The vehicle of claim 8, wherein the relative weighting of at least some tasks, functions and/or operations in assigning the score is a function of geographic location of the vehicle.

12. The vehicle of claim 1, wherein, for a first set of tasks, functions, and/or operations, the first processing module is in primary control and the second processing module is in standby mode and, for a different second set of tasks, functions, and/or operations, the second processing module is in primary control and the first processing module is in standby mode.

13. The vehicle of claim 1, wherein, in the standby mode, the second processing module at least one of (a) performs shadow processing of the at least most automated vehicle tasks, functions and/or operations and (b) synchronizes stored time-stamped processing state information with time-stamped processing state information regarding the at least most automated vehicle tasks, functions and/or operations.

14. A non-transient, tangible computer readable medium comprising microprocessor executable instructions that, when executed, designate a first processing module as being in an active mode whereby the first processing module is in primary control of at least most automated vehicle tasks, functions and/or operations and a second processing module as being in a standby mode whereby the second processing module is ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

15. The computer readable medium of claim 14, wherein the first and second processing modules are in wireless communication with one another, and wherein a state of the second processing module is maintained substantially in synchronicity with a state of the first processing module to enable a stateful failover from the first processing module to the second processing module.

16. The computer readable medium of claim 14, wherein the plurality of automated vehicle tasks, functions and/or operations comprise monitoring, controlling and/or operating a plurality of the following: an engine and/or power control unit, transmission control unit (TCU), a door setting, a window setting, a blind spot monitor, an airbag deployment control unit, a collision sensor, a nearby object sensing system, a seat belt control unit, a sensor for a seat belt setting, a power source controller, an energy output

sensor, an engine temperature sensor, oil pressure, hydraulic pressure, a headlight, an emergency light, a brake light, a parking light, a fog light, an interior and/or passenger compartment light, a tail light, a vehicle control system sensor, a wireless network, a cellular data sensor, a steering sensor, a torque sensor, an engine, power steering, a display panel, switch state control unit, and a brake control unit.

17. The computer readable medium of claim 14, wherein the plurality of automated vehicle tasks, functions and/or operations comprise monitoring, controlling and/or operating a plurality of the following: an emissions system, a seating system controller and/or sensor, an entertainment system, monitoring an ambient (outdoor) weather sensor, an odometer reading sensor, a trip mileage reading sensor, a road condition sensor, a radar transmitter/receiver output, a brake wear sensor, an oxygen sensor, an ambient lighting sensor, a vision system sensor, a ranging sensor, a parking sensor, a heating, venting, and air conditioning (HVAC) system and/or sensor, a water sensor, a air-fuel ratio meter, a hall effect sensor, a microphone, a radio frequency (RF) sensor, and/or an infrared (IR) sensor.

18. The computer readable medium of claim 14, wherein the first and second processing modules are duplicated and further comprising an arbitration module to arbitrate hand-off conflicts between the duplicated first and second processing modules.

19. The computer readable medium of claim 18, wherein the arbitration module selects one of the first and second processing modules to currently possess and/or own a token, the token indicating at least one of (i) which processing module is an active processing module and/or which processing module is a standby processing module and (ii) which processing module is responsible for a selected set of processing tasks, functions, and/or operations associated with the token.

20. The computer readable medium of claim 14, wherein the first and second processing modules are duplicated and further comprising a health check module to determine a corresponding state of health of each of the duplicated first and second processing modules to perform at least one of critical and non-critical tasks, functions, and/or operations.

21. The computer readable medium of claim 20, wherein the health check module performs a check and/or test, in response to an internally generated interrupt and/or request to determine a selected processing module's ability to perform critical and/or non-critical

vehicle tasks, functions, and/or operations, assign a score to the selected processing module based on the check and/or test results, and/or compare the score to one or more thresholds and/or to a score of a different processing module to determine a relative and/or absolute state of health of the selected processing module.

5 22. The computer readable medium of claim 21, wherein the arbitration module, based on the relative and/or absolute state of health of each of the first and second processing modules selects one of the first and second processing modules as a primary processing module in primary control of the at least most automated vehicle tasks, functions and/or operations and the other of the first and second processing modules as a secondary
10 processing module in standby mode.

 23. The computer readable medium of claim 22, wherein a hand-off procedure is activated whereby primary control is passed from the first processing module to the secondary processing module and the first processing module enters the standby mode.

 24. The computer readable medium of claim 21, wherein the relative weighting of
15 at least some tasks, functions and/or operations in assigning the score is a function of geographic location of the vehicle.

 25. The computer readable medium of claim 14, wherein, for a first set of tasks, functions, and/or operations, the first processing module is in primary control and the second processing module is in standby mode and, for a different second set of tasks, functions,
20 and/or operations, the second processing module is in primary control and the first processing module is in standby mode.

 26. The computer readable medium of claim 14, wherein, in the standby mode, the second processing module at least one of (a) performs shadow processing of the at least most automated vehicle tasks, functions and/or operations and (b) synchronizes stored time-
25 stamped processing state information with time-stamped processing state information regarding the at least most automated vehicle tasks, functions and/or operations.

 27. A method comprising:
 designating, by a microprocessor executable arbitration module, a first processing module as being in an active mode, whereby the first processing module is in primary control
30 of at least most automated vehicle tasks, functions and/or operations, and a second processing module as being in a standby mode, whereby the second processing module is

ready to assume primary control of the at least most automated vehicle tasks, functions and/or operations.

28. The method of claim 27, wherein the first and second processing modules are in wireless communication with one another, and further comprising:

5 maintaining a state of the second processing module substantially in synchronicity with a state of the first processing module to enable a stateful failover from the first processing module to the second processing module.

29. The method of claim 27, wherein the plurality of automated vehicle tasks, functions and/or operations comprise monitoring, controlling and/or operating a plurality of
10 the following: an engine and/or power control unit, transmission control unit (TCU), a door setting, a window setting, a blind spot monitor, an airbag deployment control unit, a collision sensor, a nearby object sensing system, a seat belt control unit, a sensor for a seat belt setting, a power source controller, an energy output sensor, an engine temperature sensor, oil pressure, hydraulic pressure, a headlight, an emergency light, a brake light, a parking light, a
15 fog light, an interior and/or passenger compartment light, a tail light, a vehicle control system sensor, a wireless network, a cellular data sensor, a steering sensor, a torque sensor, an engine, power steering, a display panel, switch state control unit, and a brake control unit.

30. The method of claim 27, wherein the plurality of automated vehicle tasks, functions and/or operations comprise monitoring, controlling and/or operating a plurality of
20 the following: an emissions system, a seating system controller and/or sensor, an entertainment system, monitoring an ambient (outdoor) weather sensor, an odometer reading sensor, a trip mileage reading sensor, a road condition sensor, a radar transmitter/receiver output, a brake wear sensor, an oxygen sensor, an ambient lighting sensor, a vision system sensor, a ranging sensor, a parking sensor, a heating, venting, and air conditioning (HVAC)
25 system and/or sensor, a water sensor, a air-fuel ratio meter, a hall effect sensor, a microphone, a radio frequency (RF) sensor, and/or an infrared (IR) sensor.

31. The method of claim 27, wherein the first and second processing modules are duplicated and further comprising a microprocessor executable arbitration module to arbitrate hand-off conflicts between the duplicated first and second processing modules.

30 32. The method of claim 31, wherein the arbitration module selects one of the first and second processing modules to currently possess and/or own a token, the token indicating

at least one of (i) which processing module is an active processing module and/or which processing module is a standby processing module and (ii) which processing module is responsible for a selected set of processing tasks, functions, and/or operations associated with the token.

5 33. The method of claim 27, wherein the first and second processing modules are duplicated and further comprising a microprocessor executable health check module to determine a corresponding state of health of each of the duplicated first and second processing modules to perform at least one of critical and non-critical tasks, functions, and operations.

10 34. The method of claim 33, wherein the health check module performs a check and/or test, in response to an internally generated interrupt and/or request to determine a selected processing module's ability to perform critical and/or non-critical vehicle tasks, functions, and/or operations, assign a score to the selected processing module based on the check and/or test results, and/or compare the score to one or more thresholds and/or to a
15 score of a different processing module to determine a relative and/or absolute state of health of the selected processing module.

 35. The method of claim 34, wherein the arbitration module, based on the relative and/or absolute state of health of each of the first and second processing modules selects one of the first and second processing modules as a primary processing module in primary
20 control of the at least most automated vehicle tasks, functions and/or operations and the other of the first and second processing modules as a secondary processing module in standby mode.

 36. The method of claim 35, wherein a hand-off procedure is activated whereby primary control is passed from the first processing module to the secondary processing
25 module and the first processing module enters the standby mode.

 37. The method of claim 34, wherein the relative weighting of at least some tasks, functions and/or operations in assigning the score is a function of geographic location of the vehicle.

 38. The method of claim 27, wherein, for a first set of tasks, functions, and/or
30 operations, the first processing module is in primary control and the second processing module is in standby mode and, for a different second set of tasks, functions, and/or

operations, the second processing module is in primary control and the first processing module is in standby mode.

39. The method of claim 27, wherein, in the standby mode, the second processing module at least one of (a) performs shadow processing of the at least most automated vehicle tasks, functions and/or operations and (b) synchronizes stored time-stamped processing state information with time-stamped processing state information regarding the at least most automated vehicle tasks, functions and/or operations.
- 5

ABSTRACT

The present disclosure describes a vehicle implementing one or more processing modules. These modules are configured to connect and interface with the various buses in the vehicle, where the various buses are connected with the various components of the vehicle to facilitate information transfer among the vehicle components. Each processing module is further modularized with the ability to add and replace other functional modules now or in the future. These functional modules can themselves act as distinct vehicle components. Each processing module may hand-off processing to other modules depending on its health, processing load, or by third-party control. Thus, the plurality of processing modules helps to implement a middleware point of control to the vehicle with redundancy in processing and safety and security awareness in their applications.



