The case for a Vehicle Gateway.

Equipment and Tool Institute

ETI-ToolTech_2015_Gateway.pptx

Vehicle Data Access

- Last year we proposed a “Vehicle Station Gateway” and its associated “Unified Gateway Protocol” as a potential pathway to a solution for secure vehicle data access.
- This proposal was not adopted as a new work item within ISO, even after two strong efforts from the Aftermarket and ITS stakeholders.
- As a result we still have no unified path forward for secure vehicle data access.

ISO Technical Committees

TC204

ITS Standards

V-ITS-SG

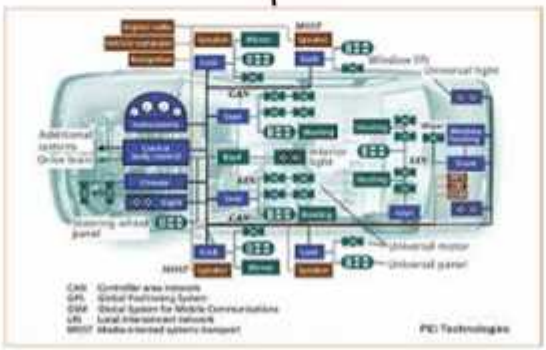
ISO TC204 responsibility

Joint Standardization

ISO TC22 responsibility

TC22

Road Vehicle Standards



ISO
TC22 and TC204

Current discussions

- At the request of TC204 there was another meeting between TC22 and TC204 March 9-10 in Berlin at VDA offices to try again to get a joint task force to implement standards for the ITS secure gateway.
- No agreements were made as the manufacturing representatives are still resisting direct access to their vehicles which is essential for real-time access for safety critical functions.
- TC204 is studying their next move to be able to have a standardized secured access point
- A mandate from some regulatory agency like NHTSA may be required for action
- SAE J2922 - DSRC Vehicle Interface Methodology

Current “Issues”

- Since last year several things have gained national attention in the news, and Vehicle “Hacking” has become front and center.
- A few of the news items I will mention:
  - The report overseen by Sen. Ed Markey, D-Massachusetts “Markey Report Reveals Automobile Security and Privacy Vulnerabilities”
  - The “60 Minutes” episode http://www.cbsnews.com/news/car-hacked-on-60-minutes/
  - The lawsuit by Dallas-based attorney Marc Stanley that slapped Ford, General Motors and Toyota with a proposed class-action lawsuit on behalf of three car owners, accusing the automakers of a negligent response to the risk of hacking.
  - The 20 Most Hackable Cars - Chris Valasek and Charlie Miller

Current “Issues”

- Partially due to this pressure, OEM’s will rapidly develop and implement enhanced security for the IVN’s (In-Vehicle-Networks), with encryption practices and proprietary certificate secure gateways.
- And as they look for “Attack surfaces” for potential hackers it is the “Remote” access that brings the most concern.
- Most OEM’s consider the SAE J1962 connector to be one of the biggest “Security” concerns.
- Aftermarket “Wireless” adapters will be scrutinized excessively.

Current “Issues”

- One path VM’s may take is to remove any and all “Non-legislated” functionality from the J1962 connector and only provide enhanced diagnostics through their proprietary wireless connections and being accessed via their corporate servers.
- The potential un-intended consequences should concern many in this room that provide aftermarket services like:
  - Handheld scan tools
  - Data-loggers
  - Vehicle monitoring
  - Remote services
  - Etc.

Current “Issues”

- How can we avoided this issue?
- Develop a standardized secure access gateway for VM’s and the Aftermarket.
  - Utilizing the enhanced security systems being implemented for V2V and V2I ITS networks.
  - Combining resources on the vehicle to leverage one access point for multiple use-cases therefore reducing the cost of the implementation and therefore vehicle cost

