THE MOBILE AIR CONDITIONING SOCIETY WORLDWIDE©

MACS SERVICE REPORTS

Total Vehicle Climate and Thermal Management™

By Bob Chabot, MACS Technical Correspondent

November 2016

THE VEHICLE COMMUNICATION INTERFACE REVOLUTION

New interfaces will change the nature of service repair, sooner than you think

For today's shops and technicians, Vehicle Communication Interfaces (VCIs) are essential to having the ability to perform serious repairs to modern and future vehicles — whether mobile air conditioning, related systems or otherwise. Think of them as onboard "gateways" into vehicles. The 16-pin underdash plugin port common in all modern vehicles was the first VCI. For more than 30 years it was the only gateway facilitating the transfer of data, software and other critical information between connected diagnostic tools, reprogramming devices, laptops, dongles, service repair technicians, automakers and more.

Well … At least it used to be.

Today, new highly securitized advanced VCIs are inbound, and some are scheduled for approval in late 2017, with implementation in 2018. Far too many automotive professionals don't know this tsunami is coming, how quickly change will arrive, or that these new VCIs have the potential to impact aftermarket service repair dramatically. Specifically, who gets access to the vehicle's data, software and other information and what level of access will be permitted are at stake. Need to know more?

The Quest for Control has a History of Pitting the Aftermarket vs. Automakers

History, like technology, can spiral forward. And sometimes, serendipity can intervene with history. In just a decade, the service repair industry has faced three major issues — each of them leading like individual stepping-stones to the VCI revolution. Follow this trend, and you'll begin to see how important interfaces have become:

- Who owns vehicle data? — This issue was the first major quest for control. It spawned Right-to-Repair, which began in 2001, and after millions were spent, was ultimately resolved by Massachusetts law and the subsequent 50-state Memorandum of Understanding (MoU). Then the pace picked up.
- Who owns vehicle software? — This issue began quietly in early 2012, when security-conscious automakers petitioned the U.S. Copyright Office (USCO) for sole and exclusive copyright over vehicle software, which was denied, thereby allowing the aftermarket, researchers and others continued access to vehicle software. The automakers again petitioned for full copyright in early 2015, but this time they were better prepared with written letters of support from the U.S. Environmental Protection Agency, California Air Resources Board, Automotive Service Association and others. But in September 2015, one month before the USCO decision was due, the "dieselgate" scandal broke — an illegal emissions software work-around by one of the automakers that was simultaneously petitioning for full copyright on software. The USCO again denied the automakers' petition, which can be applied for again in 2018. The lesson here: While the aftermarket, regulators and consumers easily noticed the scandal and ensuing penalties, none recognized as clearly, if at all, the larger threat that had been narrowly averted. Going forward, counting on getting lucky is not a wise strategy.
- Who controls access to vehicles? — The latest issue began just a few years ago, as the advent of telematics, connectivity, automated driving and cybersecurity gained traction. It is evident to almost all stakeholders that the underdash VCI, which had been in use since 1996, is archaic, unsecure, limited in users and troublesome. In 2013, asked by automakers and others to look at modernizing, improving and securing vehicle communications, the International Standards Organization (ISO) and the SAE International (SAE) began discussing standards and considering alternatives to the underdash SAE J1962 VCI. Some of those solutions — which feature innovative technologies, protocols and associated architectures — will soon enter the market.

Clearly, the quest for control of vehicle data is still on. If only the automakers control access, then the aftermarket, shops and technicians face formidable challenges ahead. So let's deep-dive first into current state of J2534 reprogramming and other connected tools reliant on the old J1962 VCI, then review some of the innovative alternatives and technologies being considered, and then finally look in-depth

Launch Tech USA

Figure 1: The SAE J2534 v05-00 standard provides faster reprogramming speed and improved communication capability for all J2534 devices

MACS Service Reports is the official technical publication of the Mobile Air Conditioning Society Worldwide, Inc., P.O. Box 88, Lansdale, PA 19446. The material published in *MACS Service Reports* expresses the views of the contributors and not necessarily that of MACS. Every attempt has been made to ensure the accuracy of the content of *MACS Service Reports*. MACS, however, will not be responsible for the accuracy of the information published nor will MACS Worldwide be liable in any way for injury, labor, parts or other expenses resulting from the use of information appearing in *MACS Service Reports*.

at the Extended Vehicle Concept (ExVe), a nearly completed advanced interface that, as written, gives control of access to vehicle data solely to automakers. If your business is in the automotive aftermarket, ExVe warrants your immediate attention and concern.