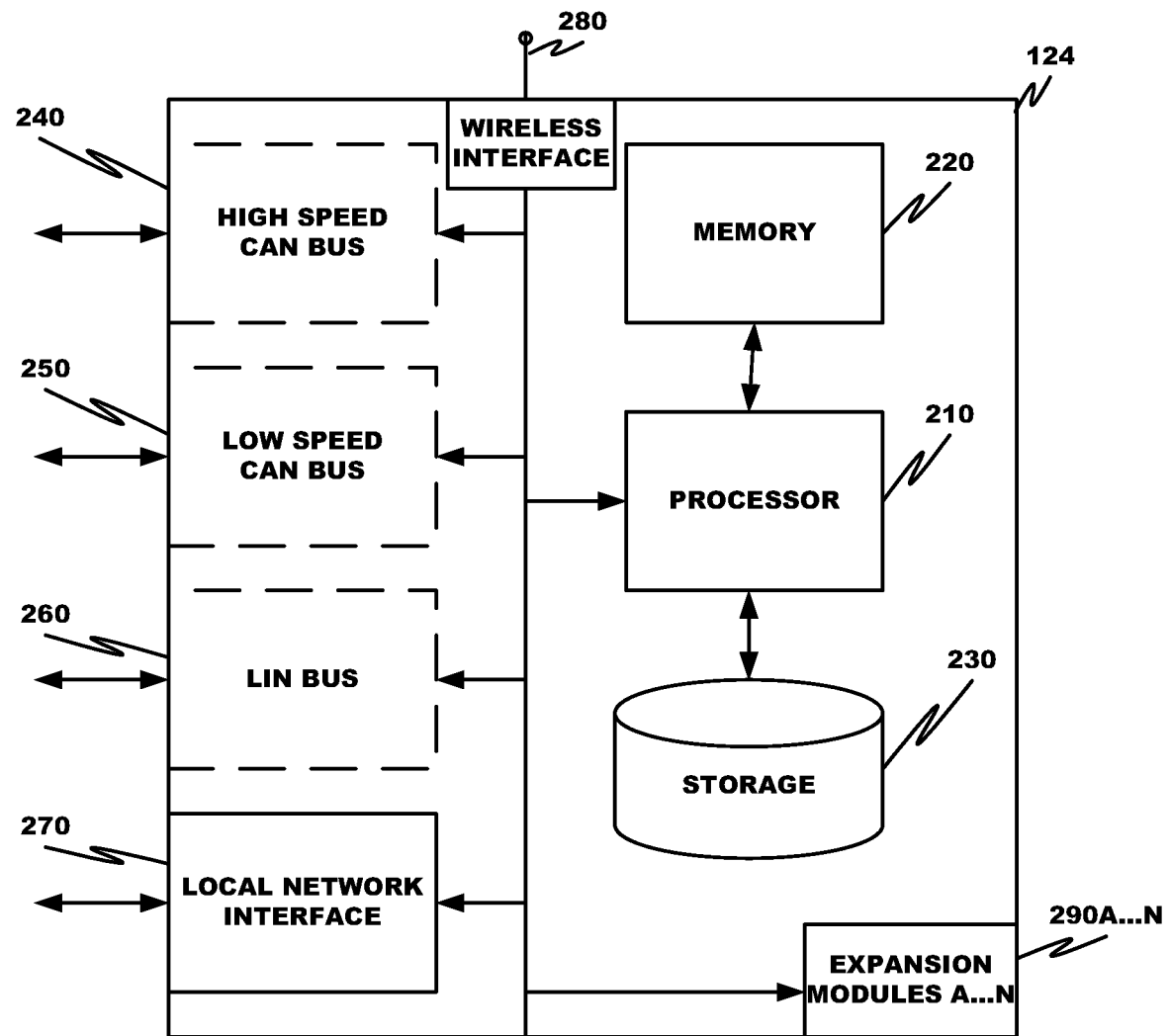


Fig. 2

200

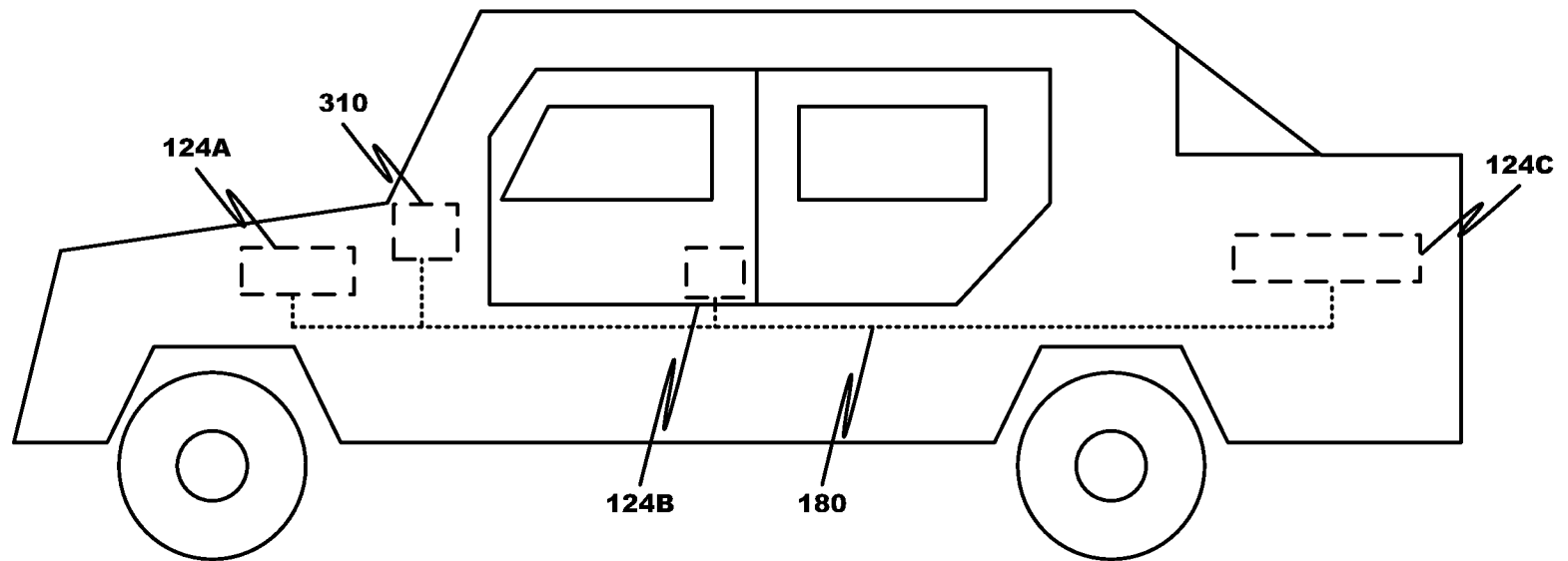


Fig. 3

300

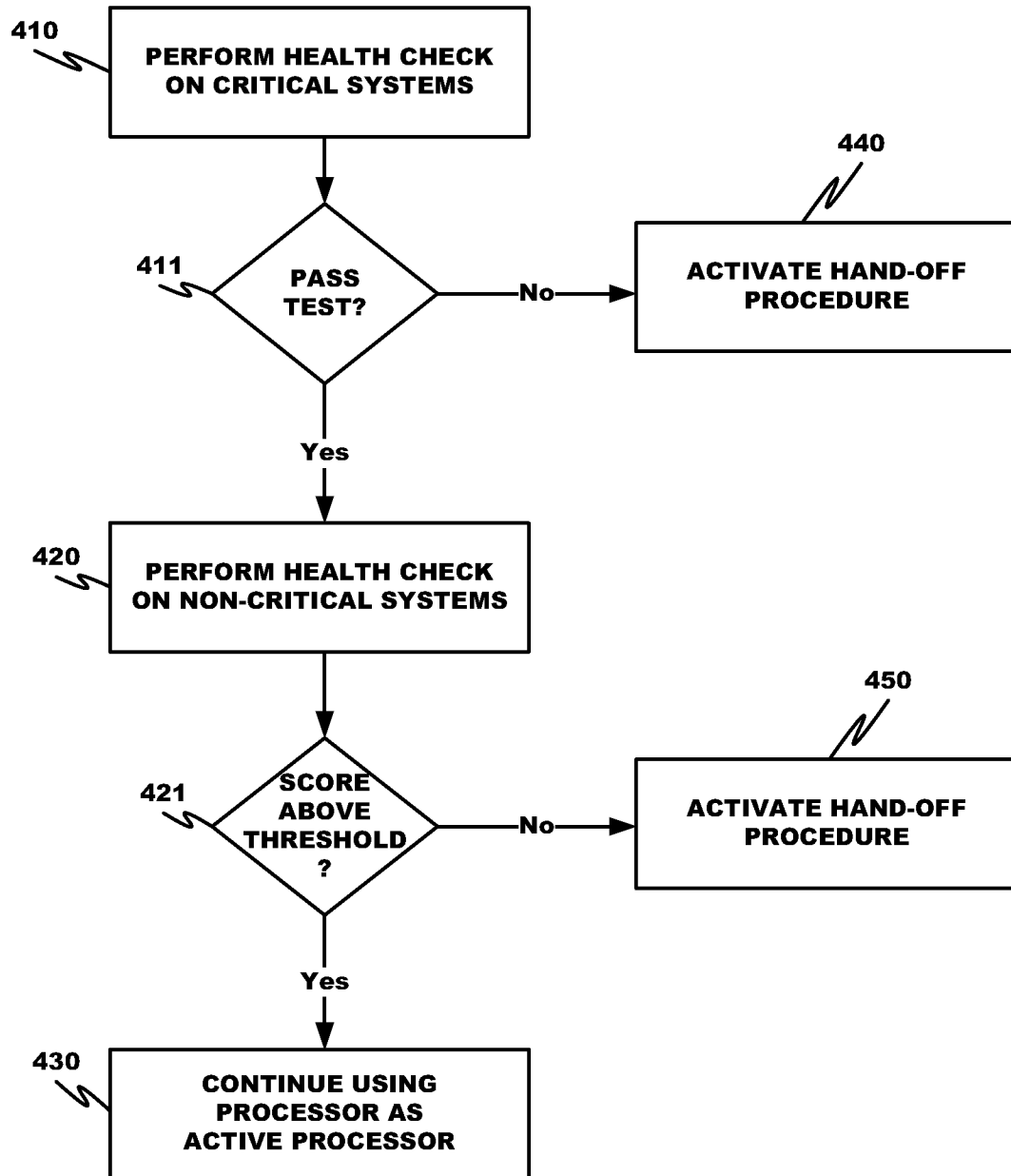


Fig. 4

400

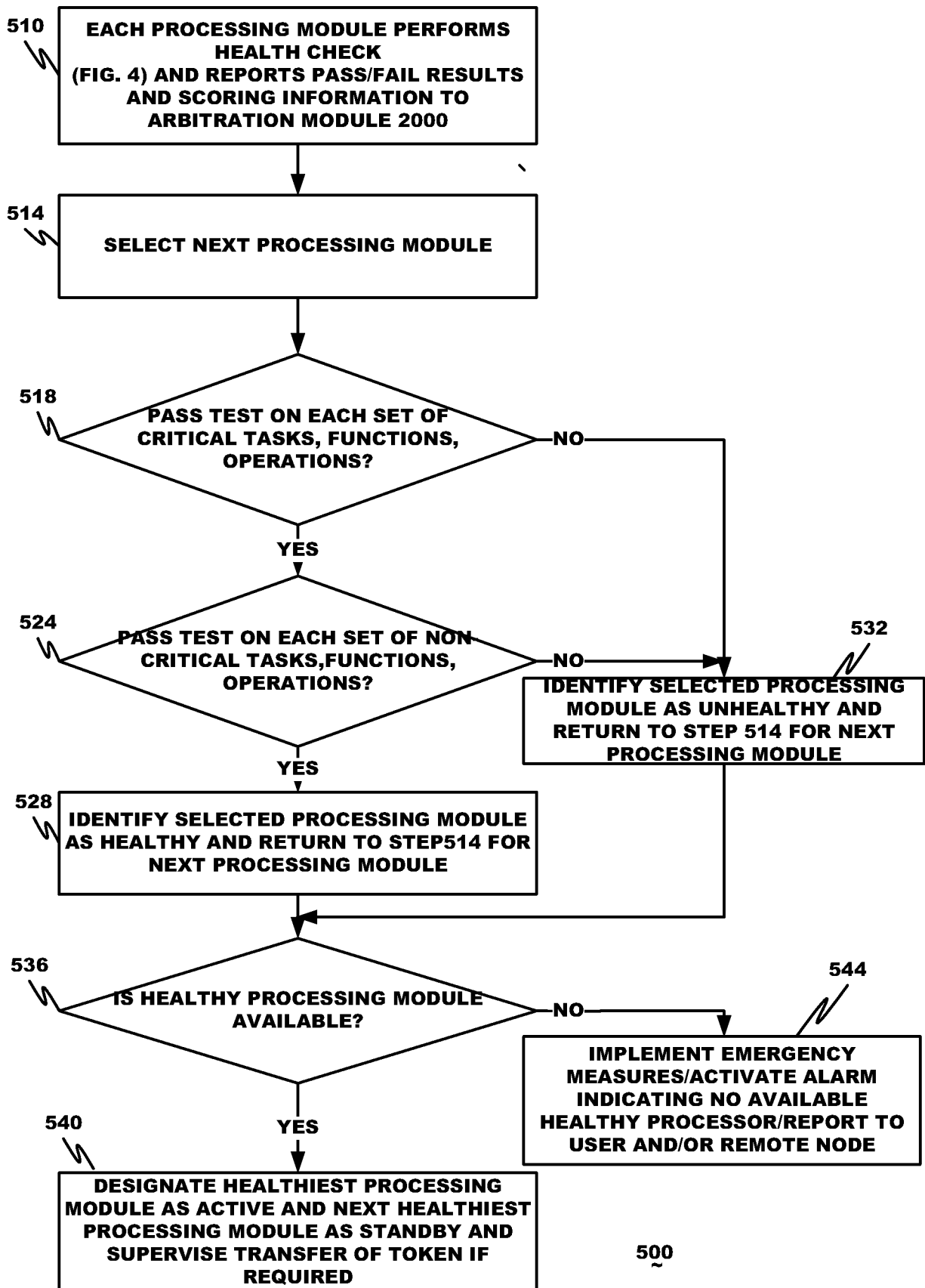


Fig. 5

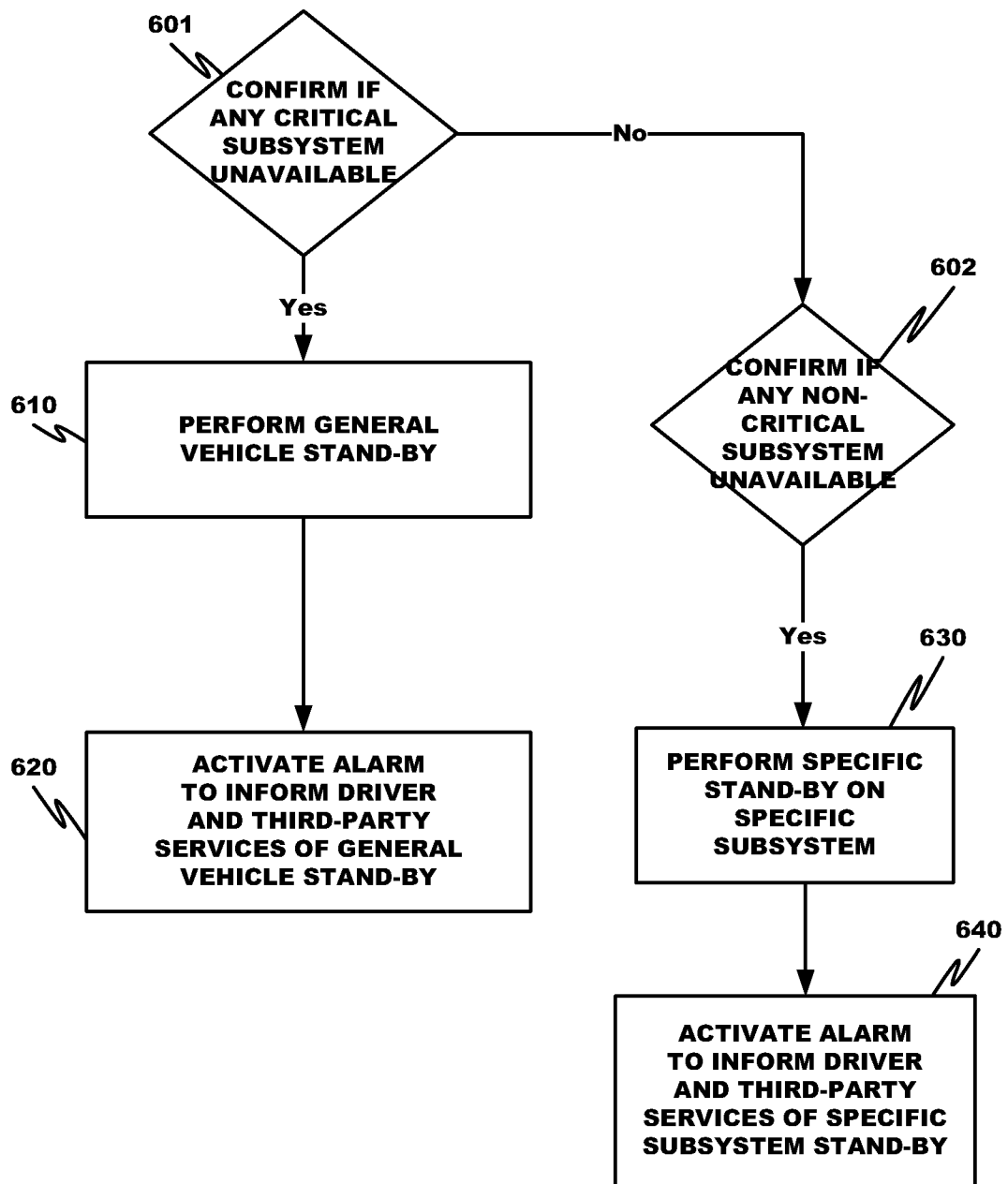


Fig. 6

600

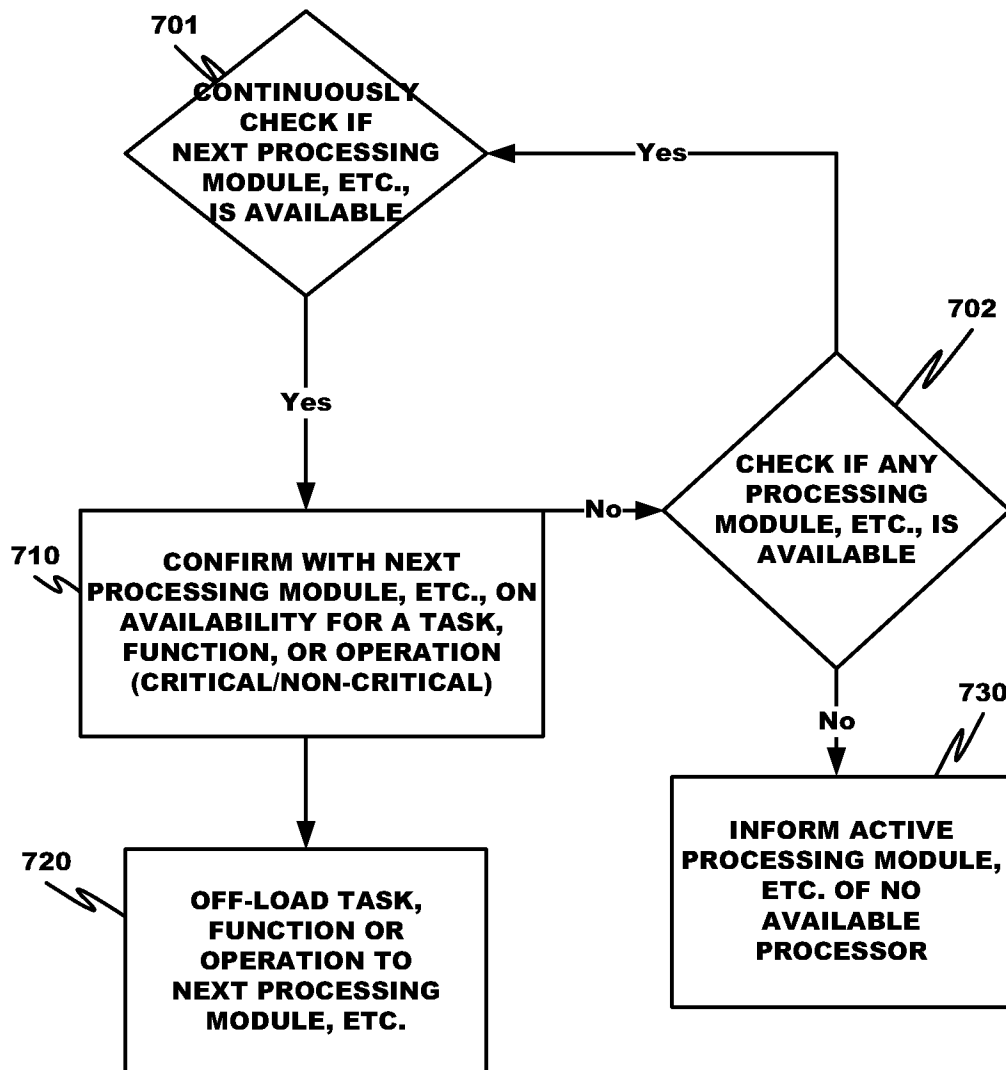


Fig. 7

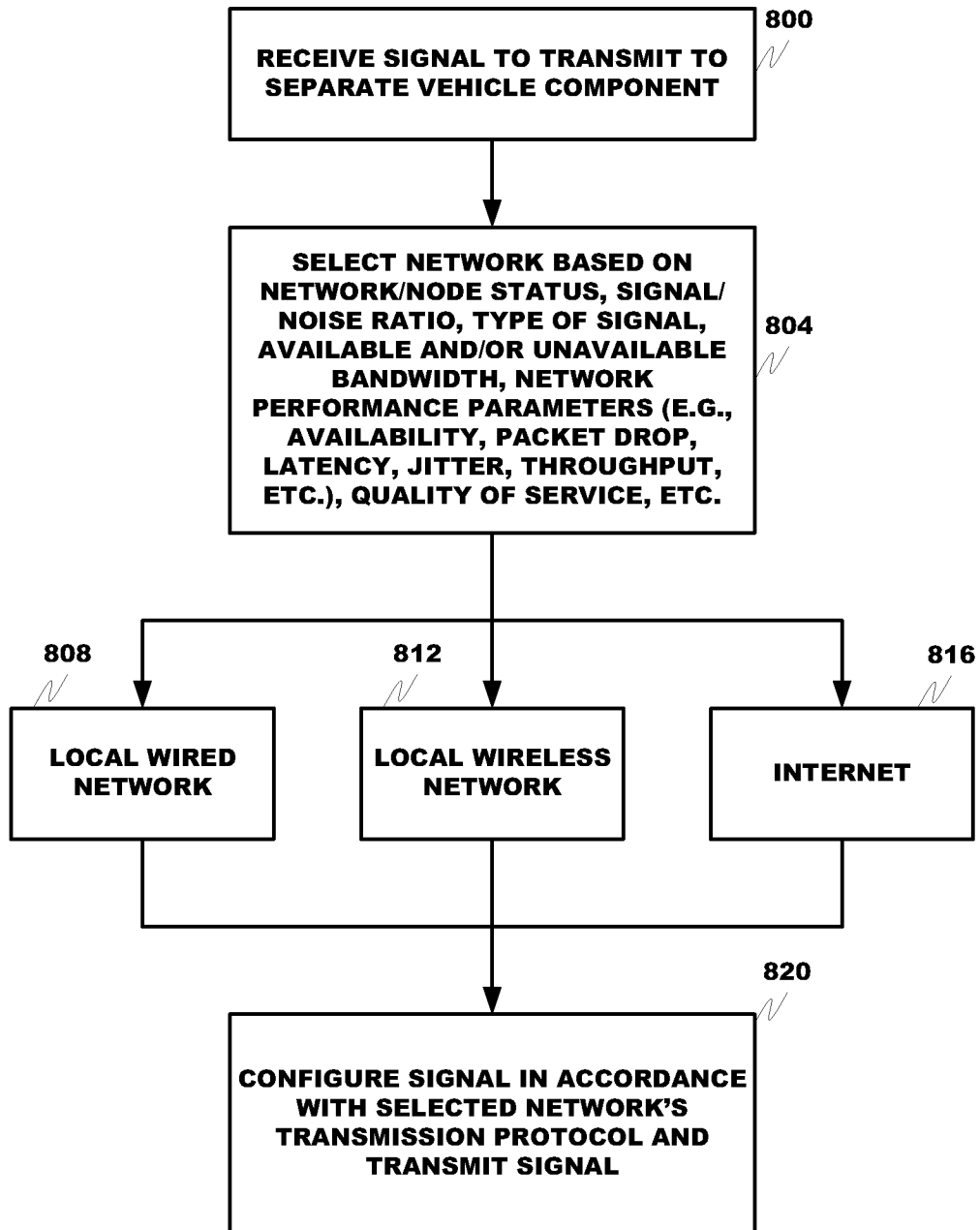


FIG. 8