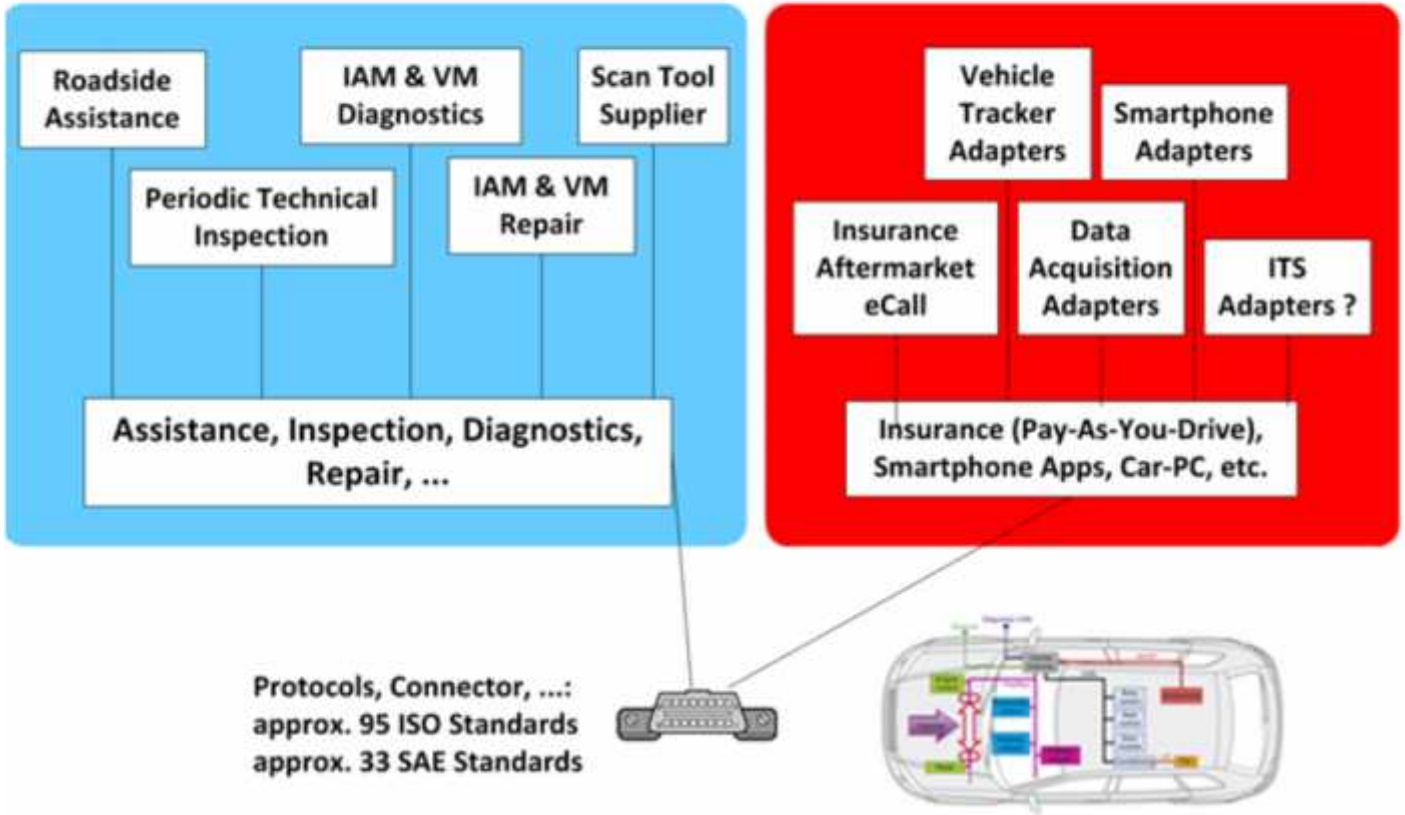
Concerns

- Known Issues related to in-vehicle data access via diagnostic connector
  - ISO 15031-5/SAE J1979 emissions-related OBD protocol does not prohibit “back to back” tester data request and vehicle ECU(s) response(s)
  - This causes uncontrolled network bandwidth problems which may impact the functional vehicle safety when driving on the road
  - Each device compatible to the ISO 15031-3/SAE J1962 diagnostic connector is authorized to access vehicle data according to legislation
  - Today’s vehicle architecture implementations are not able to provide asynchronous communication between external test equipment connected via the diagnostic connector and the in-vehicle network ECUs
  - Today’s diagnostic protocols are not designed to support multiple client (test devices) implementation support for vehicle ECUs
  - An update or redesign of the most common diagnostic protocol (ISO 14229 UDS) is unrealistic because of non-backward compatibility to existing release
  - Unauthorized access may cause violation of data privacy regulations

Current communications

CURRENT **CONCERNS**

Vehicle Data Access Occasionally Causes In-Vehicle Network Disturbance



Needs

The automotive gateway of the future should be designed to address the following challenges:

1. Support multiple networks and provide secure wireless connectivity for/between vehicles and infrastructure.
2. Provide secure, intelligent switching between different networks.
3. Sense, select, and switch to best available network automatically based on user-defined policies.
4. Create a mobile hotspot for wired and wireless devices in and around the vehicle.
5. Support various IP devices in the vehicle.
6. Support upgradeability for current / future networks.
7. Provide secure and reliable communication for all connected devices.