The New SAE J2534 Reprogramming Standard: Improved But Incomplete

In the last week of October 2015, the SAE E/E System Diagnostic Standards Committee (hence SAE Committee) published J2534 Version 05.00 (v05.00), its latest iteration, and a vast improvement over earlier versions. J2534 devices are essentially a wired, relatively insecure gateway between two different industry protocols — namely Universal Serial Bus (USB) and Controller Area Network (CAN) — which is facilitated through a simple VCI we know more commonly as the J1962 underdash connector. In short, J2534 devices are used to reprogram and reinitialize software inside various Electronic Control Units (ECUs) onboard vehicles that are connected across the various communication networks. Like scan tools, other connected diagnostic tools and dongles, J-boxes plug into the older, problematic J1962 VCI.

The new v05-00 specification follows four prior iterations and features four main components:

- J2534-1 — Defines features for a VCI device that performs software reprogramming of electronic control modules (ECMs).
- J2534-2 — Defines OEM-specific extensions for optional features and protocols that perform ECM software reprogramming so an OEM can enable reprogramming of all vehicle ECMs using a single J2534 device.
- J2534-3 — Defines compliance testing to verify that an OEM's J2534-1 VCI device meets all the requirements specified in J2534-1, to ensure reprogramming applications from OEMs will work with all compliant VCIs. Note, this specification is not yet completed.
- J2534-4 — Defines recommended practices, application requirements and needs that OEMs must disclose for Right-to-Repair (R2R) applications, such as protocols, physical layers, J1962 connector pin selection, network connections, Windows PC requirements and so forth. This specification also is not yet completed.

"The new J2534 v05.00 standard is much improved over its predecessor," explained Greg Potter, a member of the SAE Committee and also the executive manager of the Equipment and Tool Institute (ETI). He also attends ISO and numerous other industry meetings. "As is the case with other automotive tools and equipment, ETI members don't welcome or condone J2534 knockoffs; they work with both the automakers and the aftermarket, including shops, to ensure previous and now the current v05.00 standards and certification tests are met by reputable manufacturers."

The SAE Committee recognizes that automakers and aftermarket (collectively, OEMs) v05.00 device manufacturers will have to ante-up and make some modifications, which will require some reprogramming time and expense. Automakers will be impacted more than aftermarket J-box makers because their software algorithms will have to be rewritten and thoroughly tested across all models and variants to be v05.00-certified.

How will J2534 v05-00 Affect Service Repair Shops?

Automakers affirmed at a recent National Automotive Service Task Force (NASTF) meeting that writing the software reprogramming code and the scope of validation testing are indeed enormous and costly tasks. "For each Toyota model year, all the onboard control module permutations affected by v05.00 would require more than 80,000 different validation tests to cover all model year variances," explained Jill Saunders, Toyota Motor Sales' engineer responsible for Technical Information & Diagnostics.

Kurt Immekus, publications regulatory specialist for Volkswagen Group of America, agreed with Saunders, then added, "It's difficult to get a return on the substantial investment required, especially since much of the work is focused on aftermarket, rather than in-dealer, applications. There's also the challenge of adequately monetizing this investment via subsequent products and services provided to the aftermarket."

"Reputable aftermarket J2534 device manufacturers — most of them ETI members — are in favor of the new version," Potter noted. "These manufacturers say they will have to make some modifications, essentially firmware and driver updates that can be updated remotely to ensure devices already in the field can live on. This will require some reprogramming time and expense, but not the difficulty level faced by automakers, who have much more to do with their software algorithms, hardware and firmware before they are able to provide others with know-how and data via licensing or subscriptions."