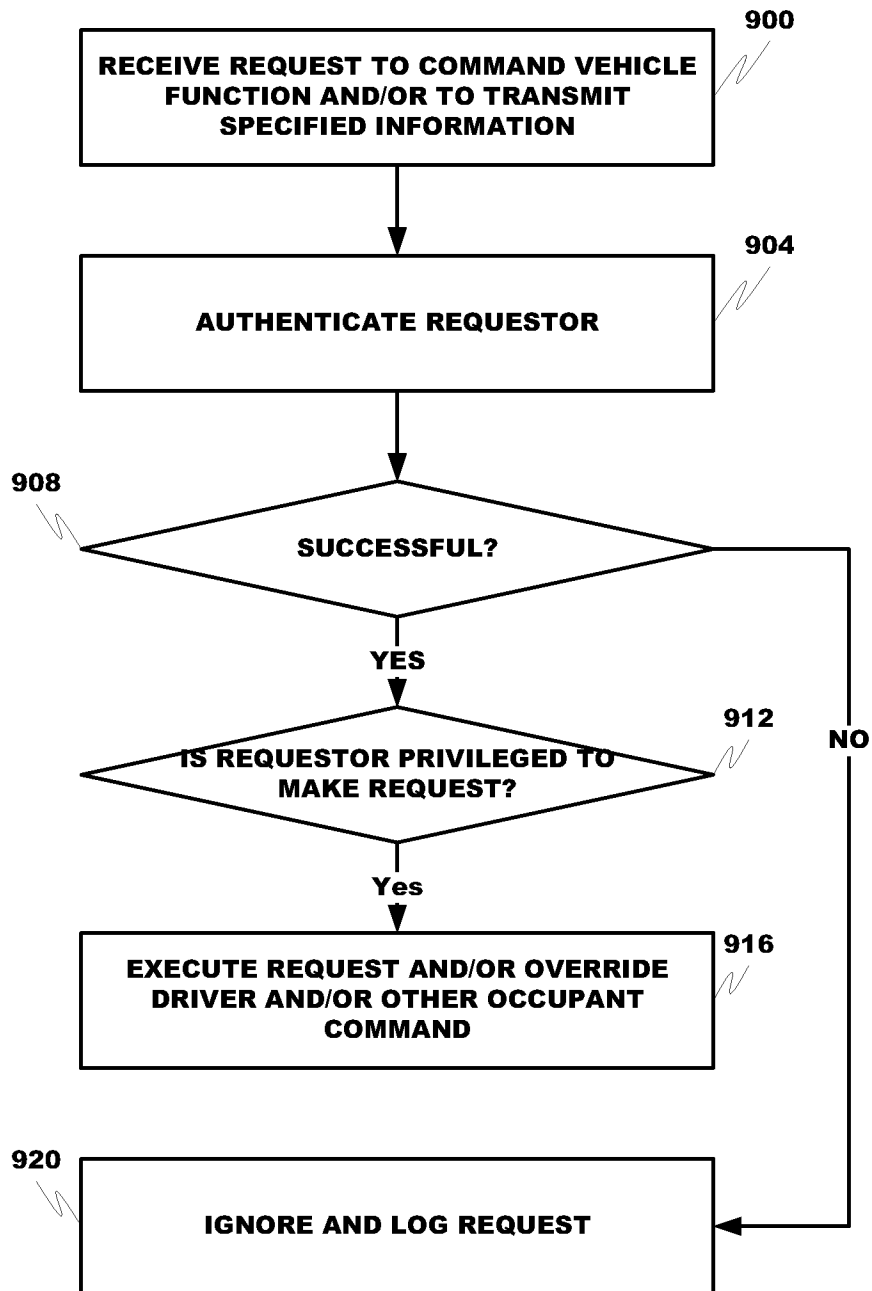


FIG. 9

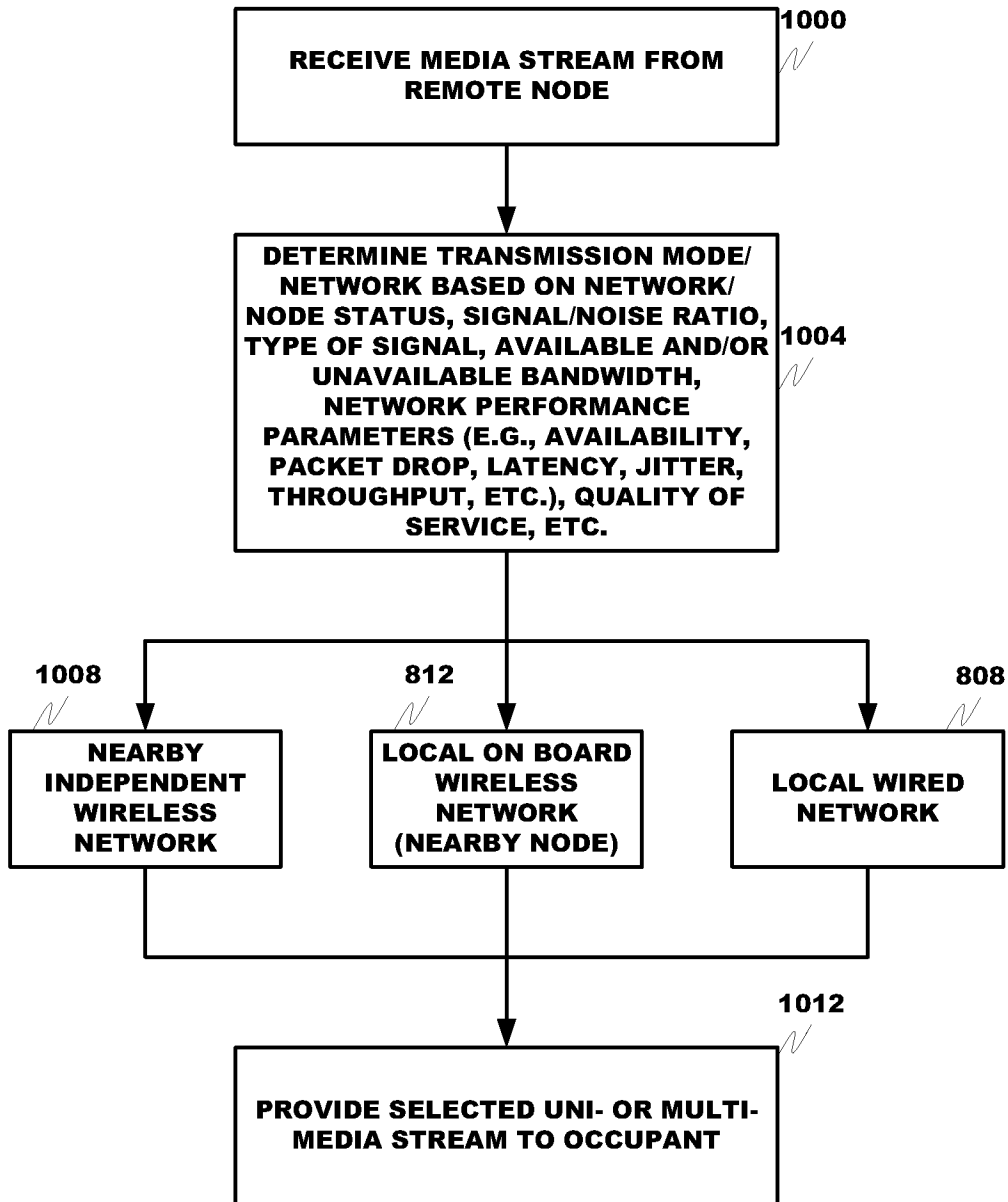


FIG. 10

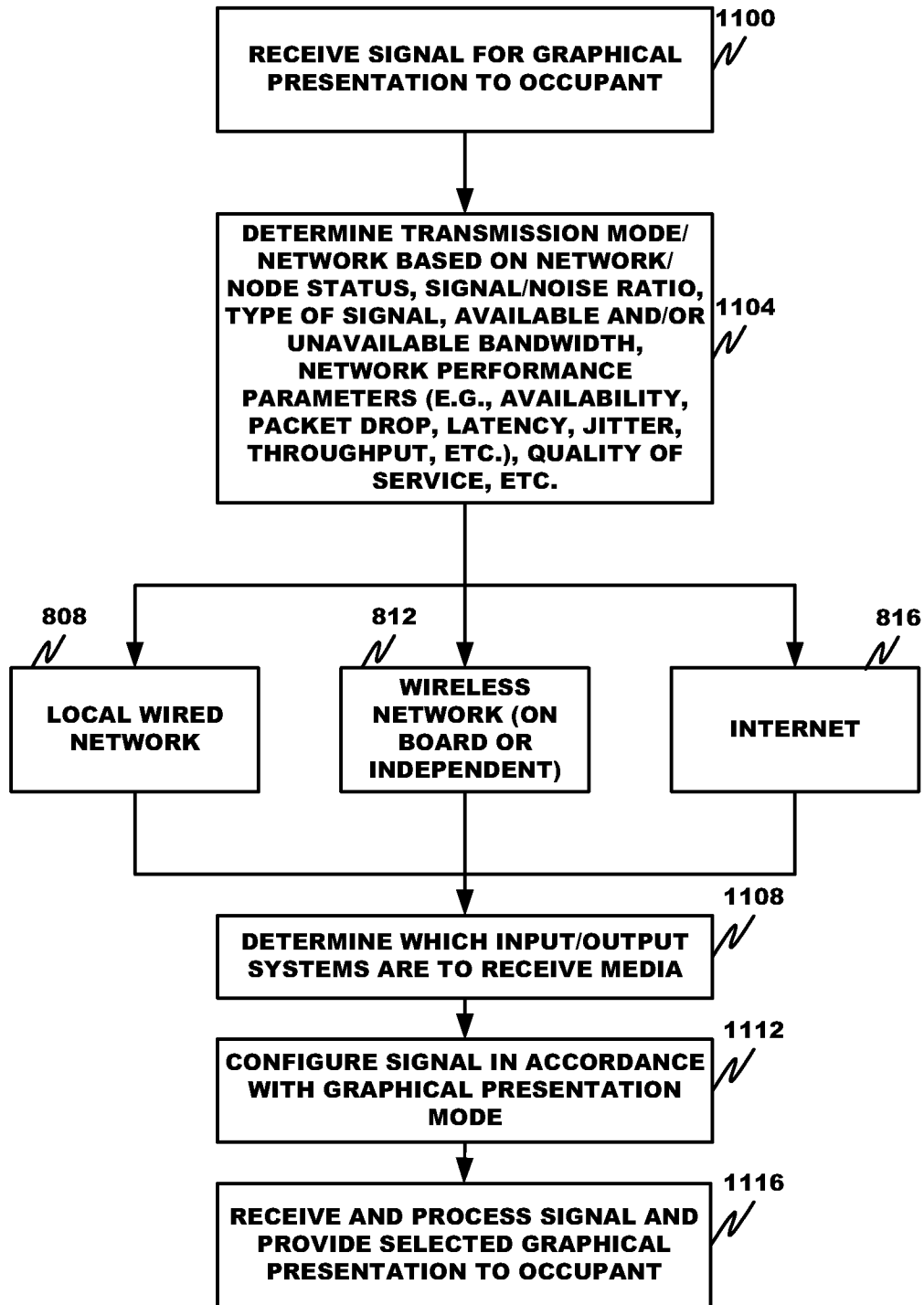


FIG. 11

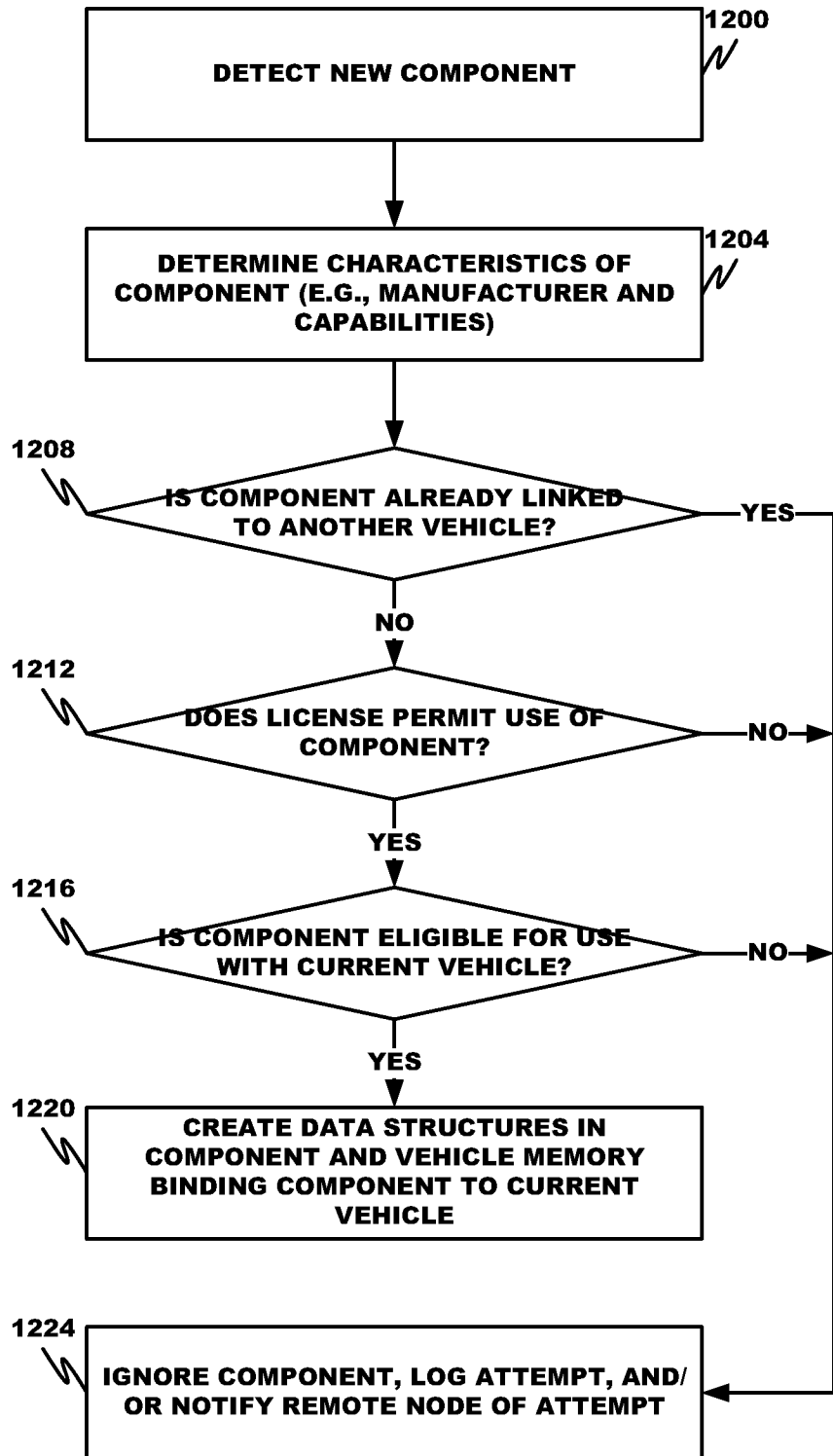


FIG. 12

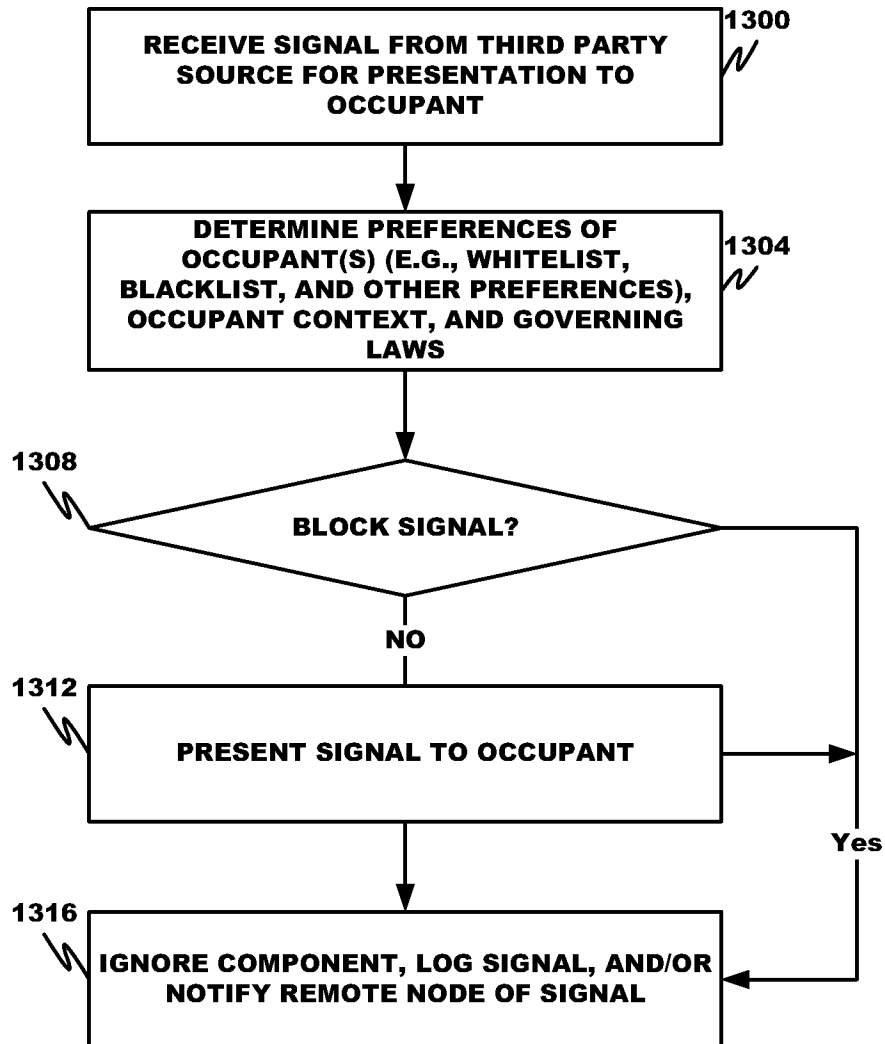


FIG. 13

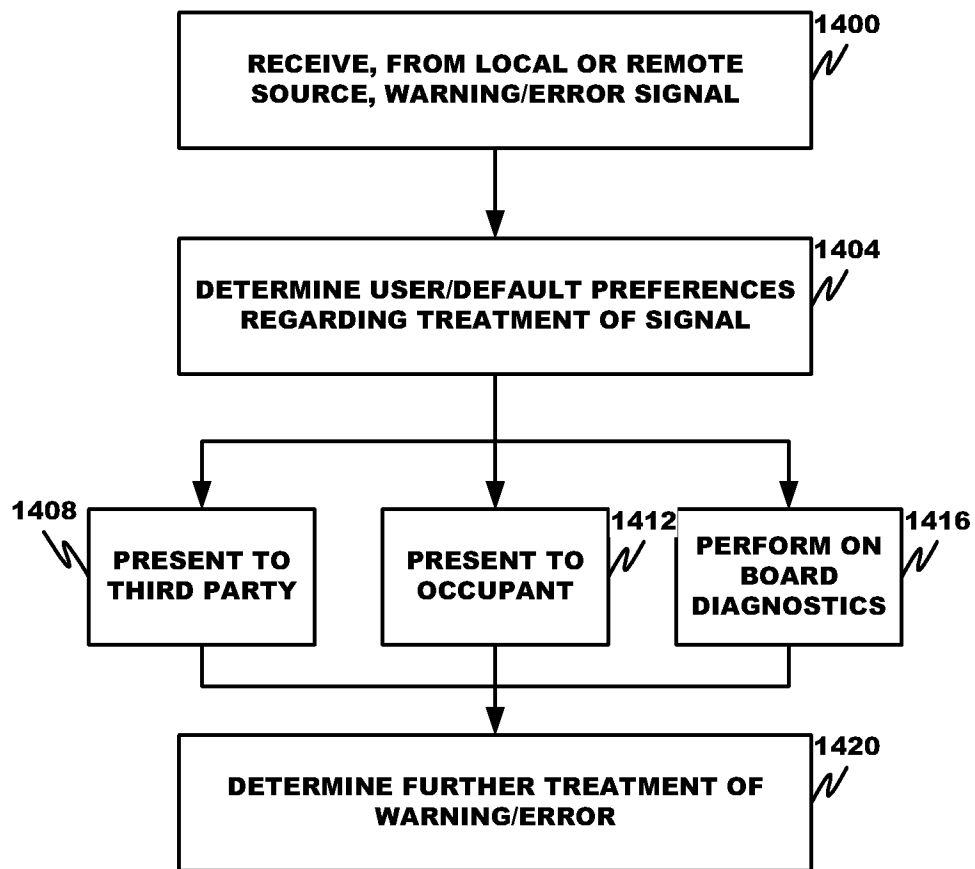


FIG. 14

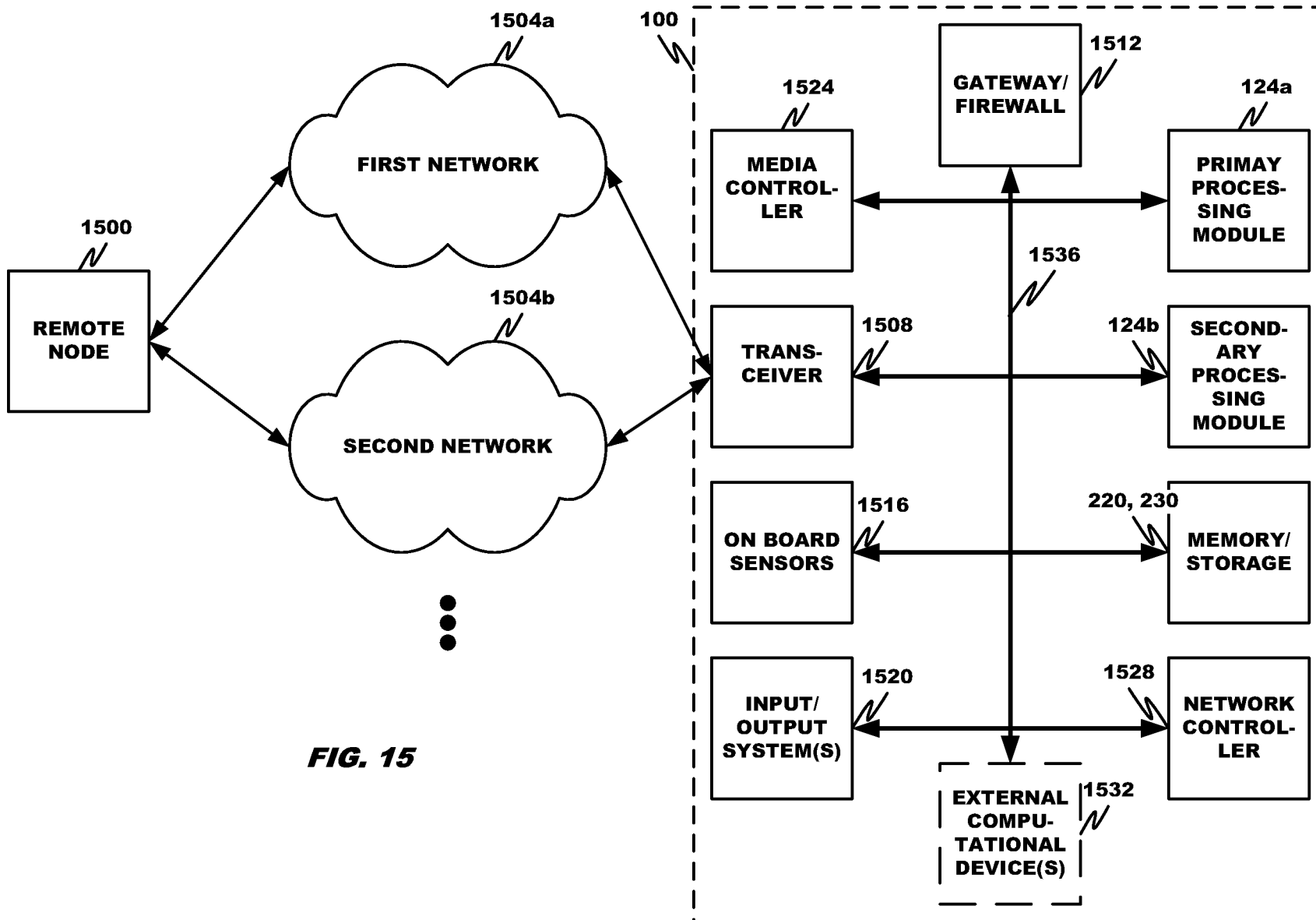


FIG. 15

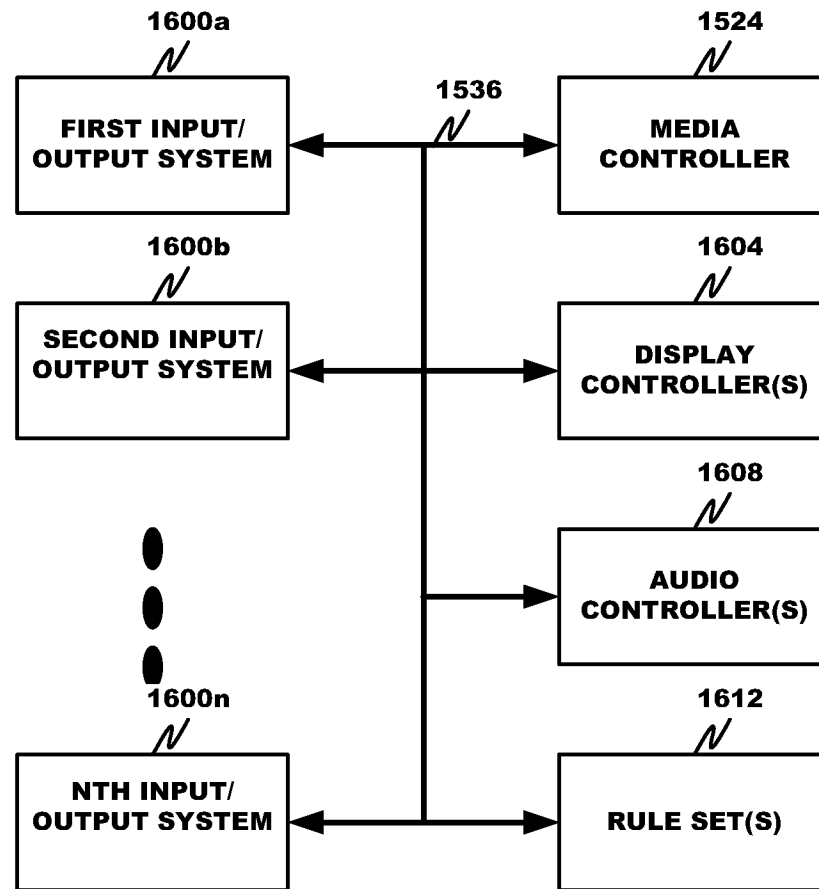