Challenges

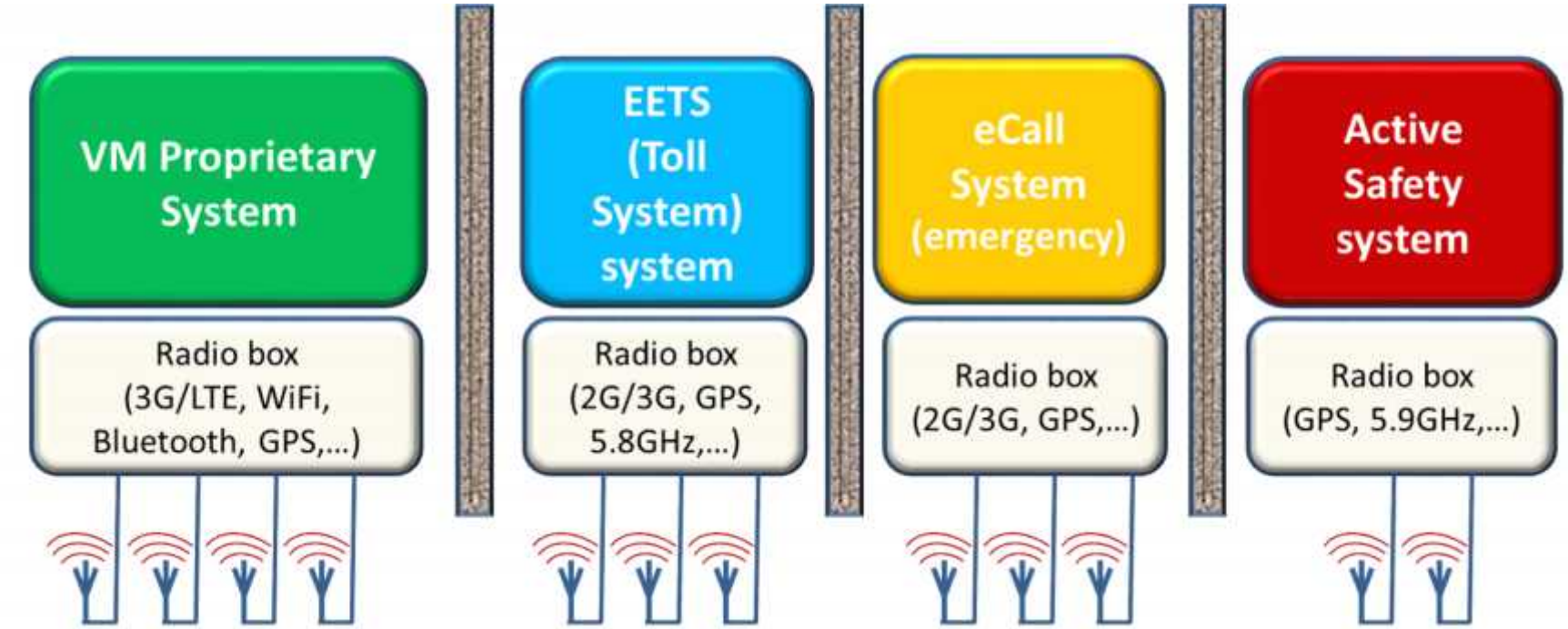
ITS-S challenges

- Vehicle internal networks are now more connected to external devices, thereby exposing the internal network to the outside world.

- Vehicles are no longer closed networks; they are potential targets for remote attacks. In-vehicle networks are safety-critical, and any unauthorized access to an in-vehicle network may have serious safety implications. Therefore, both internal and external communication networks must be secured.