FIG. 16

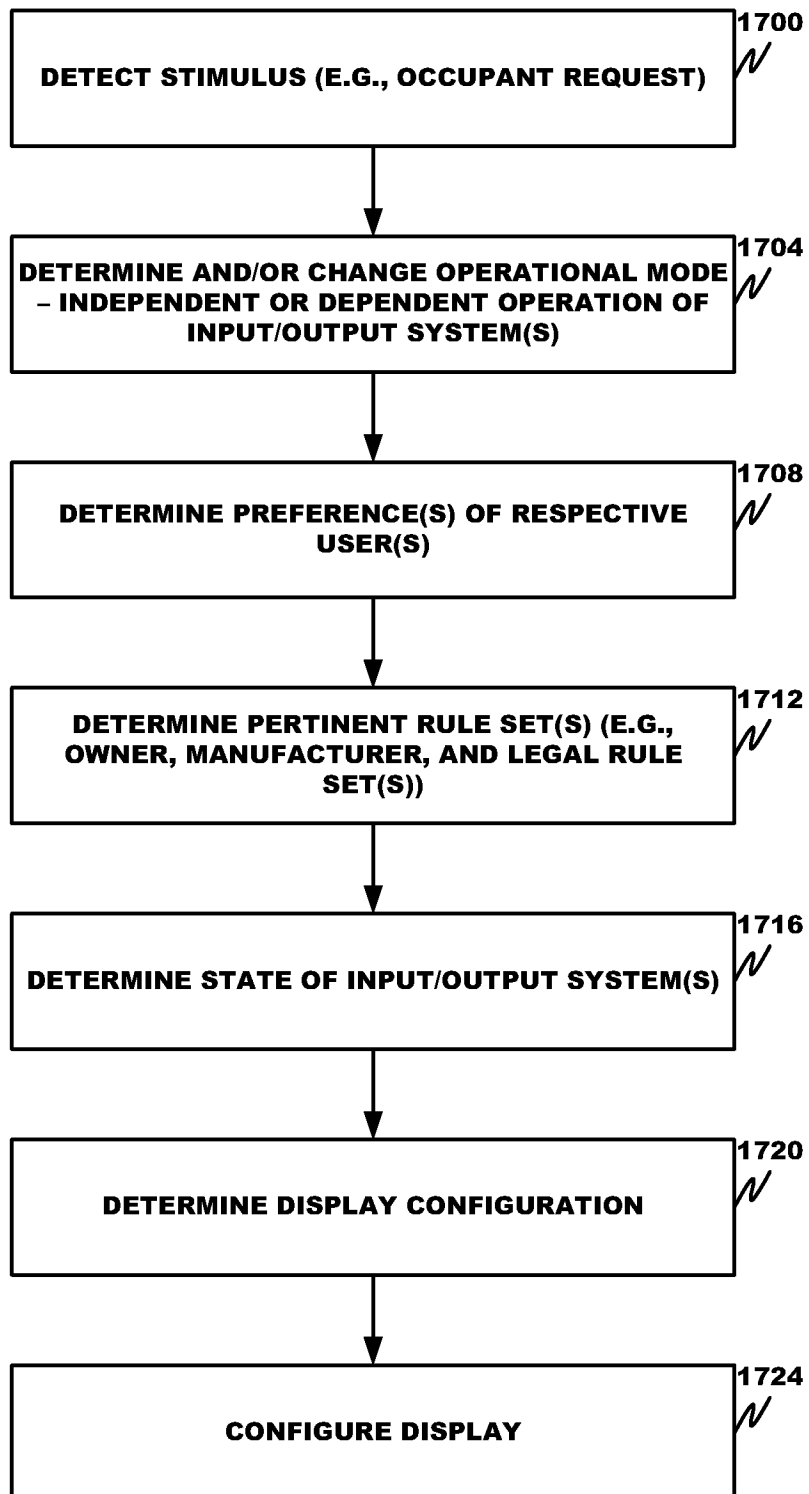


FIG. 17

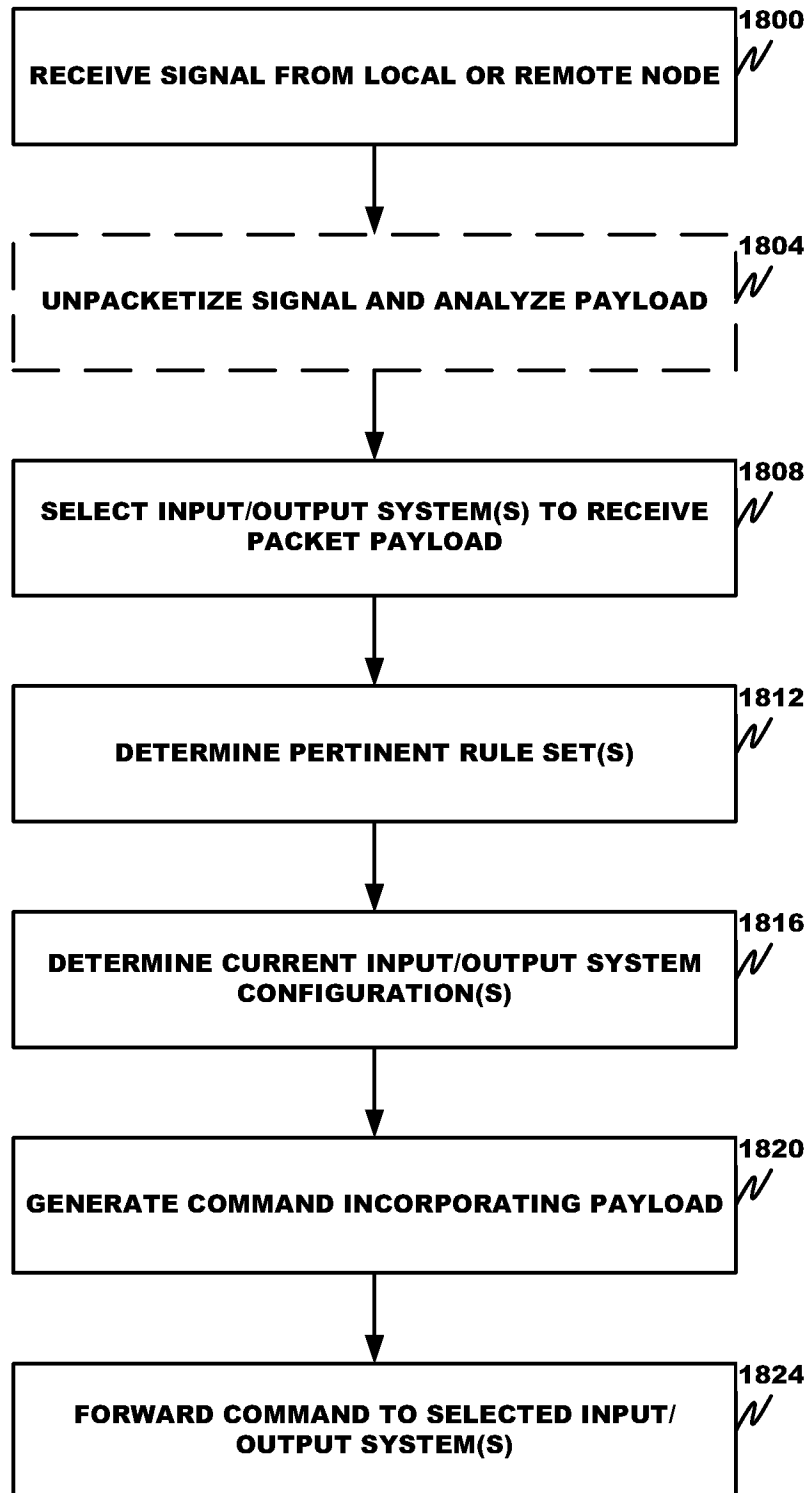


FIG. 18

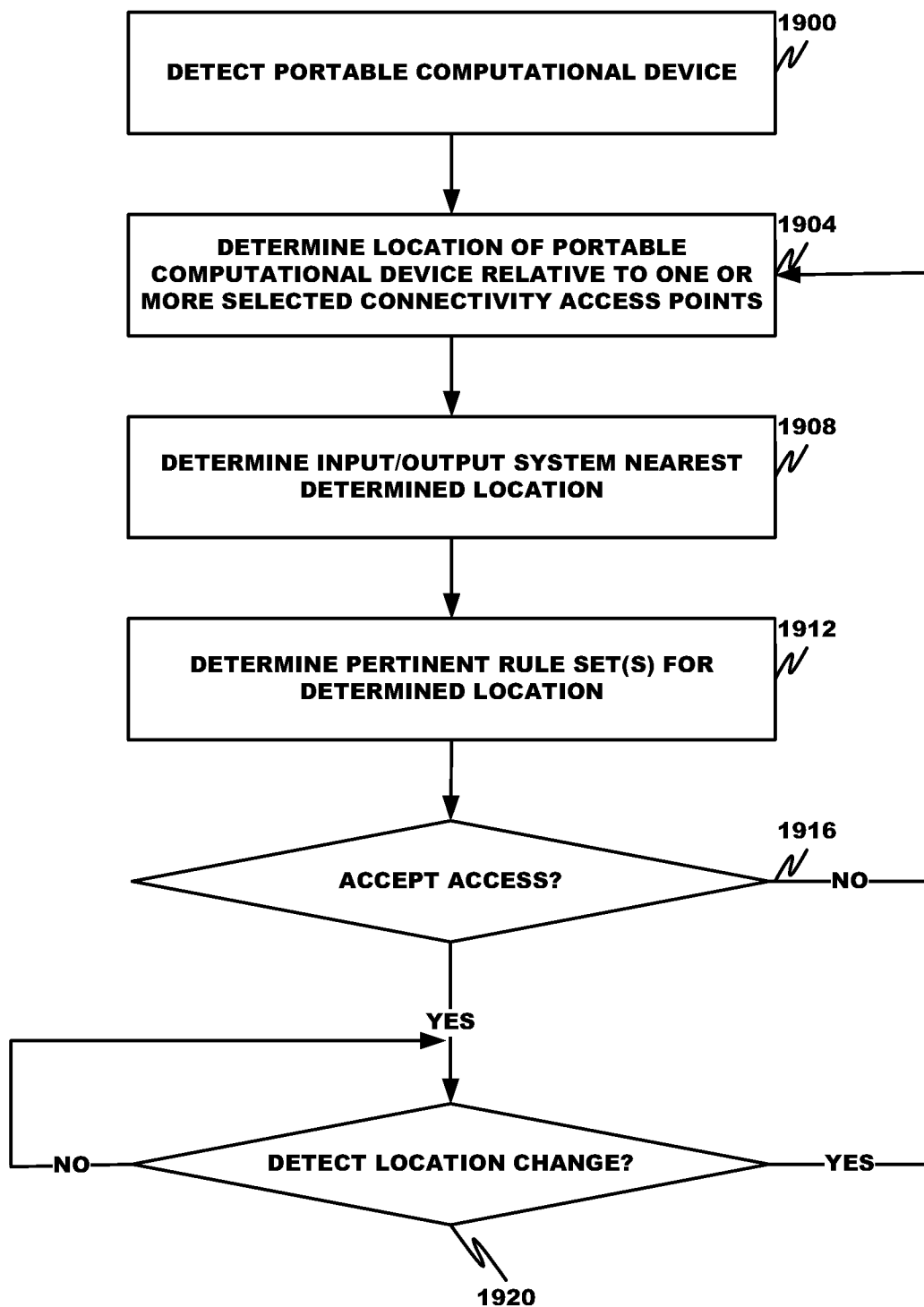
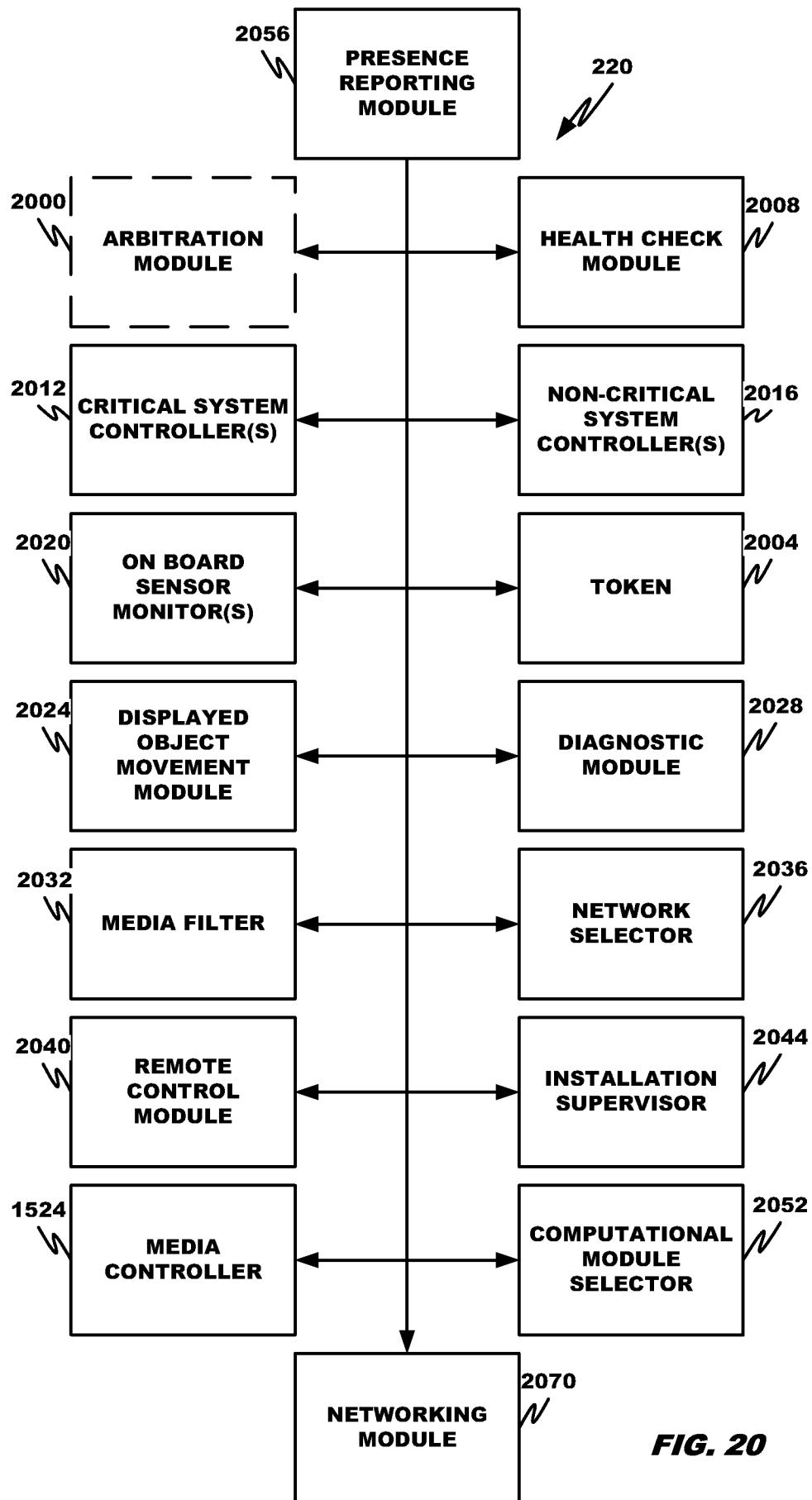


FIG. 19



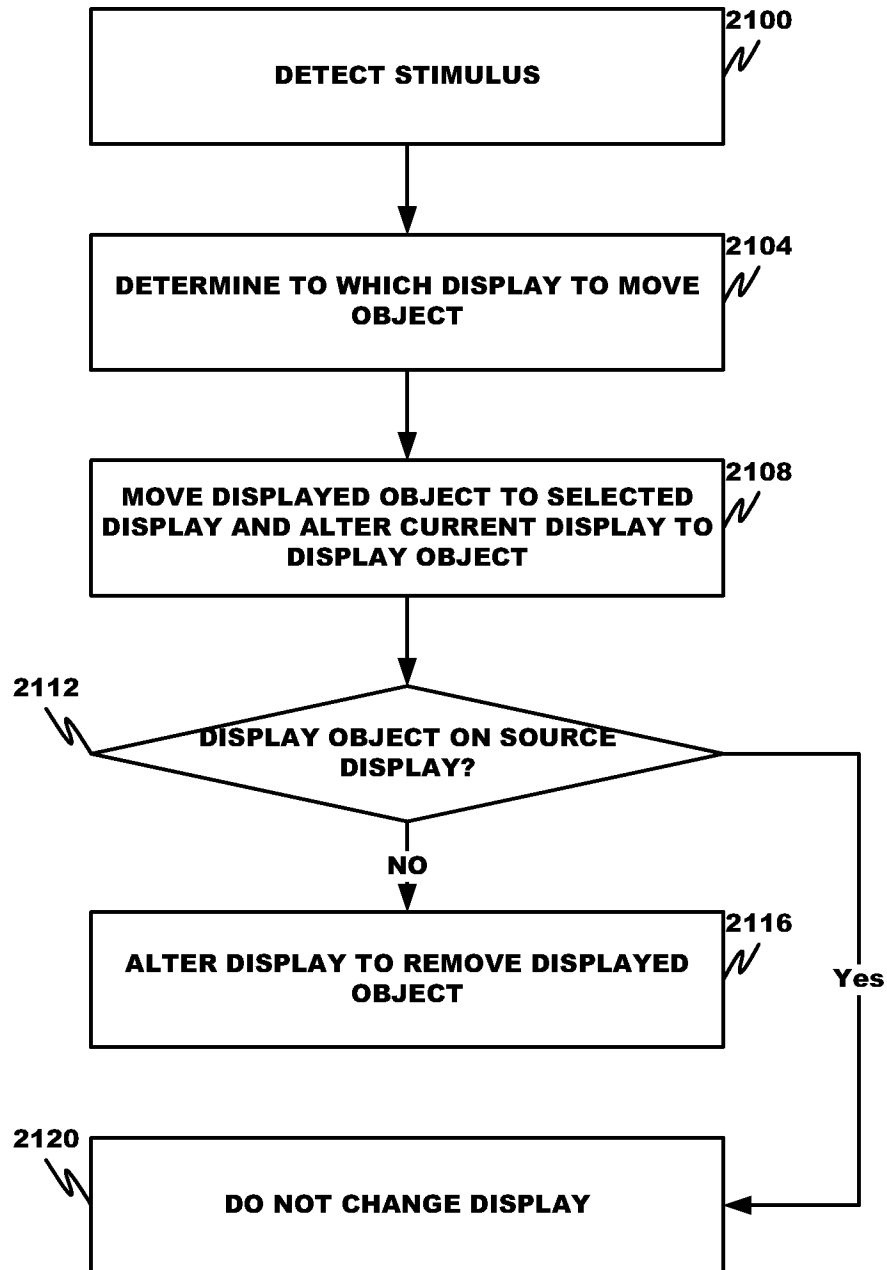


FIG. 21

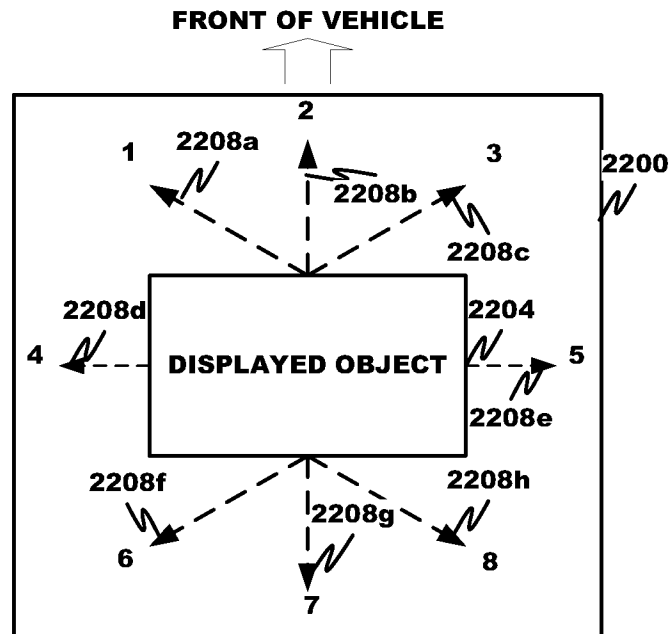


FIG. 22A

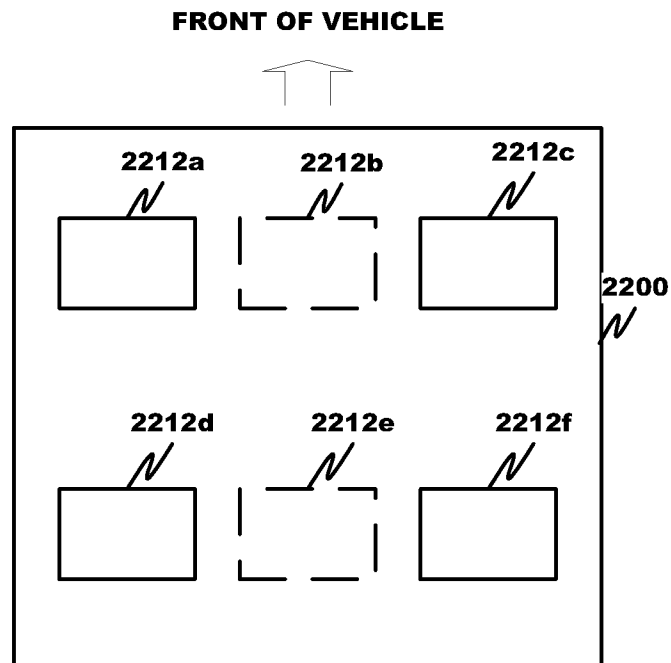
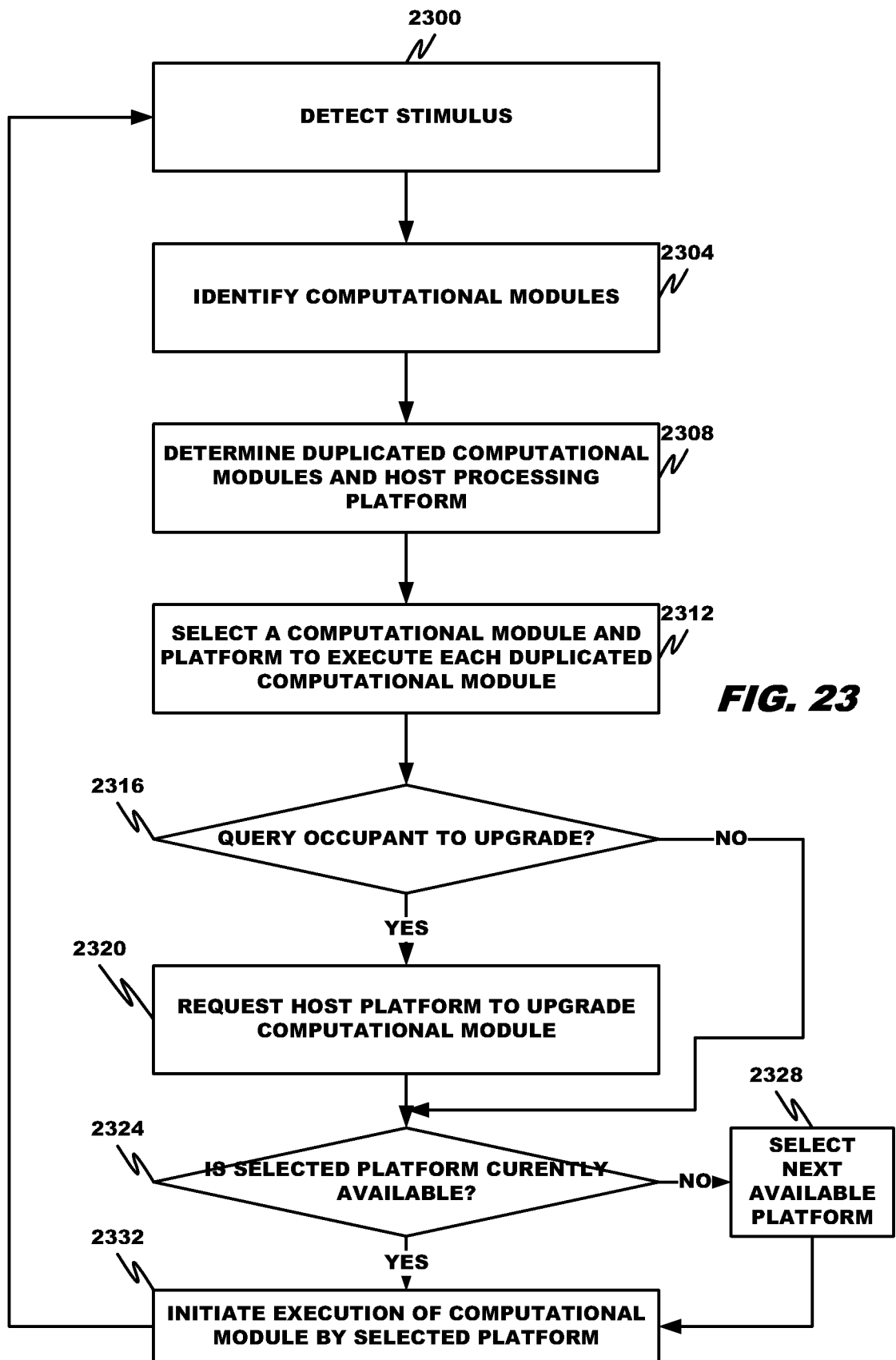


FIG. 22B



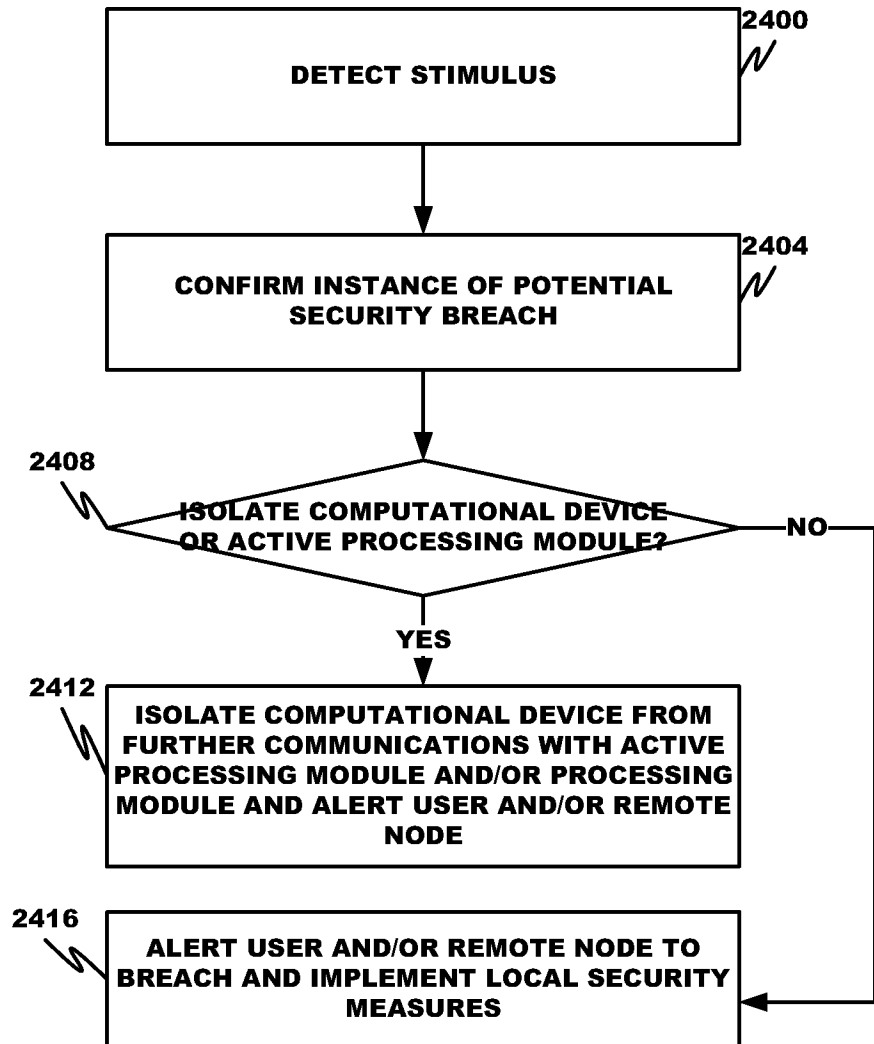


FIG. 24

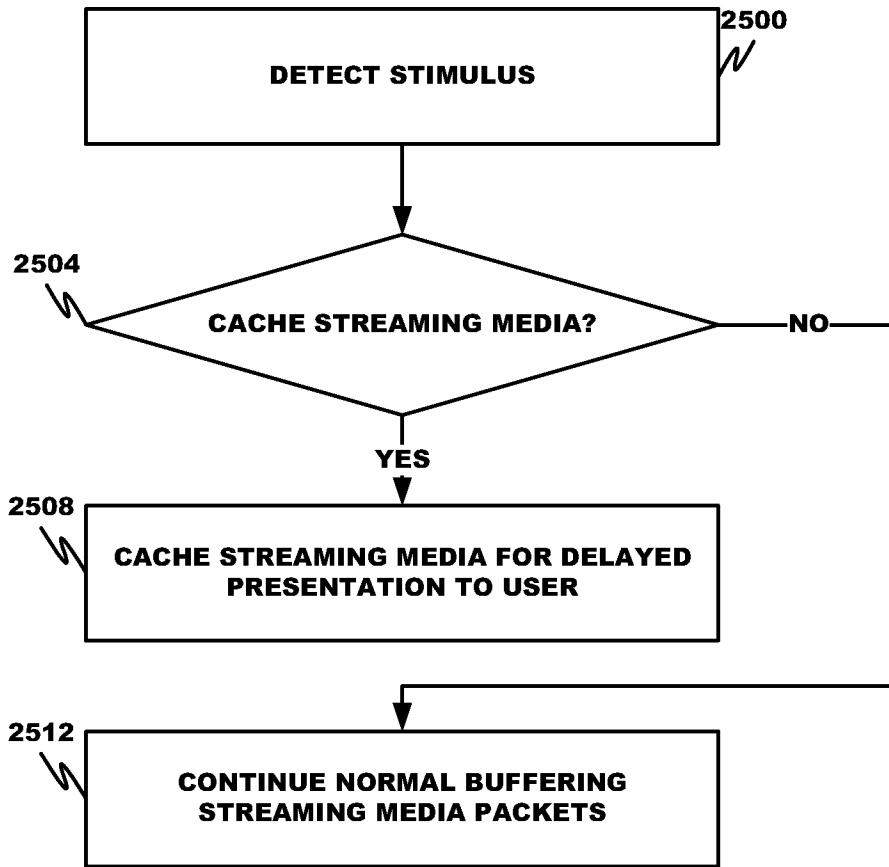


FIG. 25

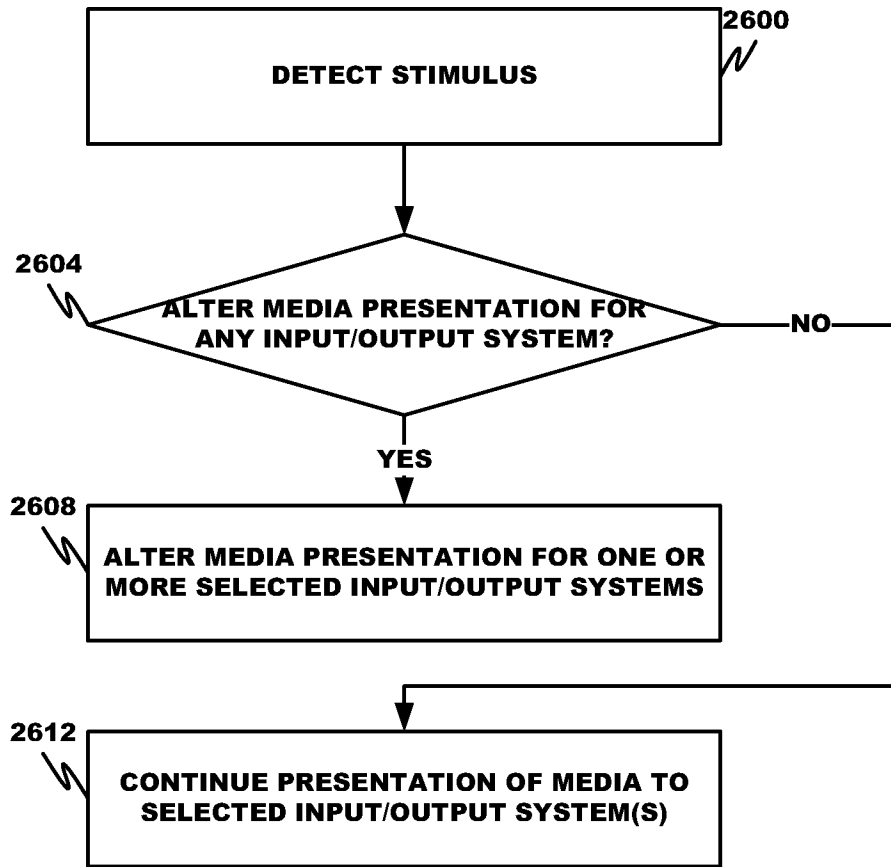


FIG. 26

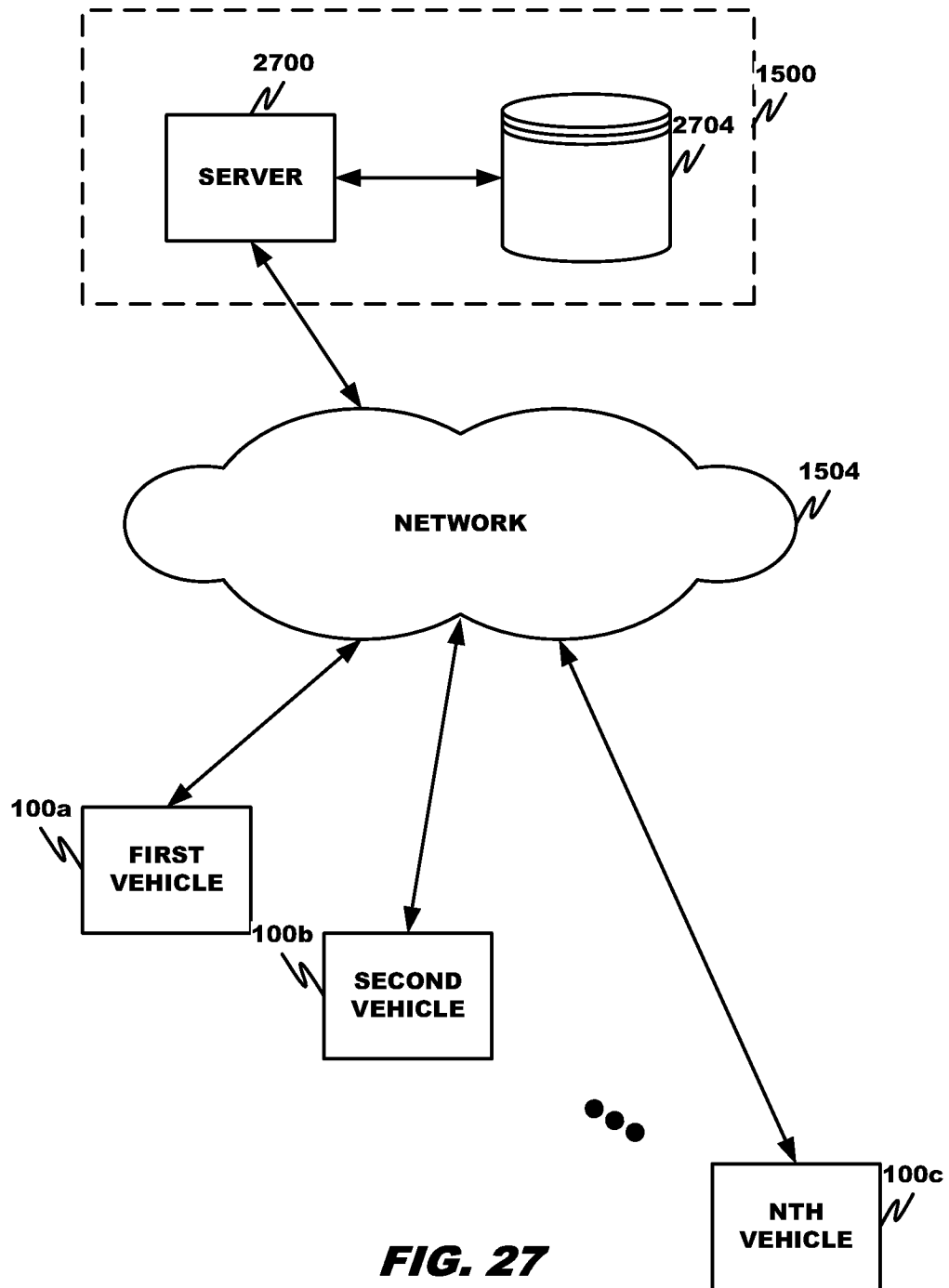


FIG. 27

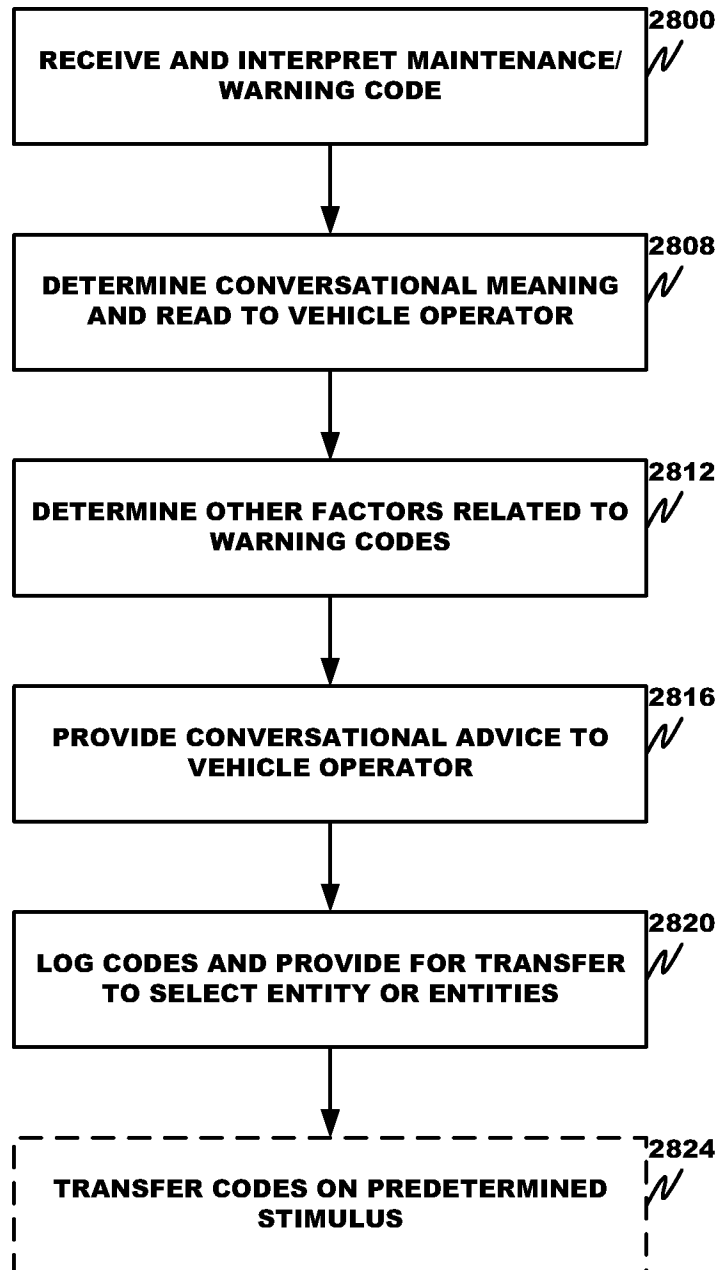


FIG. 28

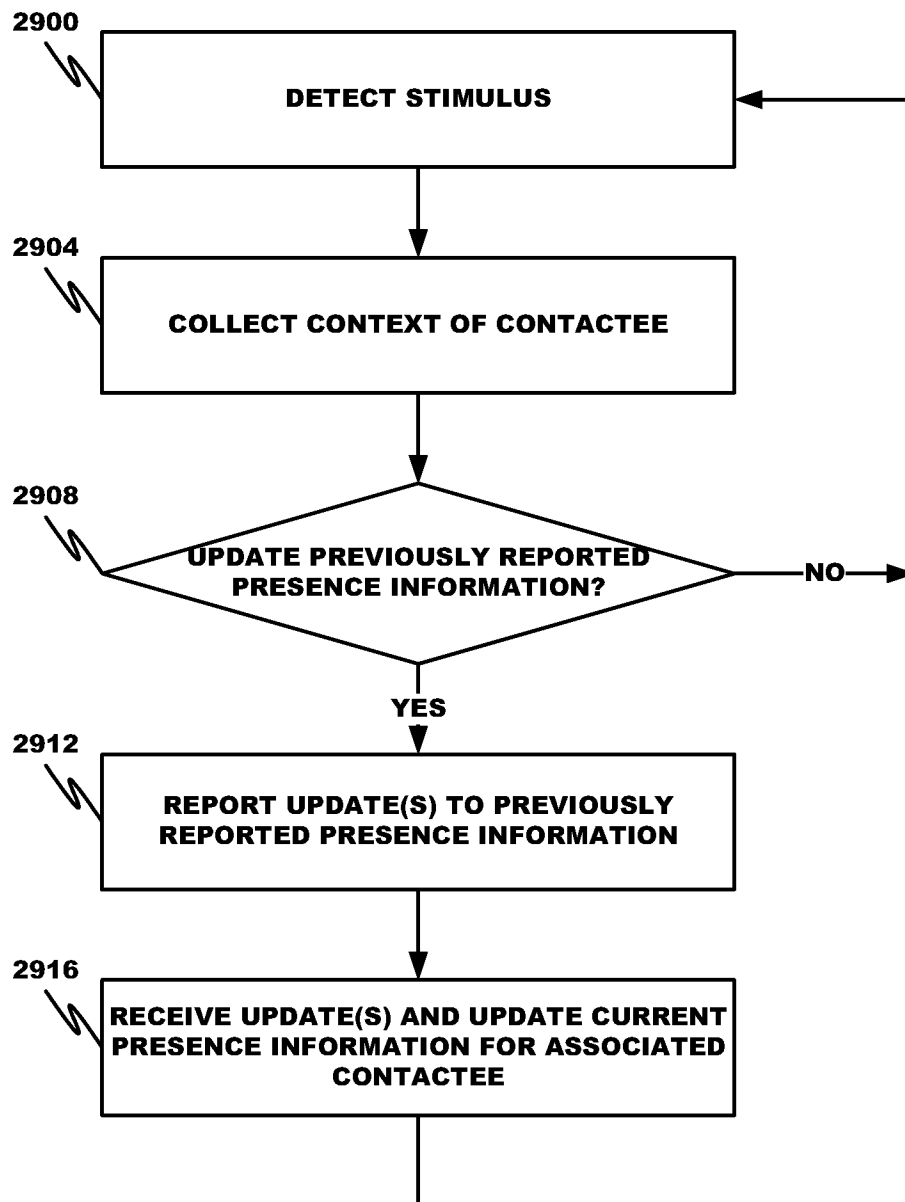


FIG. 29

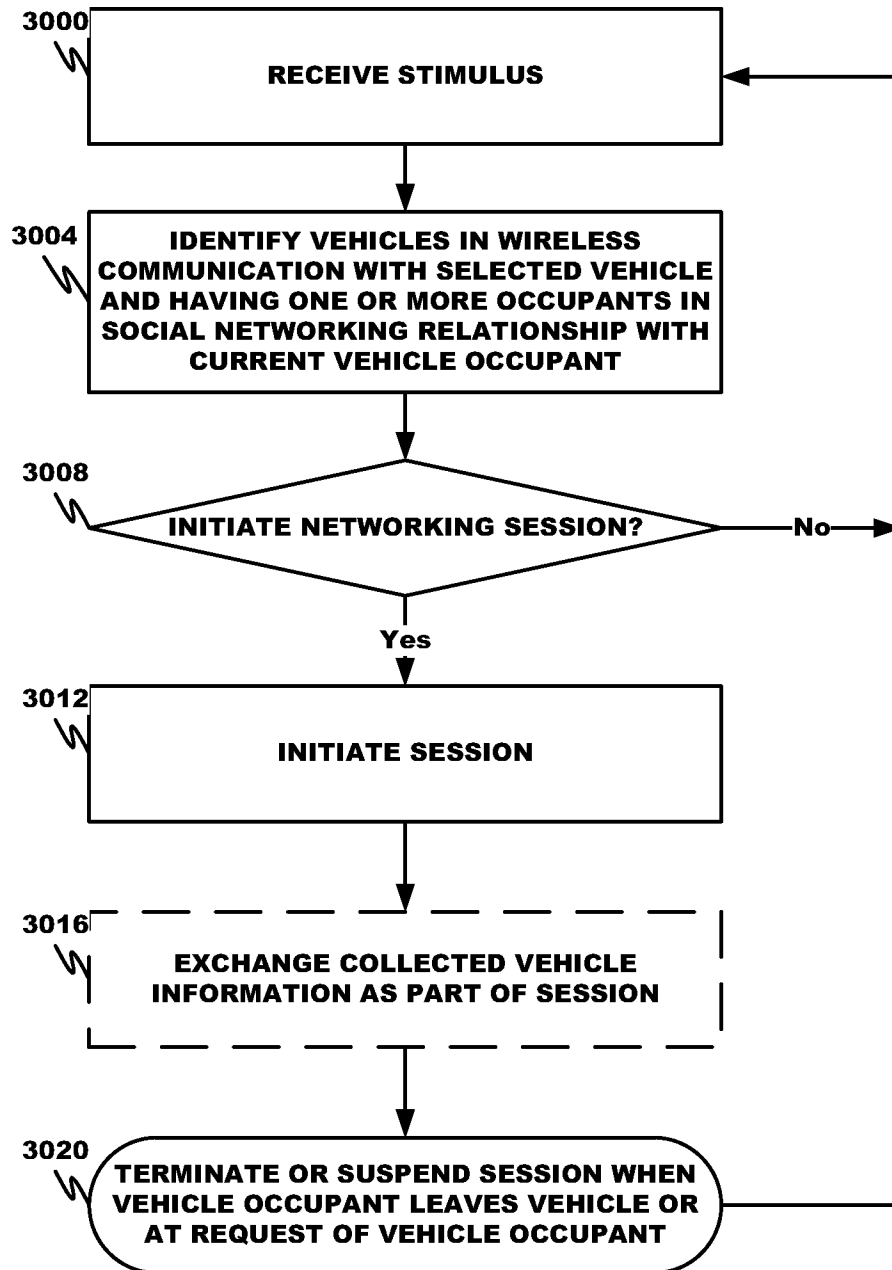


FIG. 30

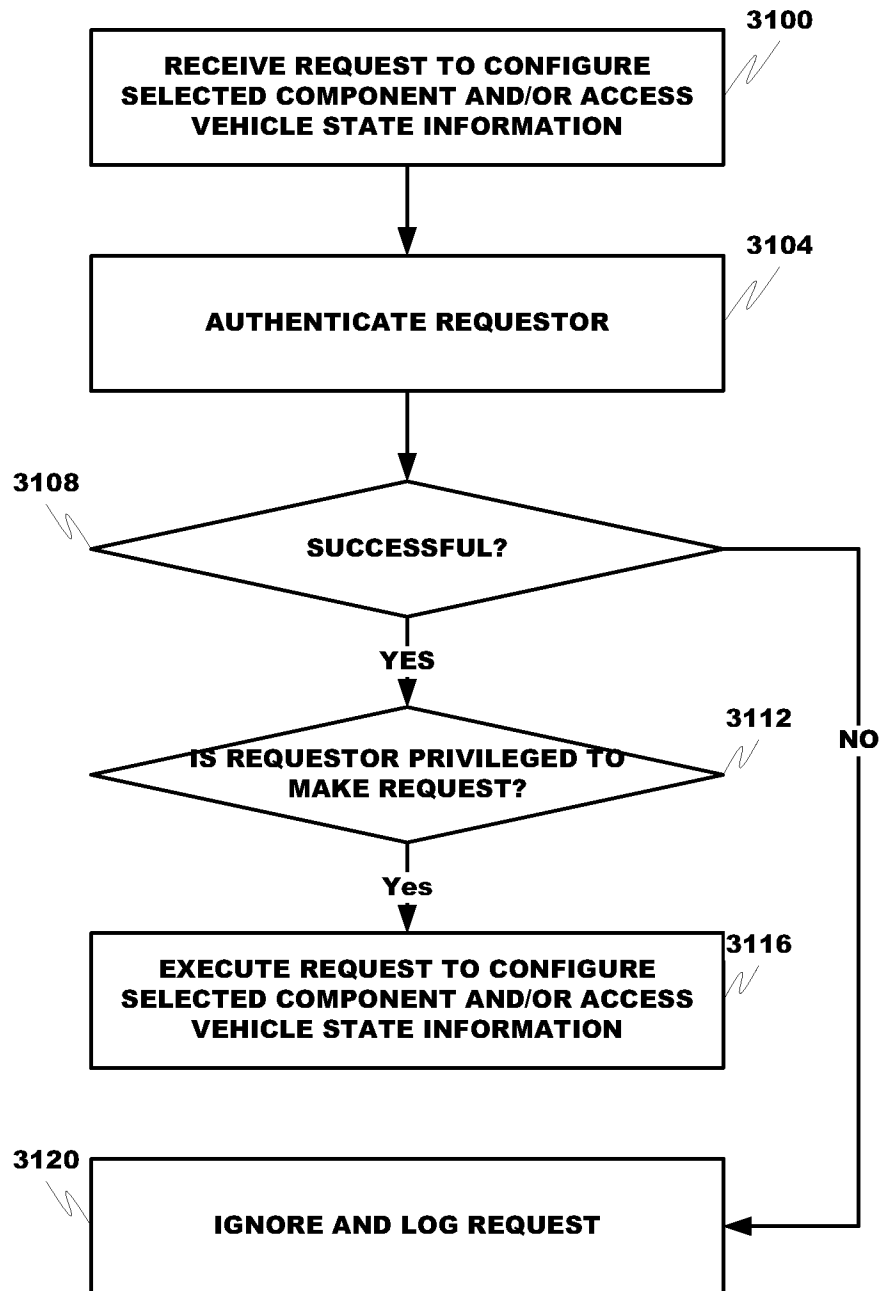


FIG. 31

EXHIBIT “A”

Project Octopus – the IP Connected Car Functional Specification

1 Why Octopus

Project Octopus was initiated by a request to design a new “infotainment” system for the automotive industry. The infotainment solutions that are currently being presented are just “add-ons” to an already complicated electronics environment present in vehicles.