- With the increased complexity of telematics services and applications, the big challenge is not to provide a platform with extensive features, rather to create a “future-proof” vehicle gateway that has the flexibility to adapt and accommodate rapid changes and the ability to support new functionality that holds the key.

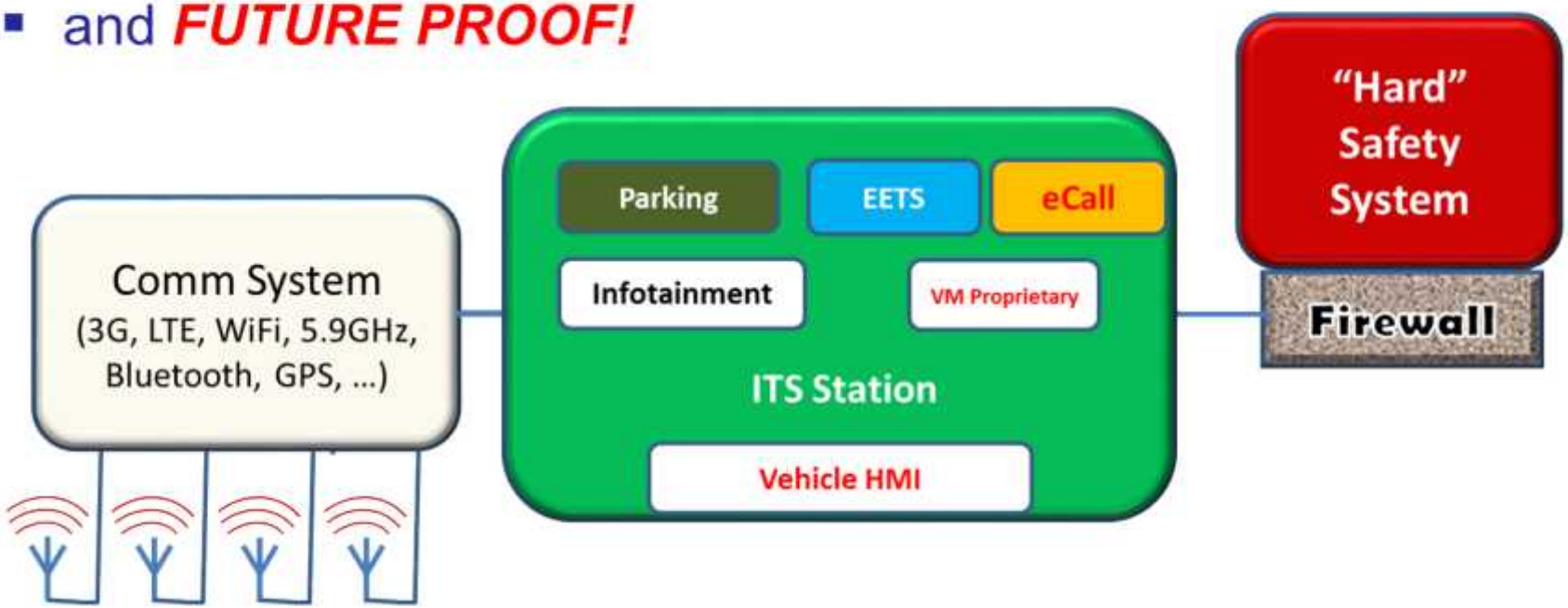
Current “Silo” systems



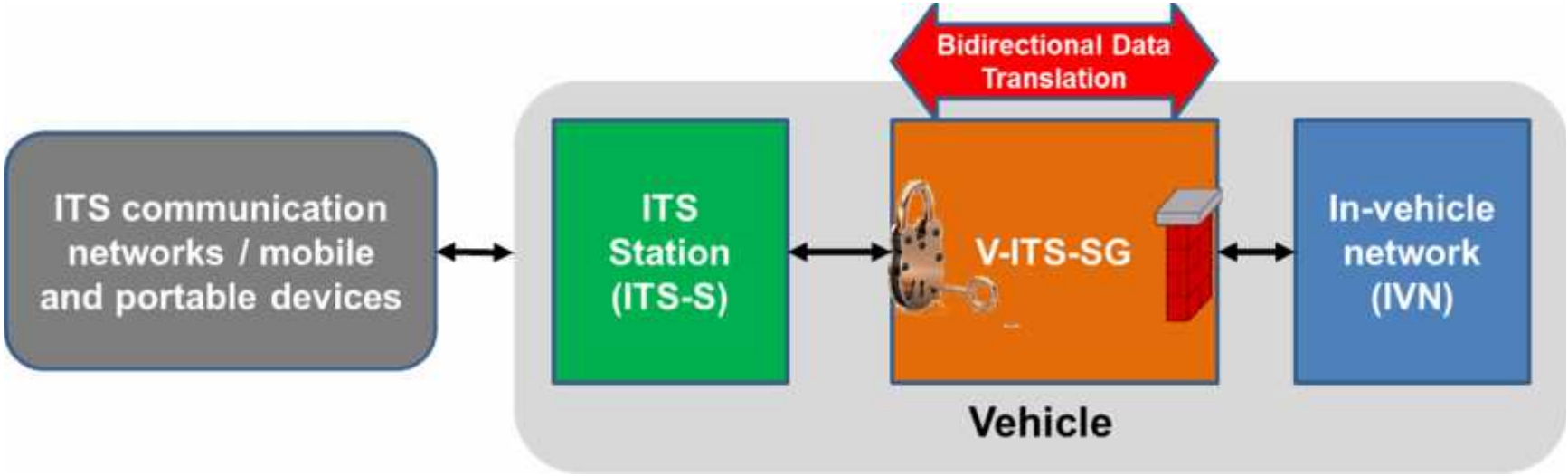
- Mandated and value-added applications implemented in "silos“ … duplication of equipment and no sharing of data and resources … ***SUBOPTIMAL & EXPENSIVE!***