As the research for this infotainment system was being done, it was realized that the environment could be simplified if one stepped back and looked at the car as a distributed system, interconnected by a high speed network.

The name “Project Octopus” (aka “Octopus”) comes from the fact that the distributed system has tentacles everywhere in the vehicle, as illustrated in Figure 1.

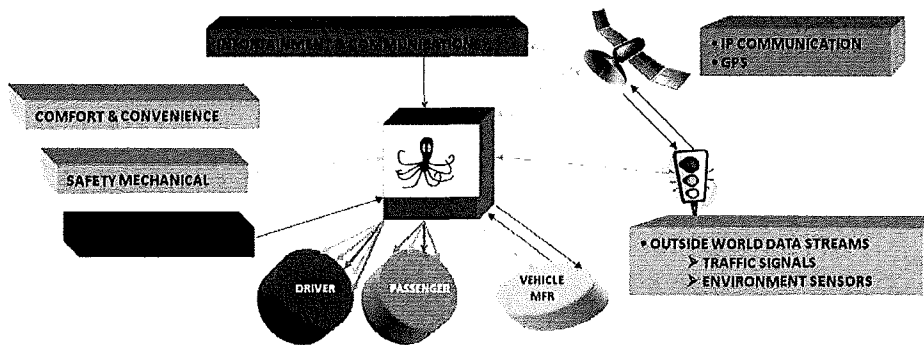


Figure 1- Octopus Data Stream Management

2 Overview

Project Octopus, the IP Connected Car, is designed to take advantage of the pervasiveness of IP, as well as the volume of hardware components that are made for IP based distributed systems, including the dominant transport – Ethernet.

Project Octopus has been developed as a modular distributed system architecture that is meant to be upgraded and extended over time. Octopus can be expanded over time without changing the basic processing architecture. In fact, since the various subsystems communicate with one another by protocol based messages, there is no requirement that all the programs be written in any specific language or

Project Octopus – the IP Connected Car Functional Specification

run on any specific operating system. This allows developers to use the most appropriate run time environment for the subsystem being developed. In other words if a Real Time Operating System (“RTOS”) is required because of the timing constraints of the run time environment (i.e. real time control of a function), a subsystem could be developed using any RTOS, without constraining the run time environment of less demanding systems (e.g. console subsystem).

Octopus is positioned to take advantage of the development of new families of sensors and control elements, which can be readily integrated using the new generations of Single Twisted Pair Ethernet components. Since Ethernet components are pervasive in all types of communications their cost is continually driven down, making Ethernet an attractive way to implement new sensor and control systems. With the advent of new families of low power/low cost processing elements, it becomes possible to distribute intelligence throughout the vehicle¹.

Project Octopus is built upon the premise that all communications with the car are IP based. An additional premise is that the IP connection is an “information pipe” that is supplied through the vehicle manufacturer, allowing services to be provided and data to be collected for the vehicle².

3 Flex Adaptive Automotive Architecture

Octopus meets the requirements for the Next Generation Media System. This system supports “smart device” input, WiFi access, streaming of media (video content as well as Satellite media), as well as the usual input of AV via removable storage media (USB, DVD, etc.). Octopus includes an “always on” IP connection and enforces secure input of data with a firewall³.

All the components of Octopus are connected via GigaEthernet, using Ethernet switch technology. This allows components to be developed, enhanced, or replaced easily requiring only a common definition of protocols to allow system integration.

¹ Siemens – Pictures of the Future – Fall 2012

² Daimler – The Telematics Future of Mercedes-Benz: @yourCommand – 26 October 2011

³ Potentially a revenue source with a subscription to upgrade virus definitions, etc.

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

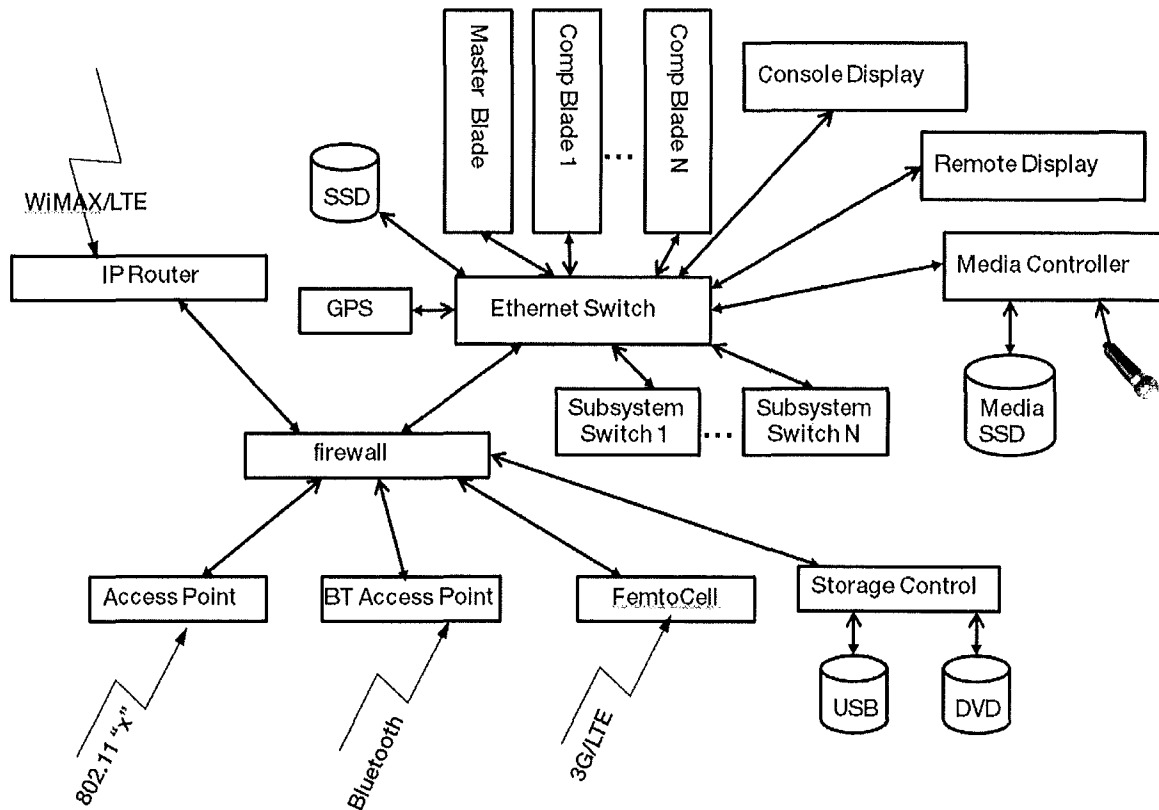


Figure 2 – Octopus Functional System Diagram

However, Octopus goes further in that it begins the evolution to the NextGen Ethernet based vehicle. The Flex Adaptive Automotive Architecture (“FlexA3”) implements vehicle systems as an interconnected set of subsystems.

At the heart of a FlexA3 implementation is the FlexA3 crate, with multiple slot system bus (FlexZIF System Bus) that contains 3 or more FlexA3 “blades”. The minimum system will have 3 FlexA3 blades:

- FlexA3 Master Blade
- Flex A3 Firewall Blade
- FlexA3 Multimedia Controller Blade

Being modular, Octopus can be upgraded by adding one or more application execution blades. Additionally, the FlexA3 system allows different options to be

Project Octopus – the IP Connected Car Functional Specification

added in a modular fashion. For example, a NAV subsystem would require the addition of

- GPS receiver/antenna and computational unit
- NAV computation application executing on an application processor
- NAV UI executing on Multimedia Controller blade.
- NAV display on console
- Heads Up Display (optional)

Depending upon the system loading, this might mean just adding the GPS unit and connecting it to the Ethernet backbone, while loading software onto the appropriate blades. For more heavily loaded systems, a blade upgrade might be required.

3.1 Functional Structure

Octopus functional units all have a similar architecture that includes:

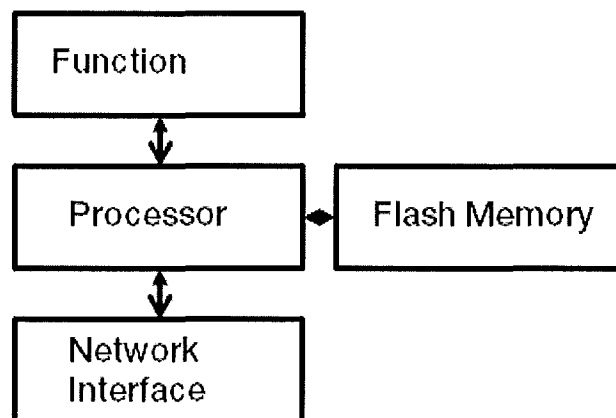


Figure 3 - Octopus Functional Unit Structure

The “function” can be a 802.11 Wifi interface, Bluetooth radio, Cellphone radio, storage unit, or GPS. The entire capability is implemented using a low power, relatively simple processor which only needs to support the capability and response time required to implement the function. The output of the functional unit is an IP message framed into an Ethernet packet. The software that is part of the functional can be upgraded via the Ethernet interface.

In Figure 3 the “functions” may be software or a combination of software and hardware that are required to implement a particular capability.

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

All components of Octopus self test on powerup, with a status report being delivered to the manufacturer⁴.

The Octopus functional structure allows the system to be extended to upgrading existing data and control systems without requiring a simultaneous upgrade of all vehicle systems.

In the vehicle of the future, it is entirely possible to envision sensor and control systems that are distributed throughout the vehicle, placing them as close to the operational component being monitored or controlled¹. While this is the desired end-state, the current methodology would be to change over the entire control system on a given model year design.

Octopus, with its functional structure architecture allows an incremental approach to be taken. For instance, the current Car Area Network (CAN) assumes that the sensors are connected to a relatively slow, serial bus that brings all control to one or more control computational units. The CAN control system can be integrated into an Octopus implementation by terminating the CAN bus(es) in one or more Ethernet bus controllers.

The software can then be written as if it were talking to discrete Ethernet based sensors or controllers, with the translation to the CAN protocol being made at the CAN Ethernet Controller Subsystem. Over time, as the sensors/controllers are replaced with Ethernet based units, the control software running on the FlexA3 blades stays the same, communicating directly with the sensors/controllers.

This concept can be extended further to allow for optional upgrades to occur without changing the basic structure of the system (Section 13).

4 FlexA3 Computational Subsystem

The FlexA3 system is based on a collection of blade processors that are housed in a “crate”. The “crate” has a PC-style backplane connector, as well as on-backplane Ethernet(s) that allow FlexA3 blades to communicate with one another using Ethernet.

4.1 FlexA3 Backplane

The Octopus Functional System Diagram (Figure 2) can be re-drawn to in a configuration more closely resembling the actual FlexA3 Crate with a backplane

⁴ Requires an interconnect connection and a service
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

installed. As indicated in Figure 4, the backplane must be capable of keeping the “red zone” and “green zone” separate.

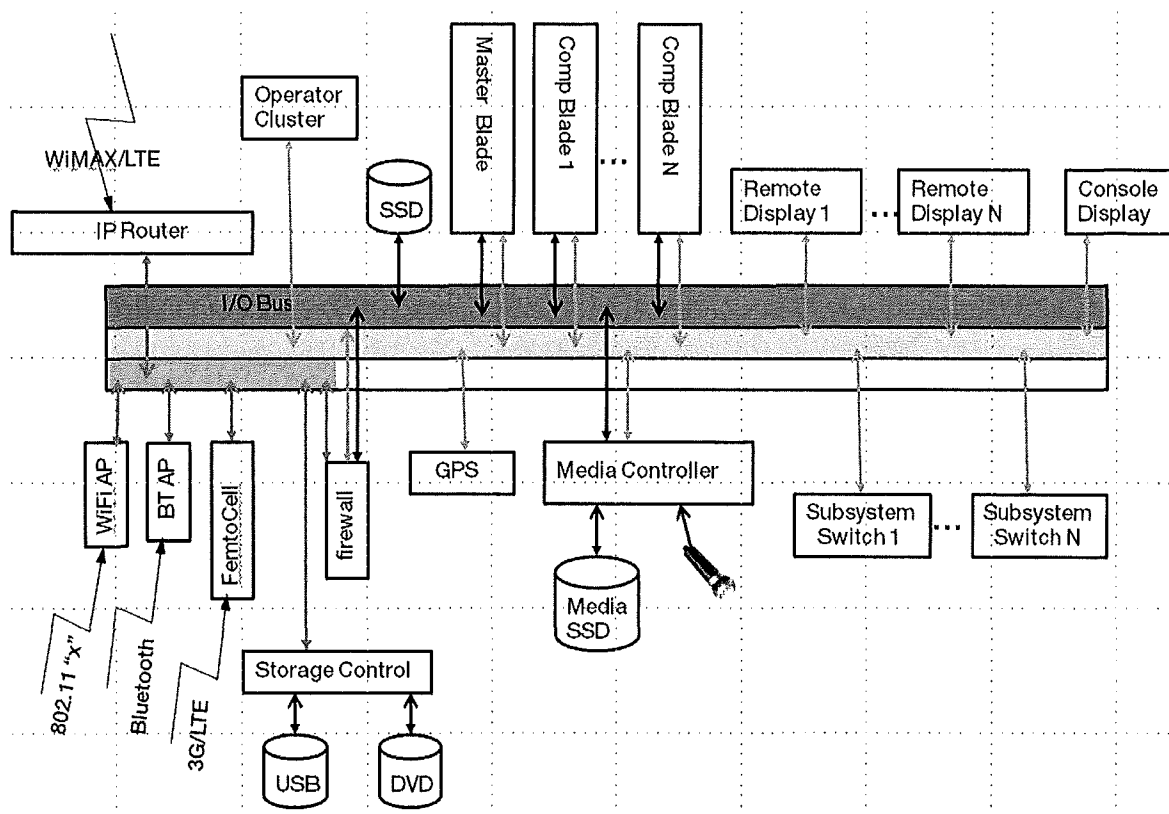


Figure 4 Ethernet Security Zones

The backplane must further be able to have individual external connectors that are connected to the Ethernet switch that is part of the Firewall. Only trusted components either provided or approved by the manufacturer after testing can be attached to the “green zone”, which by definition is the “trusted Ethernet”.

While the diagram indicates that there are 5 external connections to the Firewall switch, provision should be made for 8 ports⁵. It is expected that the external port connections will be made through a manufacturer configurable modular connector panel.

Additional connectors will be required to connect such elements as the console display, remote display and GPS receiver/antenna, as shown in Figure 4

⁵ There is some indication that the industry is using an “odd number” of ports on Ethernet switch chips. The requirement can be relaxed to at least 5 ports, preferably with one or more spare ports.
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

There are actually two separate Ethernet backbones on the backplane. The first (red zone) only needs to go from the modular connector panel to the input side of the backplane connector of the Firewall switch. The second Ethernet, goes from the output side of the Firewall, and generally defines the Trusted Ethernet (green zone). The Ethernet on the backplane essentially implements an Ethernet switch for the entire system, defining the Ethernet backbone of the vehicle. All other modules (i.e. “blades”) connect to a standard backplane bus AND the Trusted Ethernet. Some number of “switch ports” need to be reserved to connect to the Output Modular Connector Panel in order to distribute the Ethernet throughout the vehicle (i.e. connecting the displays and other sensors/controllers). The two Ethernets (untrusted and trusted) are NOT connected, which also implies that the connector geometry for the Firewall is different than all other blades that are part of the FlexA3 system.

The FlexA3 backplane also has a normal I/O backplane that provides power and I/O functions for the computational elements of the system.

4.2 FlexA3 Master Blade

The FlexA3 master blade is a designation for the first computational blade in the system. The Master Blade is identical to all the other computational blades in the system, save for some scheduling and control software⁶. The Master Blade instantiates the “Service Manager” that is a distributed service that inventories hardware and software capabilities that are available on the system. Requests to the Service Manager allow various applications to access distributed services or automatically disable features that are not supported by the system.

The Master Blade coordinates the “health check” for the entire system and is responsible for ensuring that a “keep alive” message is sent to the “operator warning” display circuitry⁷. The Master Blade “startup health check” is also responsible for determining what the minimum set of system capabilities must be operational before sending the reset message used to clear the Operator Warning circuitry within the allocated timeframe.

The Master Blade also executes the “start application” request, when a new application wishes to run. The Master Blade checks the application resource requirement entries in the “application resource table” and assigns the application to a Computational Blade that has the most applicable resources. If an application

⁶ There are only three types of blades in the system: Computational, Multimedia Controller, and Firewall

⁷ This ensures that the operator warning message area knows that the system is really working and not just stalled

Project Octopus – the IP Connected Car Functional Specification

has specific requirements for execution (e.g. multimedia infotainment app) then the application is assigned to and locked to a specific blade (i.e. to the Multimedia Controller).

In the event that the FlexA3 system is configured for high availability⁸, the Master Blade will create an HA “set” with the required number of computational blades⁹. A table is created on the FlexA3 SSD that controls the priority of which blades are capable of becoming Master Blades.

If an application that is designated as “HA capable” is started, shadow copies are created on every member of the HA “set”, but they do not execute. Applications that are HA capable must write all variables to a file created at application initiation that resides on the FlexA3 SSD. The variable write process uses the Two Phase Commit Class driver of the FlexA3 SSD.

Additionally, once a HA capable application is initiated, it wakes up the HA “keep alive” service. The “keep alive” service interrogates its “partners” on every member of the HA “set” at a pre-defined interval. If the “keep alive” times out on a specific Blade, the “keep alive” service determines which Blade has failed.

Once the keep alive service is started, a “keep alive service table” is created in every member of the HA “set”. The table contains information about the application, members of the HA set, and pointers to the variable file for the application on the SSD. A second request to start the “keep alive” service simply causes new entries to be made in the “keep alive” service table”.

If the “keep alive” service detects a failure, the HA capable applications are started on another running blade server by the Master Blade Application Control Service. The Master Blade Application Control Service is capable of redistributing applications to blades and/or stopping applications in order to achieve maximum performance for the entire system. Once a blade has failed the Master Application Control Service logs a failure onto the support area of the FlexA3 SSD (module ID, VIN, GPS coordinates, environmental variables).

If the blade that fails is the Master Blade, then the Master Blade Reconfiguration program is started. The Master Blade Reconfiguration process causes the blade designated as “alternate” to start up all vehicle control programs and re-distributes other applications across the remaining blades. The Master Blade Reconfiguration

⁸ High Availability does NOT mean non-stop computing, lock-step computing, or voting

⁹ The HA “set” is determined from configuration parameters on startup. The “set” is defined by the manufacturer. The HA “set” does not have to include all the computational blades in the system.

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

program is able to stop low priority applications from running in the event that resources become constrained.

The Reconfiguration Program marks the original Master Blade as “failed”. The Reconfiguration program interrogates the “service manager” to see if there is a constant IP connection and Manufacturer Support Service available:

- Manufacturer Support Service = available, then failure message with module ID, GPS coordinates, VIN are sent to the Manufacturer Support Center via an IP message. Failed Component message (i.e. check engine light) is displayed in Operator Warning messaging area, Heads Up Display (if available) and Console
- Manufacturer Support Service = NOT available, then failure message with module ID, GPS coordinates, Vin are logged into support area of FlexA3 SSD. Failed Component message (i.e. check engine light) is displayed in Operator Warning messaging area, Heads Up Display (if available) and Console

4.3 FlexA3 Storage System

Octopus uses a SSD (>100GB capacity) as the main storage for the FlexA3 system.

Access to the SSD is via class drivers that implement both standard I/O, as well as Two Phase Commit I/O.

The SSD contains separate volumes that support:

- Application storage
- Application Variable storage (for HA)
- Configuration information (for HA)

The SSD Blade contains its own microcontrollers to handle I/O requests from Computational Blades and specialized controllers (e.g. GPS). The SSD Blade processes normal mass storage I/O requests and also implements the Two Phase Commit I/O channel.

Communications from the I/O class drivers to the SSD controller are formatted messages, allowing different operating environments to gain access to the SSD as necessary¹⁰. These messages can either be bus based or IP based.

Multimedia Storage is handled by the SSD associated with the Multimedia Controller.

¹⁰ This allows different operating systems to be used on different components that need access to the SSD.
project octopus - functional spec - v002a - 041413.docx

5 Project Octopus – Component Description

5.1 Display Subsystem

The display subsystem includes the video controller and frame buffer for the display. The data is received as a stream and unpacked by the processor and loaded into the display buffer. The processor and video controller deal with optimizing the display based on the characteristics of the screen. The screen may be output only OR include a touch screen interface.

Physically, the display subsystem can either have speakers or multiple headset connectors.

On power up, the display subsystem initializes the frame buffer and creates the entries for the service manager. These entries include

- Screen size
- Touch screen input
- Voice control input
- Refresh rate
- Resolution in pixels
- Size of the frame buffer
- Horizontal refresh rate
- Hardware/software revision level

The media controller software uses the service manager tables in the device controller to determine how to format packets for the display controller.

The display controller responds to:

1. Requests for services messages
2. Display buffer fill commands

5.2 GPS Subsystem

The GPS subsystem is built with a conventional GPS chip for receiving satellite signals. The GPS subsystem converts the GPS signals into latitude and longitude values for use by the Navigation Subsystem. Additionally, the GPS subsystem records the latitude/longitude and time stamp in a buffer every 10 seconds. This

Project Octopus – the IP Connected Car Functional Specification

information can be used by public safety officials to reconstruct vehicle operation prior to an accident. A minimum of 1 hour of data should be stored. The buffer can be overwritten as necessary after the mandatory retention period.

On vehicle “power on”, whether or not the engine has started, the GPS system will begin to synchronize with satellites to enable the T_0 position to be determined. This reduces the “startup” time that is typical of GPS systems.

The initial state of the GPS is to have the latitude/longitude/timestamp memory locations to be cleared. This allows the unit to respond to information requests, but indicates to the requesting program or subsystem that the unit has not yet “synced” with the satellite system. In the event that the GPS cannot determine the position within a specified timeframe, the unit continues the attempt to determine the location.

The GPS subsystem is implemented separately from the NAV subsystem to allow the lat/lon data to be used with the “vehicle information scan” that is accessed by the manufacturer as part of the “customer care” system.

The GPS subsystem is a separate unit that is connected to the “green zone” Ethernet backbone of the vehicle.

6 Console Subsystem

The console provides the control for the audio entertainment systems, “radio” entertainment systems, navigation systems, multimedia entertainment screens and (optionally) the vehicle comfort and convenience systems¹¹. The console function is implemented using the multimedia subsystem and a touch enabled display subsystem, with information being supplied via other Ethernet connected subsystems as necessary.