The “Single” solution

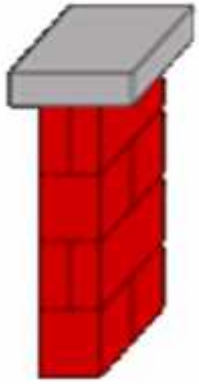
- Sharing of equipment and data … it’s a ***BETTER CONCEPT!***
- and ***CHEAPER!***
- and ***SAFER!***
- and ***FUTURE PROOF!***



Multiple Security Levels



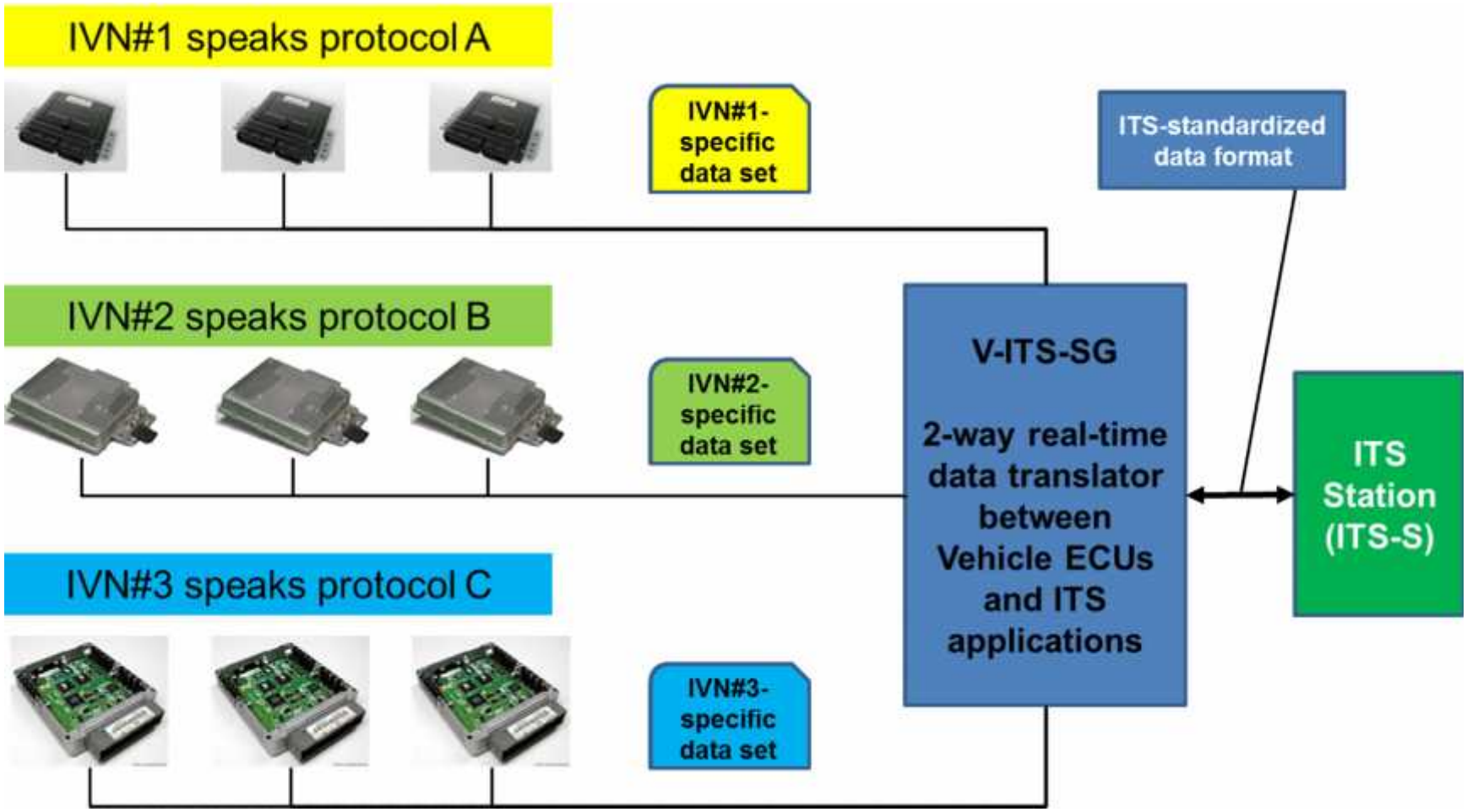
- The Vehicle ITS Station Gateway (V-ITS-SG) is an entity in a vehicle that has:
  - firewall functionality
  - data translation functionality
  - secure real-time information (data) exchange functionality
- Important:
  - The Vehicle ITS Station Gateway (V-ITS-SG) is part of the vehicle and does not mean anything outside the vehicle



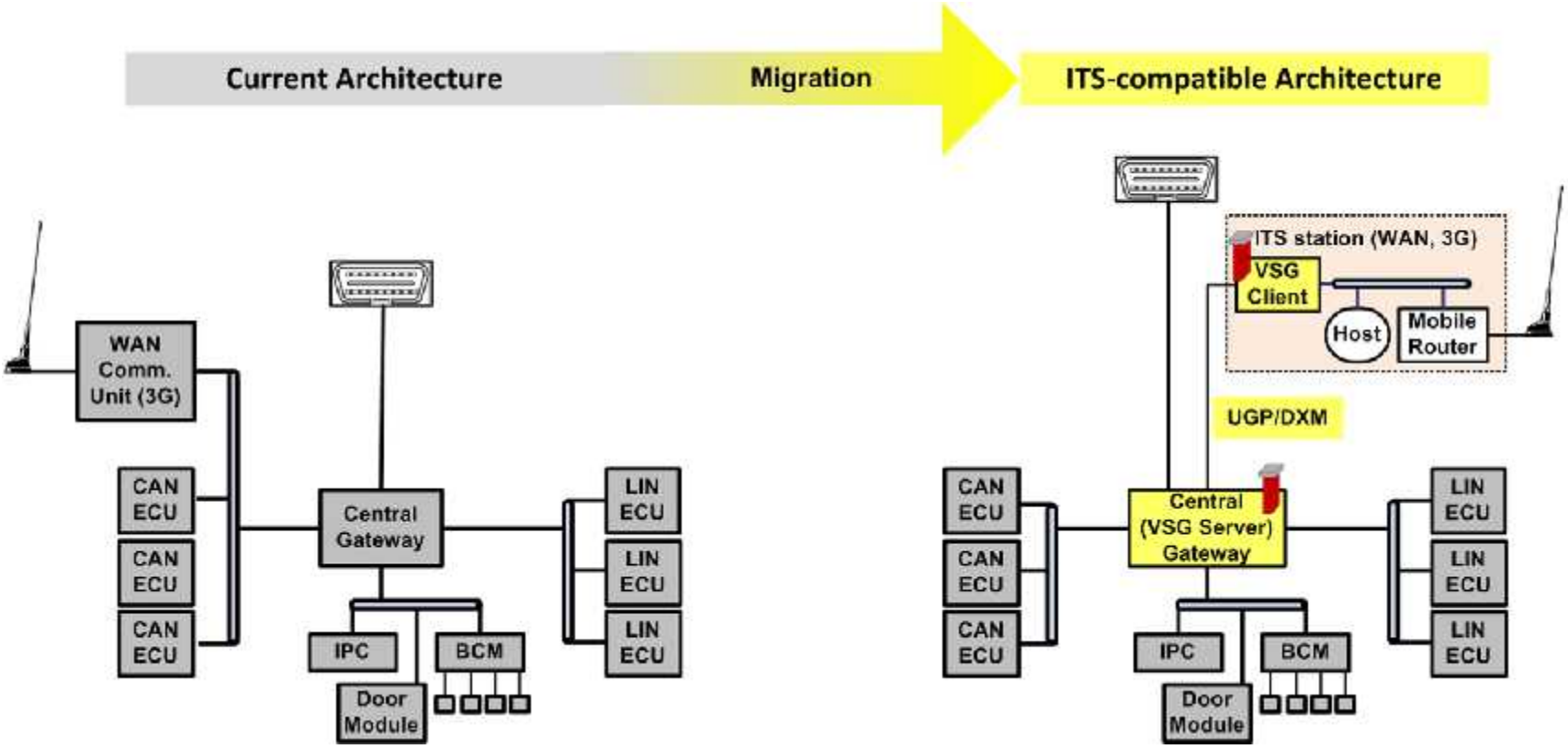
- The V-ITS-SG firewall functionality:
  - Protects the IVN from "attacks" originating in the ITS communication network and other mobile and portable devices
  - Protects the ITS-S and ITS communication networks (and other devices) from "attacks" launched using the IVN