The console does NOT support multimedia entertainment (i.e. video). All multimedia entertainment is displayed on remote display subsystems that are dedicated to a specific seating position.

¹¹ Only if the vehicle is equipped with a FlexA3 computational system
project octopus - functional spec - v002a - 041413.docx
© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

6.1 Console Menu

The menu is displayed on vehicle “power on”, whether or not the engine is running. The console remains active as long as the “key” is in the “ignition”¹².

The console has a “button” that activates the “configuration application”, allowing the user to personalize the console display. When the configuration application starts up, it determines what capabilities are available on the vehicle through the service manager. The “configuration application” displays the available options. The operator can select the options to display AND their positions on the screen. Once the selection has been completed, the operator selects “done” and the menus are saved.

How the file is saved depends on the subsystems available on the vehicle:

1. For a vehicle with a FlexA3 subsystem, the file will be saved on the FlexA3 SSD, along with other personalization data.
2. For a vehicle without a FlexA3 subsystem, the file is saved on the multimedia subsystem SSD.

The console “configuration application” determines the location of the personalization file by interrogating the service manager for the multimedia subsystem.

In either case, when all the information has been chosen and arranged on the console display, the user chooses “done” from the menu and is asked for a distinctive name with which to save the information. For a new user, a new file is created on the storage unit. If the user name exists, the user is asked whether to overwrite the file or create a new name.

7 Navigation Subsystem

The Navigation Subsystem (“NAV”) is implemented using the GPS receiver subsystem and map information that is stored on the multimedia subsystem SSD.

The NAV system executes as an application on one of the FlexA3 blades, sending a request to the GPS subsystem and receives the current location of the vehicle, which it then uses to plot the location on the console display subsystem and/or the Heads Up Display (if present) .

¹² The “key” may be a RFID chip enabled device that is in close proximity to a RFID transceiver.
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

The NAV subsystem interrogates the service manager to determine whether the Heads Up Display is present and then generates data streams for the console and the Heads Up Display (if present).

On initial configuration, the console is used to determine whether to load the map data from external removable storage or from the owner's Cloud Storage account. In either case, the active map data is loaded onto the multimedia subsystem SSD. T

The NAV system is controlled by input from the Multimedia Subsystem, using the console, handheld device/tablet, or voice input. The user interface to the NAV system executes on the Multimedia Subsystem, where commands are translated into messages that are transferred via Ethernet to the NAV subsystem. For console or handheld device/tablet input, the NAV system is selected from a menu that is displayed¹³ on the device. The NAV UI then continues on those devices. If a voice command is issued, then the commands continue with voice input. Input devices cannot be mixed, with a different choice requiring a cancellation of the current operation.

Stored routes, favorite destinations or points-of-interest are stored on the Multimedia Subsystem SSD. This information can be “backed up” to the owner's Cloud Storage account using the console or handheld device/tablet menus.

Similarly, the turn-by-turn instructions are converted into messages that are sent to the Multimedia Subsystem and then synthesized into “spoken commands” using the speech synthesis hardware.

8 Firewall

The Firewall is always part of the Octopus system, with all communications to external data sources being transmitted through the firewall. This includes all WiFi, Bluetooth, Cellular and removable storage. This is illustrated in Figure 5, which also illustrates the two versions available for the Firewall.

- Dash1 – the basic firewall functions (solid blocks only)
- Dash 2 – the advanced firewall (solid blocks plus dashed blocks)

The external inputs include access points for WiFi, Bluetooth and Cellular that are described below.

¹³ Handheld device/tablet must have delegated capability to allow input via Wifi
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

The storage controller includes ports for connecting USB enabled devices and a SATA based DVD reader for entertainment systems. The storage controller contains a processor/memory/Ethernet transceiver (e.g. Figure 3) for accepting requests from the multimedia controller to access files on either device. The Storage Controller software implements the file system primitives necessary to access the devices, including the hardware abstraction for the storage devices and the actual physical drivers for the device. To generalize the approach, the storage controller implements a Network File System. This allows the storage controller to be used in systems that may or may not use homogeneous operating systems across all components.

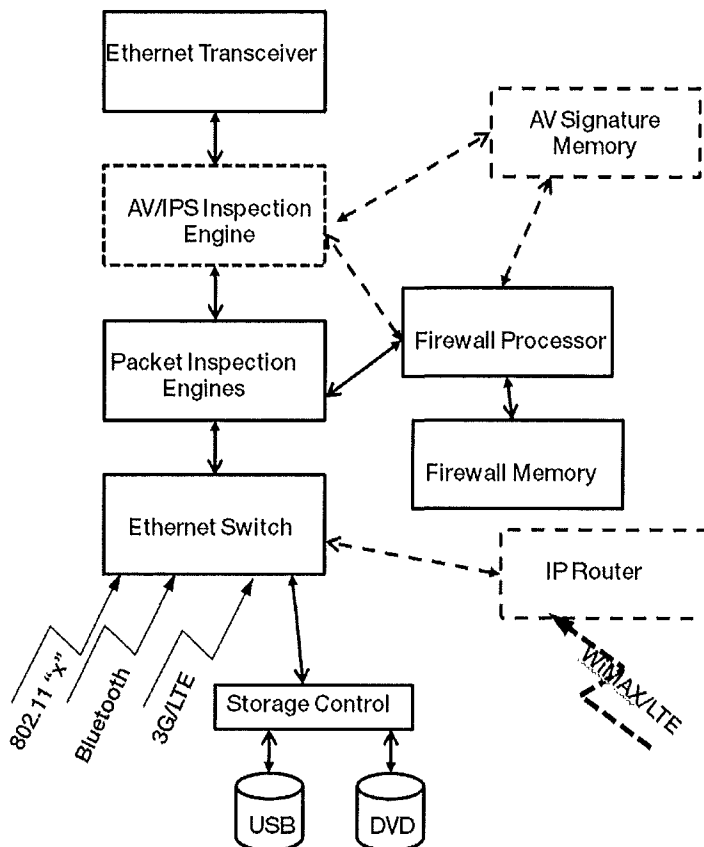


Figure 5 - Firewall w/external connections

8.1 Dash1

The Firewall basic version (Dash1) has packet inspection engines for Stateful Packet Inspection and Deep Packet Inspection that use a “standard” signature package

Project Octopus – the IP Connected Car Functional Specification

that is provided by the manufacturer. The “standard” signature package is loaded into NVRAM memory when the unit is built and not changed.

The Dash1 includes an Ethernet switch for connecting the access points and the storage controller. There is a spare port on the Dash1 Ethernet switch to allow the same blade to be used for both the Dash1 and Dash2.

The Dash1 is illustrated in Figure 5 by the solid “boxes”.

8.2 Dash2

The Firewall advanced version (Dash2) has additional components that allow a subscription program to be implemented, together with periodic updates of signatures.

The Dash2 adds an external device (IP Router) that is connected through the DashX Ethernet switch. The Dash2 blade also contains additional NVRAM to hold the AV signatures that are used in the advanced Firewall functions, which are implemented with an onboard AV/IPS engine.

8.3 Dash“x” Operation

When the Firewall starts up, it does an internal consistency check to see that all engines are operational. The unit then determines whether it is a Dash1 or Dash2 by checking the service manager tables. If it is a Dash2, it examines the time-stamp of the AV signatures and, if necessary, starts an update process via the IP router to the Cloud-based subscription. The AV signature file is buffered in local memory and then transferred to the AV Signature memory when the vehicle is inactive.

The unit then interrogates the service manager to determine what options have been installed on the DashX Ethernet switch. This allows the Firewall processor to correctly configure the Firewall ports to allow/deny the correct traffic through the Firewall.

8.4 802.11 “x” Access Point

WiFi is actually the principal way that devices connect to the car infrastructure, whether infotainment or communications. The Access Point can support up to 10 WiFi devices.

The access point allows users to BYOD to the vehicle for infotainment purposes.

When BYOD's are in the vehicle this is the preferred means of “connecting” the device to the car, because of the speed of the connection.

Project Octopus – the IP Connected Car Functional Specification

The access point also does some packet inspection to ensure that VOIP packets are processed by the “cone of silence” subsystem (see below).

8.5 Bluetooth Access Point

The Bluetooth access point provides connectivity for Bluetooth capable devices. Any data passed through the BT access point must be in the form of IP packets, since the BT access point only supports data connections. In other words, direct connection of sound devices (headsets, microphones, speakers) is not supported with the BT profiles that are associated with the access point.

If the access point determines that the end-user device is a cellphone or smartphone, it ensures that the packets are VOIP packets and that they are processed by the “cone of silence” subsystem.

The Bluetooth access point implements the Bluetooth radio standard to interface with Bluetooth devices. The access point connects to the Octopus system using an Ethernet IP connection and all communications across that interface use the packetization feature of the Bluetooth standard.

8.6 FemtoCell

Cellular phone access is obtained by connecting the cellphone to a FemtoCell, which regenerates a “cell tower” capability, but routes the packets over the IP network. The transmitter power of the FemtoCell is sufficient to guarantee that the cellphone device connects to the FemtoCell rather than to any other external cell tower.

Once the cellphone connects, the transmission is converted to VOIP packets, processed by the “cone of silence” subsystem and then routed to the “phone” network.

VOIP capability adds the ability to use the “presence” features that come with VOIP implementations to be used automatically in call handling.

The FemtoCell must be capable of supporting 10 individual devices.

The FemtoCell is implemented with a low-power radio/antenna system to interface with the cellphone/smartphone. The FemtoCell interfaces with the Octopus system with an Ethernet connection.

All communications into and out of the vehicle are transmitted as IP packets, which limits the exposure of the manufacturer to changes in technology at the FemtoCell.

Project Octopus – the IP Connected Car Functional Specification

8.7 IP Router

The IP router implements the “always connected” IP connection for the vehicle. It has a global unicast address assigned. The router functions as a standard IP router, with the added restriction that all communications between the vehicle and the Internet traverses the Firewall before being allowed onto the in-vehicle Octopus implementation. Communications out of the in-vehicle Octopus implementation also traverse the Firewall before leaving the vehicle.

The router has a WiMax/LTE radio to connect to the public backbone, which would be unique to the Wireless Internet Service Provider. Different manufacturers or different generations of vehicle communication systems may use different service providers. The Octopus architecture insulates the manufacturer from different communications standards since the router connects to the in-vehicle system with an Ethernet IP connection.

The router uses the Octopus Functional Unit Structure (Figure 3) with additional logic to implement the routing function. The processor and memory provide the control logic and the buffering for the radio subsystem.

9 Multimedia Controller

The media controller consists of a dedicated blade that implements the media related functions of the system. In particular, the media controller provides:

- Voice input
- Voice output
- Library functions for multimedia
- Display control for various “passenger positions”.

Project Octopus – the IP Connected Car Functional Specification

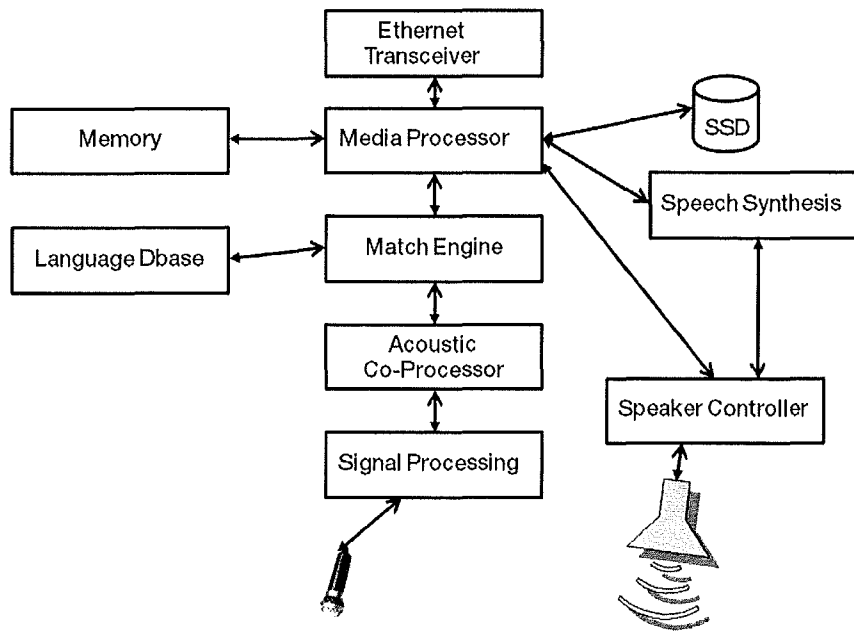


Figure 6 Multimedia Controller

The multimedia controller has both a local IPv6 address and a routable, global unicast address. The latter allows direct addressing of the multimedia controller for streaming of data from Internet resources (i.e. Cloud Storage accounts).

For “backseat”¹⁴ entertainment, the multimedia controller allows the user to request entertainment media from the controller and display it either on the fixed mount display at that seat position OR route the entertainment to a tablet device through the wireless access point¹⁵.

Infotainment requests can be made either through a tablet device (using the wireless access point) or a menu display on the main console. In either case, a menu is displayed that allows the user to choose from media previously loaded into the multimedia SSD, previously loaded into Cloud Storage, subscription channels, or general Internet resources.

If the request can be filled locally from material that is stored on the SSD that is part of the blade (this is done merely to improve latency), the multimedia controller starts to transmit the data to the display device.

¹⁴ Any passenger position other than the driver

¹⁵ It is expected that most interactive media will use the wireless tablet option
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

If the request can't be filled locally, a request is made to cloud storage for the information, which is cached on the multimedia SSD. Transmission to the display device is done in parallel to caching the information on the multimedia SSD.

Subscription channels can either be paid (e.g. Pandora, HBOm Hulu) or free (e.g. radio or TV). All multimedia input is streamed via the Internet connection of the car. The car does not support any radio antennas outside of the mobile IP connection.

General internet resources will require a tablet device at the "seating position" in order to provide the necessary interaction with the internet resource. Note that general purpose voice input control of media distribution to multiple "seat positions" is not supported¹⁶.

9.1 Operation

The multimedia controller must be able to service 10 independent clients simultaneously. Each client ("seat position") must be able to create a playlist of audio or a playlist of video, from independent sources. If the source is Cloud Storage, the multimedia controller must allow the user to specify the URL of the source and enter the appropriate account information. Only handheld/tablet devices are supported for creating "playlists" or interacting with the multimedia controller.

The multimedia unit also supports voice input for various functions. The input is done through a microphone connected to the speech recognition section of the multimedia blade. This allows the command to be decoded and matched to the possible functions that are available on the vehicle. Output is done via speech synthesis on the multimedia blade.

9.2 Configuration

When the car is first put into service, the owner will have to configure the multimedia controller menus. Initially the menu allows for all "seat positions" to have access to any media that are available through the multimedia controller. The initial configuration menu allows profiles to be created for different types of environments (i.e. passengers). By creating profiles, the owner is able to allow/disallow access from seat positions. This includes the access to menus. The configuration program also allows the owner to limit access based on MAC address of the device, in the case of handheld/tablet devices. This latter feature ensures that control is not only position based, but device based.

¹⁶ This would require multiple voice input with the ability to discriminate among seating positions. While this is theoretically possible using a technique similar to the "cone of silence", it will not be implemented at this time.
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

One of the initial control settings is whether or not to allow delegation of menus from the console to a “seat position”. In this situation, the profile would allow access to menus from one or more seat positions. In the general case, an “open” profile could be generated that allows access to menus at each seat position through a handheld device. Fixed position displays are not assumed to have touch screen input.

For most devices, the multimedia system will interrogate the device to determine the features that are available on the device. This will ensure that software that cannot run successfully on the remote device will not be loaded onto to that device.

The language database is loaded on the device at the point of manufacture. If the language module must be changed, this can be done via accessing administrative functions on the multimedia blade and loading the new language models from USB devices.

The administrative functions are available either on the consoled device or can be delegated to a specific handheld/tablet device that is authorized using the MAC address¹⁷.

9.3 Physical Media Access

The Octopus system supports the use of physical media with the multimedia system. The physical media can be used to load entertainment on the multimedia SSD or to stream entertainment directly to the display subsystem at each “seat position”. The console menu can be used to load the media and direct it to the appropriate display devices OR if the configuration has allowed delegation, a handheld/tablet device can be used to configure the streaming from the source to the display device(s).

Once the physical media access has been set up, the multimedia system sends a request to the source device to begin the file streaming, while at the same time setting up the display device to receive the streaming. This allows the system to determine if this will be using the in-vehicle hard-wire Ethernet or the wireless

¹⁷ This implies that there needs to be a supervisor mode that can be accessed by a dealer. The most logical way to do this would be to have a tablet device with a security token that authorizes supervisor mode. Supervisor mode access will have to be part of the NVRAM that is used to load the multimedia controller. At a depot repair site, a reset function will be required before access to the device can be obtained.
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

access point. If the wireless access point is used, a request is made to the Cone of Silence subsystem to ensure that the media is appropriate for the seat position¹⁸

The stream is buffered temporarily on the multimedia SSD to reduce latency. The multimedia software is also capable of determining how much buffer memory is available on the display device and pre-load data as necessary.

9.4 BYOD Physical Media Access

Many owners wish to use their personal communication devices as sources for infotainment, even though they have access to their infotainment media that is stored in their personal Cloud Storage.

Octopus allows such devices to be connected to the Multimedia Controller using either WiFi or Bluetooth wireless networking. The device will require an “app” to be loaded from the Manufacturer’s “app store” that interacts with multimedia requests to pull information to the Multimedia Controller, from where it can be streamed to its final destination. Typically the interaction will be made using the console menus, which treat the “personal device” as just another removable disk. The “app” will also allow the user to interact with the Multimedia Controller from the device to create the pull requests¹⁹.

Similarly, the user can create requests for media from a “personal device” by using the voice command system that is part of the Multimedia Controller. The voice commands are translated into IP messages that interact with the “app” on the device to cause infotainment to be streamed.

BYOD supports multiple devices as disk devices.

9.5 Cloud Storage for Media

If the vehicle has an IP router that comes with a Cloud Service, vehicle data is stored in the Cloud Storage. This includes specific vehicle performance data that is used for “customer care” associated with the vehicle.

The Cloud Storage can also be used as an aggregation point to hold “media playlists” that are actually served by other Cloud Storage Services. For instance, if a family subscribes to Netflix to provide for multimedia entertainment for the

¹⁸ This ensures that the operator does not get a movie streamed to the console or to a handheld device/tablet in their possession. It might be possible to implement a parental control module that would be an “add-on” to the “cone of silence” subsystem.

¹⁹ Messages that interact with the multimedia controller and that originate on the device go through Cone of Silence processing.

Project Octopus – the IP Connected Car Functional Specification

“backseat”, the playlist that is stored in the vehicle cloud storage would be loaded into the multimedia controller and executed.

The “playlists” can be organized by vehicle operator, which allows a subset of playlists to be loaded into the multimedia controller based on the operator personalization that is stored in the Cloud Storage.

Cloud Storage is accessed through several indexes, which include:

- VIN
- Owner ID

The Operator Personalization are always stored as records accessible through the indices.

The Cloud Storage is configurable through the console, handheld device/tablet with delegated console functions, or by accessing the Cloud Storage with a web application that is supplied by the vehicle manufacturer.

While the Cloud Storage is accessible to the owner/operators of the vehicle, the database must have sufficient security that the vehicle operational data is only accessible to the customer care or safety engineering departments of the vehicle manufacturer. Information for insurance purposes would have to be extracted and sent to the insurance company²⁰. Similarly, access to accident information would have to be made via a documented request²¹.

The requirements for separating access to information may require more than one Cloud Storage system, accessed through the VIN mapping.

²⁰ It is possible to conceive of a situation where an Insurance Company would provide a “safe driver” application through the “app store” OR an actual hardware/software subsystem that would connect to Octopus and communicate directly through the IP router.

²¹ Whether this would have to be a court order is left to the amusement of the lawyers
project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

10 Operator Cluster

The “operator cluster” (aka the dashboard or instrument cluster) is composed of a dedicated display controller and an optional “heads up” display controller. The operator cluster is fed data from the FlexA3 computational system via an Ethernet connection. The unit is configurable by the operator, with multiple “driver personalities” stored in the SSD that is part of the computational system.

The operator cluster is configured by enabling the “configuration application” on the display. The “button” is always “hot” on the touch screen when the vehicle is NOT in motion. Entering the “configuration” application allows the operator to choose from a set of “gauges” that are displayed, with the restriction that the “speed indicator”, “gear choice”, and “operator warning area” be part of the in vehicle display. The configuration application will enforce the requirement that a “speed indicator” and “operator warning” are clearly in the most visible part of the display²². If the configuration application detects the presence of the heads up display controller, the speed indicator is made part of that display also²².

The configuration application has a graphical list of other vehicle information that the user may want to be displayed in the “instrument cluster”. The user will be able to choose the information and move it to the appropriate place on the “operator cluster” display through the (enabled) touch screen. When all the information has been added to the “operator cluster” display, the user chooses “done” from the menu and is asked for a distinctive name with which to save the information. For a new user, a new file is created on the storage unit of the FlexA3 computational system. If the user name exists, the user is asked whether to overwrite the file or create a new name. Once the file has been created, the device controller disables the touch screen except for the configuration application “button”.

The configuration software will have to manage the screen real estate to insure that the “gauges” and “information” are always visible and clear. This will require the configuration application to manage nearest neighbor information and ensure that it all fits. If the information does not fit or it becomes cluttered²³ the configuration application does not allow the user to exit the program until the problem is resolved.

²² The speed indicator and operator warning area will be confined to specific parts of the display based on manufacturer preference or legal requirements

²³ This will be a manufacturer selected option. The configuration application must allow the discrimination values to be altered easily (i.e. parameter file)

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

For a case of fit, the offending information graphic will be highlighted. For the case of clutter, the “display cluttered” message will be displayed.

When the vehicle is started, the operator sees the last “operator cluster” display that was used. If a different operator display is needed, the operator can choose to change the display by activating a “button” and selecting the correct file from the display.

10.1 Operator Warning

The Operator Warning area of the Operator Cluster is a reserved messaging area for the Octopus system. When the system starts up, the Operator Warning area contains a “checking system” message.

The system health check is controlled by applications running on the “master blade” of the system. The health check interrogates all the subsystems (including the vehicle sensors) for operational consistency. Once all the subsystems pass operational consistency, the Operator Warning display changes to a date/time/temperature display.

The operational consistency check must be completed within 10 seconds²⁴. The consistency check completion causes a timer on the Operator Warning display to be terminated. If the consistency check is not completed within 10 seconds, the display times out and is replaced with a “fatal error”²⁵ message, after which the ignition system is disabled.

10.2 Default Operator Profiles

The vehicle manufacturer will create a Default Operator Profile Template that is modified whenever the driver chooses to personalize the console and Heads Up displays.