- The V-ITS-SG data translation functionality:
  - Translates information (data) from IVN representation to ITS-S representation and vice-versa
- The V-ITS-SG secure real-time data exchange functionality:
  - Allows an ITS-S to obtain IVN data in real-time for safety and traffic efficiency applications/services (and others)


Vehicle
Access


IVN#1 speaks protocol A
IVN#1-specific data set
ITS-standardized data format
IVN#2 speaks protocol B
IVN#2-specific data set
V-ITS-SG
2-way real-time data translator between Vehicle ECUs and ITS applications
ITS Station (ITS-S)
IVN#3 speaks protocol C
IVN#3-specific data set


Vehicle
Access


Current Architecture
Migration
ITS-compatible Architecture
WAN
Comm.
Unit (3G)
CAN
ECU
CAN
ECU
CAN
ECU
Central
Gateway
LIN
ECU
LIN
ECU
LIN
ECU
IPC
BCM
Door
Module
ITS station (WAN, 3G)
VSG
Client
Host
Mobile
Router
UGP/DXM
CAN
ECU
CAN
ECU
CAN
ECU
Central
(VSG Server)
Gateway
LIN
ECU
LIN
ECU
LIN
ECU
IPC
BCM
Door
Module

Benifits

- Benefits to the VM’s
  - Keeps the IVN completely isolated from the outside world
  - Uses common components for multiple uses therefore reducing costs.
  - Provides state-of-the-art security that is updateable
  - Provide safe and secure pathways for the Aftermarket to access “authorized” data
  - Adoption of ITS communication technologies (including security services and functions) will open up new markets for services, some of which will open opportunities for auto OEMs to financially benefit significantly.

Summary

- The below is taken from an Automotive News ad for a Webinar.
- “The recent IBM Institute for Business Value study, released in January, shows that the dynamics of the consumer-vehicle-enterprise relationship are starting to change drastically as traditional industry boundaries disappear. Automotive enterprises must adapt to the new ways consumers access vehicles and use them in their digital lives, and fit into an increasingly complex web of transportation options.”

Summary

- “Interconnectedness is the essence of the creative disruption ahead: between consumers and automakers; between consumers and vehicles; and among traditional and non-traditional participants in the industry ecosystem. Looking toward 2025, the enterprises that welcome openness are setting the stages for success.”

Summary

- What next?
  - Keep beating the drum!
  - SAE J2922
  - ISO 204
  - NHTSA