By convention, the vehicle always has one default driver profile (built from the template) that is active on the vehicle. If the driver does not choose to personalize a profile, the default profile is in effect when the vehicle is started.

The default profile cannot be deleted from the FlexA3 computational storage SSD.

10.3 Personalized Operator Profiles

If the operator has chosen to personalize a profile, this profile is stored in the on-board FlexA3 Computational Storage SSD. If the FlexA3 computational system

²⁴ This is somewhat arbitrary and the actual value is determined by the vehicle manufacturer

²⁵ The actual wording is determined by the vehicle manufacturer

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

detects an IP router and Cloud Account, the profile creation application backs up the profiles to the owner's Cloud Storage Account.

10.4 Heads Up Display

The Heads Up Display (“HUD”) is an optional component for a vehicle. The HUD is implemented as an Ethernet based subsystem. The HUD is capable of displaying a subset of the information available on the Operator Cluster and the Navigation Display. This information includes:

- Speed
- Tachometer (optional)
- Temperature (optional)
- Navigation display
 - Map
 - Speed limit
 - Next turn indicator
- Operator Warning

The HUD is implemented as a Hologram projected through the windshield and the viewing distance can be adjusted to compensate for operator vision restrictions (i.e. projected further out if the driver is far sighted, etc.).

The Navigation display is a subset of the display that is available through the console. It is designed to ensure that the driver's attention is not distracted by a center mounted display. The HUD display is supplemented by the speech synthesized turn-by-turn directions available through the speakers of the multimedia subsystem.

The HUD information options, viewing distance and display arrangement can be set up through the console menus and stored with a driver profile. If the user does not specify options, the HUD will default to displaying

1. Speed
2. Navigation display
3. Operator Warning display

The HUD is used whenever the FLeXA3 computational unit detects its presence on the vehicle. The operator is not able to disable the HUD. The default display arrangement is chosen by the vehicle manufacturer and stored in the driver profile template.

Project Octopus – the IP Connected Car Functional Specification

11 Manufacturer Support Service

If the vehicle is equipped with the “always on” IP connection and has the “manufacturer support service” (“MSS”) option, then the vehicle continually transmits operational status to manufacturer support center. This is implemented with the Event Data Recorder Subsystem.

The Event Data Recorder Subsystem (“EVRs”) is designed to capture operational data as a continuous sampling process, with data being transmitted to Cloud Storage associated with the vehicle on a “batch” basis. The data could be collected by an insurance company as part of a ‘good driver’ program, the vehicle manufacturer as part of a quality and performance assurance program, or by the owner of the vehicle.²⁶

11.1 Normal Operation

Data is collected as a fixed packet and includes such operational parameters as speed, brake sensor position, steering wheel sensor position, GPS coordinates, number of occupants, and diagnostic code if applicable.

During normal operation, EVRs collects data every 30 seconds, buffering this data in the FlexA3 SSD, until pre-defined criteria are met. At that point, the EVRs creates a data packet and moves the data to Vehicle Cloud Storage

Any failure information that is created by the Master Blade Application Control program is transmitted as part of the EVR transmission.

11.2 E911/E112 Operation

The EVR Subsystem collects multiple data packets, presumably with one or more diagnostic codes, over a predefined period. The Octopus System is designed to remain operational for 10 seconds after an E911/E112 event, collecting data for this time period. The E911/E112 packets are transmitted to the Vehicle Cloud Storage as they are created.

11.3 Customer Care/Advanced Analytics

As noted above, vehicle performance data is collected continuously and stored in Cloud Storage, accessible by Customer Care and Safety Engineering. As part of the “connection package”, the manufacturer routinely performs analytics on the data allowing maintenance or faults to be detected.

²⁶ Vehicle owner could be a car rental/lease company
project octopus - functional spec - v002a - 041413.docx
© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

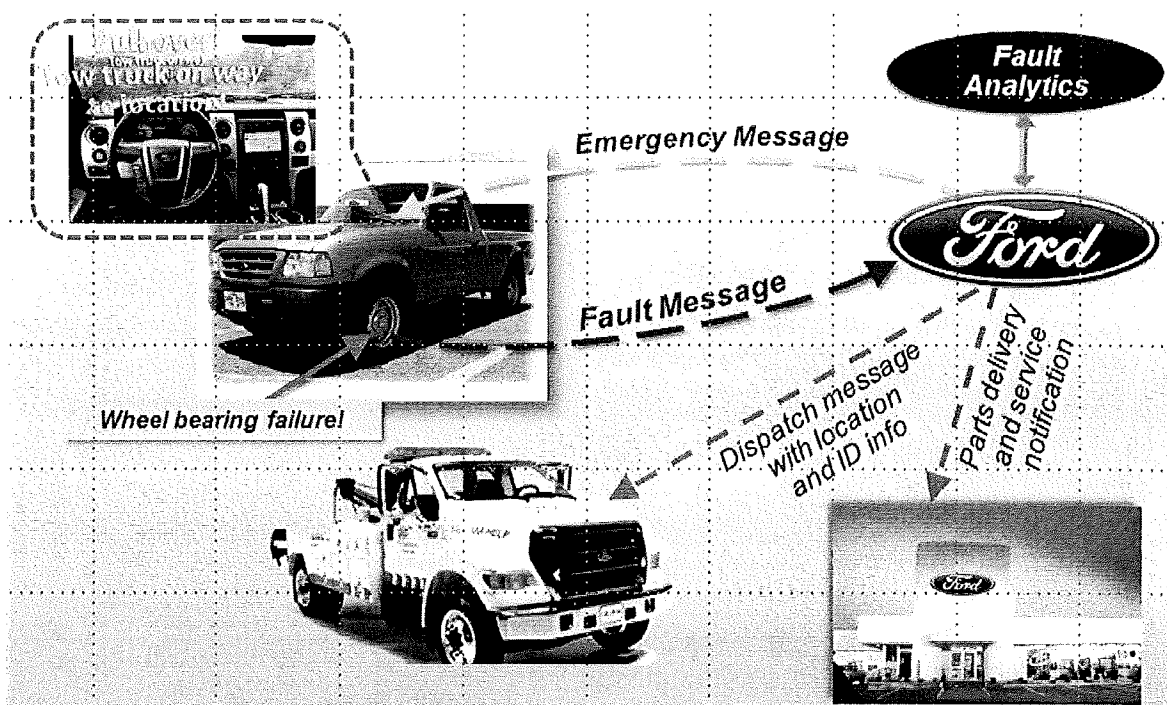


Figure 7 Vehicle Analytics & Customer Sat

The scenario in Figure 7 illustrates a possible scenario when the real-time vehicle analytics determine a hazardous fault.

Additionally, by looking at analytics over families of vehicles and model years, the manufacturer would be able to offer predictive analytics. If the data were to be shared among manufacturers, systemic component problems could be identified. This would allow the manufacturer to identify systemic vehicle or component problems earlier, allowing a better response to component problems²⁷.

12 Cone of Silence Subsystem

12.1 System Expansion Example

The CoS functionality is an example of the way new features can be added to an existing implementation. The Ethernet-based components, together with the

²⁷ Forbes – Big Airbag Recall Affects Toyota, Honda, Nissan and GM, But Effects Probably Won't Last Long
– Jim Henry – 12 April 2013

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

message based IP implementation simplify creating new options or new generations of control systems.

12.2 Technology Overview

The Cone of Silence (“CoS”) is an advanced function that allows hand-held device location to be determined within a vehicle. CoS is implemented by positioning WiFi and cellular antennas throughout the passenger compartment which interact with any WiFi or cellular devices that are present. The signal strength measurements from multiple antennas, and the MAC addresses of the device, are then used to create a real-time “map” of where the devices are. The CoS scan also identifies the type of device that is associated with the MAC address, since only certain device functions may be altered or limited by the CoS processing.

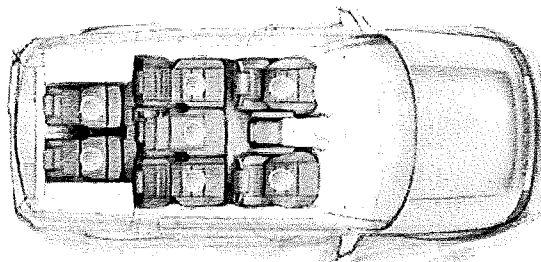


Figure 8 - Cone of Silence Senors

Additionally, “seat weight” sensors are used to ensure that there a “user” is at that location. This eliminates the possibility of a device being “thrown” on an empty seat and not being tied to a particular seat position, such as the driver’s position,

The sensor assemblies are implemented in the form of the Octopus Functional Unit Structure, with several antennas attached to the same functional unit. In addition, the “seat weight” sensors are connected to a functional unit. These send scan packets on a pre-defined interval to the CoS mapping function that executes on a blade processor. The Octopus system diagram for this case is shown in Figure 9

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

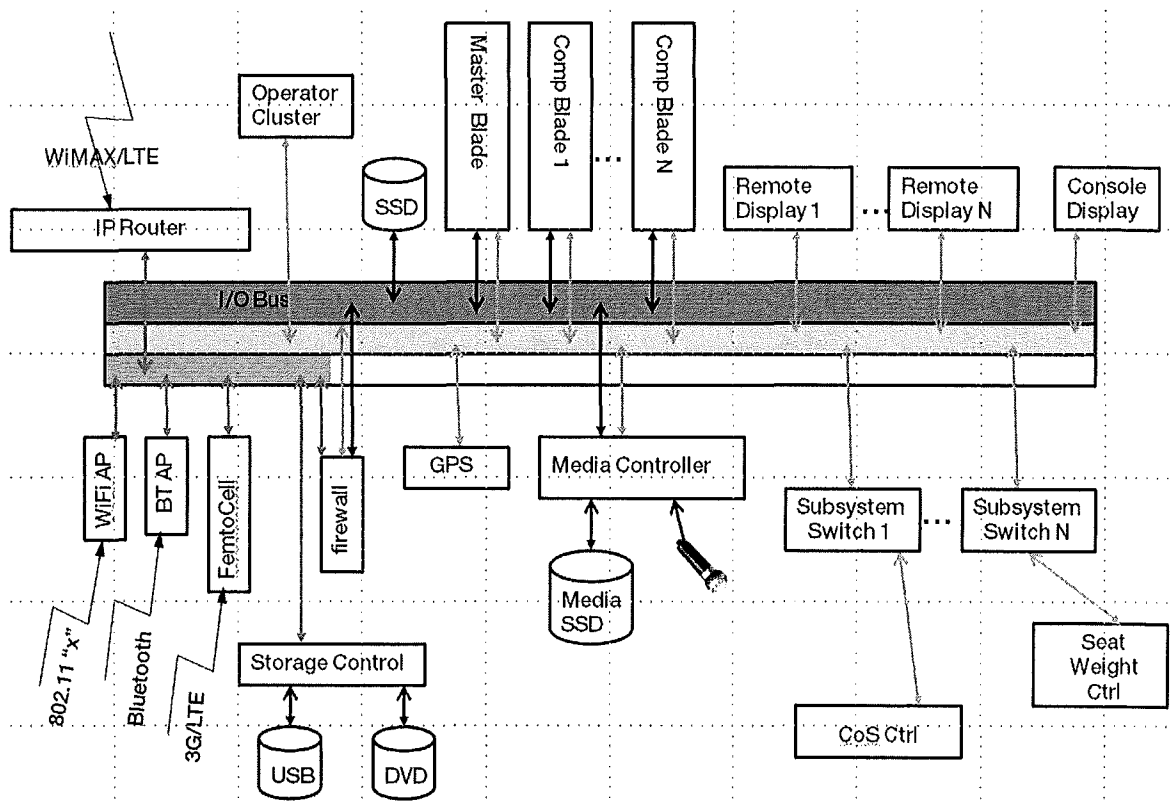


Figure 9 Octopus Cone of Silence System Diagram

The CoS mapping function executes continuously as a Blade application, ensuring that no unexpected location changes occur for the devices in the vehicle.

12.3 CoS Operation

The Cone of Silence (“CoS”) is used to control the operational aspects of any hand-held devices that are in the vehicle. The CoS depends upon the fact that Octopus uses “preferred hotspots” or access points for either or both WiFi and Cellular handhelds/tablets (described above), so that handheld/tablet devices will attempt to connect to those access points rather than external access points.

The access points contain code that compare the MAC address of the source to the location table generated by the CoS scanning function. This table is updated every 10 seconds at the access point. If the MAC address matches the source address of a “special” seat location, the packet is sent to the CoS application for special processing. The special processing allows for enforcing “usage rules”, such as:

- In some jurisdictions (e.g. Massachusetts) text messaging may not be allowed for a driver. Hence this would be a “usage rule” that would be enforced by

Project Octopus – the IP Connected Car Functional Specification

Octopus, while the vehicle was a) operational (drive train in gear) and b) in Massachusetts.

- In another example, the use of a hand-held device by a teenage operator (as required in Massachusetts) could be selected by parents and entered into the Octopus preferences.²⁸ Then when the conditions of a) teenage driver, b) drive train engaged, and c) handheld on are met, no handheld activity would be allowed.

The granularity of the control can be defined in the preferences for Octopus, with the caveat that regulatory rules cannot be over-ridden. Not all device functions are subject to CoS processing. Using the device as a multimedia source could still continue, even if the device was prohibited from being used as a communication device.

Octopus preferences can be created using the console, a tablet with delegated console functions, or a web application. All these preferences are stored in the owner's cloud service area. When additional driver profiles are created, the owner can specify "parental controls" at which time the "parental rules" are loaded into the profile and cannot be changed by the driver.

The usage rules that are mandated by jurisdictions are activated based upon the vehicle location. Periodically CoS processing accesses the GPS unit to determine the vehicle location²⁹.

If the CoS determines that sensors required for CoS processing are not present, the CoS processing application is a passthrough.

In the event that the vehicle owner has more than one vehicle, the CoS processing will use the VIN in addition to the MAC address to determine how various device functions are treated.

13 Modularity – Gracious Upgrades

Since Octopus is an Ethernet connected distributed system, it is possible to change the electronics/control systems in a modular fashion once the FlexA3 system is installed.

²⁸ Part of the parental control selection process is to register the MAC address of the teenager's phone with the Octopus Network Controller.

²⁹ An alternative would be to have the NAV system track vehicle location and send a message to CoS processing to indicate when a jurisdiction had changed. This would require an ancillary monitoring program in the NAV subsystem to track location AND an inventory of jurisdictions that have restrictions.

project octopus - functional spec - v002a - 041413.docx

© 2013 – Flextronics, Inc. - Confidential

Project Octopus – the IP Connected Car Functional Specification

This means that the investment in the current generation(s) of sensors and control electronics do not have to be simultaneously changed, with installing a FlexA3 distributed system. A further implication is that options can be selectively offered for different classes of vehicles.

13.1 Modularity – “and how would you like that configured?”

An Ethernet distributed system allows various components to be developed separately and then be integrated into the system without re-engineering the entire system.

In the Octopus design, this means that components such as

- IP router
- Heads Up Display
- Bluetooth Access Point
- WiFi Access Point
- Femtocell

do not need to be present in all models of all vehicles. The options can be added simply by plugging them into the backbone Ethernet and installing the appropriate software.

This would also allow a true “ecosystem” to be established where approved 3rd party suppliers could provide these components, which would integrate seamlessly with the base system.

It is also possible to design and implement Octopus so that the actual control code would always be present in the vehicle “software image”, but would only be active once the components were added. To protect the vehicle manufacturer in that case, the “options” would come with an ID, 3rd party registration number, and serial number. Once the option was installed and the car restarted (i.e. rebooted), the Octopus software would connect to the manufacturers support site to activate the options³⁰.

Alternatively, the option might come with an ID, 3rd party registration number, and serial number for use when the vehicle doesn’t have an “always on” Internet connection. These would be hashed with an “activation number”. The installer would enter the activation number when the unit was installed, activating the unit. If at some point in time the vehicle was connected to the Ethernet and the vehicle had

³⁰ This would obviously require that the car had an “always on” internet connection.
project octopus - functional spec - v002a - 041413.docx

Project Octopus – the IP Connected Car Functional Specification

access to the Manufacturer Support Service, the validity of the unit IDs could be confirmed.

13.2 Transition to the Future

In the current generation of vehicle control systems, the Car Area Network (“CAN”) bus is used to connect discrete sensors and control elements together. This is illustrated in Figure 10

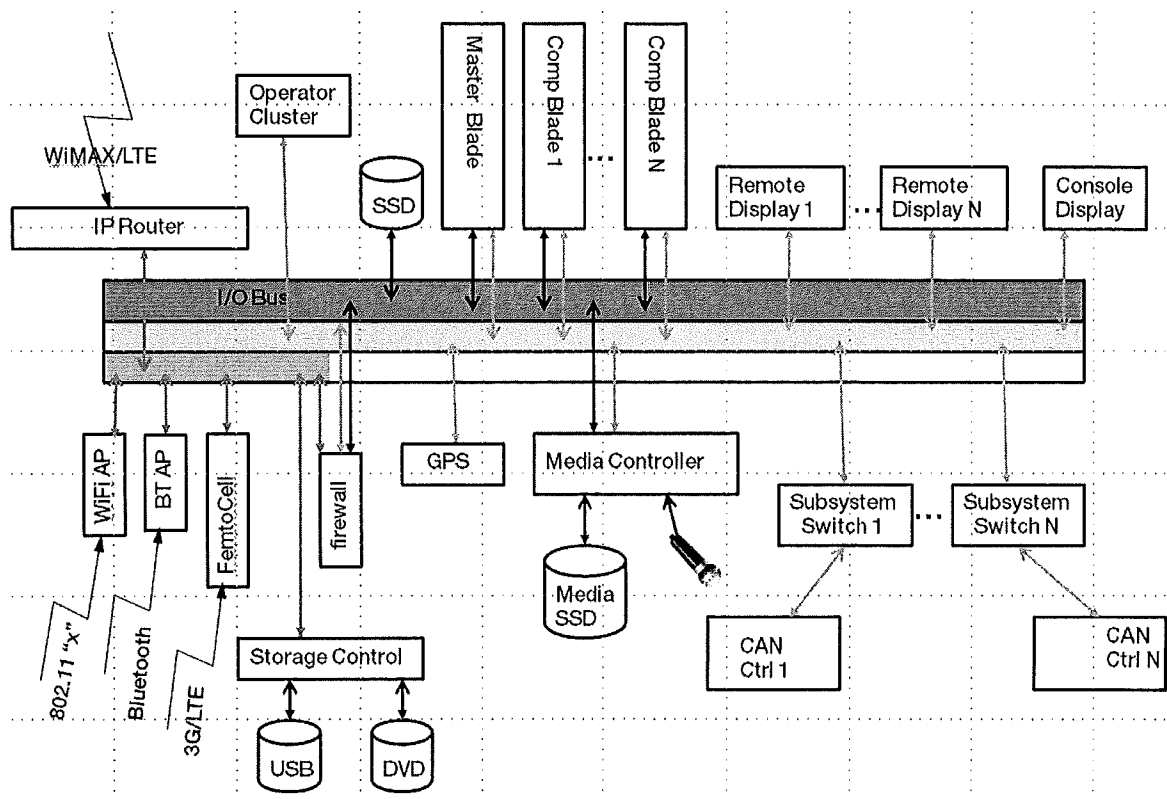


Figure 10 Octopus Transitional Implementation

In a transitional implementation, the CAN bus controller is now an Ethernet based device, which implements the translation of the Ethernet packets to CAN packets. The control logic executes as an application on one of the FlexA3 Application Blades.

The transitional implementation also outlines how new capabilities can be added to the system, either using “transitional adapter controllers” or a new generation of Ethernet based sensors and controllers.

Project Octopus – the IP Connected Car Functional Specification

By working with a “transitional implementation”, the operating code can be written once and then used with new sensors or controllers as they are phased in.

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

FUNCTIONAL SPECIFICATION FOR A NEXT GENERATION AUTOMOBILE

First Named Inventor/Applicant Name:

Christopher P. Ricci

Filer:

Douglas W. Swartz/Christine Jacquet

Attorney Docket Number:

6583-474-PROV

Filed as Large Entity

Provisional Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
-------------	----------	----------	--------	----------------------

Basic Filing:

Provisional Application Filing	1005	1	260	260
--------------------------------	------	---	-----	-----

Pages:

Prov. Appl Size fee per 50 sheets >100	1085	1	400	400
--	------	---	-----	-----

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				660

Electronic Acknowledgement Receipt

EFS ID:	15519182
Application Number:	61811981
International Application Number:	
Confirmation Number:	3582
Title of Invention:	FUNCTIONAL SPECIFICATION FOR A NEXT GENERATION AUTOMOBILE
First Named Inventor/Applicant Name:	Christopher P. Ricci
Customer Number:	111285
Filer:	Douglas W. Swartz/Christine Jacquet
Filer Authorized By:	Douglas W. Swartz
Attorney Docket Number:	6583-474-PROV
Receipt Date:	15-APR-2013
Filing Date:	
Time Stamp:	15:55:45
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$660
RAM confirmation Number	2874
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	6583-474-PROV-CoverSheet.pdf	1477009	no	3
			9eed336ee8c0420d7a4f1ff4cebb14ca716bc58e		
Warnings:					
Information:					
2	Specification	6583-474-PROV-Spec.pdf	346176	no	96
			70b82a7b561127e8ade997098d8c0c81e5a241da		
Warnings:					
Information:					
3	Drawings-only black and white line drawings	6583-474-PROV-DrawingsFinal.pdf	137461	no	31
			d9f581eaf1d45507d1317fe8ec13f5f54580f99d		
Warnings:					
Information:					
4	Appendix to the Specification	6583-474-PROV-Exhibit-A.pdf	3787712	no	34
			167aaec85be4c475d9956e01e37c91917c2fe2fd		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	31863	no	2
			25a748aef687a2ca2e66b876ae682164ff5574ea		
Warnings:					
Information:					
Total Files Size (in bytes):			5780221		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/811,981	04/15/2013		660	6583-474-PROV		

CONFIRMATION NO. 3582

111285
Sheridan Ross P.C.
1560 Broadway
Suite 1200
Denver, CO 80202

FILING RECEIPT



OC000000061435252

Date Mailed: 05/29/2013

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Christopher P. Ricci, Saratoga, CA;

Applicant(s)

Christopher P. Ricci, Saratoga, CA;

Power of Attorney:

Douglas Swartz--37739

If Required, Foreign Filing License Granted: 05/22/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/811,981**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

FUNCTIONAL SPECIFICATION FOR A NEXT GENERATION AUTOMOBILE

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same

page 1 of 3

effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with

respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.