"We all need to understand that for every version of J2534, validation testing has been an ongoing large-scale annual reality and process for OEMs," Potter advised. "This is because J2534 box components are constantly changing too, as new materials and innovations are introduced (e.g., improved processor chips). It's not enough for a J2534 device manufacturer to claim its new, improved device operates the same as its predecessor. They have a responsibility to their market to be certain, so they must test, validate and certify on a large scale continually. J2534 device purchasers and consumers deserve and expect no less."

The SAE Committee advised that as shop owners and technicians become more aware of the new and improved v05.00, it's important they understand it is intended to provide two significant advantages:

- Faster, factory-equivalent reprogramming speed times.
- Better communication compatibility between hardware and software for all J2534 devices, regardless of manufacturer.

"As v05.00 becomes mainstream, v05-00 certification will provide OEMs, service repair purchasers, regulators and consum-

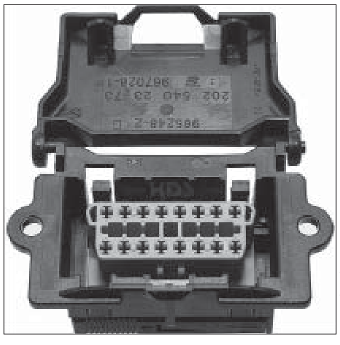

Daimler AG

Figure 2: The common J1962 underdash VCI is archaic. It's 30+ years old, insecure and is limited to one user at a time

ers with tangible evidence that a J-device is compliant,” Potter shared. “In time, the service repair industry can expect the number of different J-devices to decrease, which will also reduce the amount of annual validation testing and expense required by OEMs. In addition, depending on the architecture, technology, capabilities and packaging involved, expect J2534 devices to get smaller over time.”

Potter also identified some issues that are still outstanding from a shop perspective. “One intent of the Massachusetts law and subsequent 50-state MoU — which preceded the publication of J2534 v05.00 — was that a shop should be able to purchase one J2534 device that could be used to reprogram software on all vehicle makes and models. However, as it’s written right now, the wording of the MoU does not precisely define what a J2534 device actually is. Without clear definitions and boundaries, realizing that intent could be difficult. Any OEM can have unique proprietary J2534-2 attributes or other protocols that would require a shop to continue to have an OEM-specific J-device or accessory to reprogram its brands and models — a GM device, a Ford device, etc., similar in nature to OE-specific factory scan tools — and still comply with the MOU.”

“It’s crucial that the SAE Committee address this concern, which was also problematic with all earlier versions of J2534,” Potter emphasized. “A shop may have to own four or five J-devices or accessories to service most, but still not all, makes and models. For example, an aftermarket shop with one J2534 device today may be able to reprogram all Toyota models with a $500 Mongoose cable. However, that shop’s J-device and accessories may not be able to reprogram unique GM’s single wire CAN, Honda’s Diag-H UART and other automaker J2534-2 protocols.

“To make the MoU’s intent a marketplace reality, continued good-faith collaboration is needed by the SAE Committee to complete the J2534-3 and -4 components,” Potter added. “These will complement and dovetail with the J2534-1 and -2 elements to provide a solid foundation for improved performance, test mechanisms, protocols, legal aspects. This is the type of industry participation that benefits all — automakers, tool vendors, service repair facilities, other users and consumers alike. In addition, implementing a complete v05.00 standard will help avoid a repeat of the painful history for Right-to-Repair diagnostics. It will also simplify the lives of the shops and technicians who service and fix the vehicles automakers build.”

Is the J1962 Connector Expendable?

Once the SAE and ISO began addressing standards for new vehicle communication interfaces, OEMs began developing improved gateways for vehicles with telematics, connected, automated and ITS applications that are far more sophisticated than the J1962 connector could ever handle. These new secure vehicle communication interfaces are also capable of replacing or eliminating the J1962 VCI, should the OBD-II related regulatory mandate be lifted or updated to reflect modern realities that didn’t exist 30 years ago. In addition, these new gateway interfaces are positioned onboard the vehicle, where it safeguards entry into the vehicle’s communication network topology and ECUs from the current J1962 VCI and any future wireless entry.

In contrast to J1962, the advanced interfaces:

- Are internal and embedded into vehicle architecture. They are not plugged into.
- Cannot be as easily hacked as the underdash J1962 VCI.
- Have enough built-in intelligence and security/encryption protocols to discern whether or not users should get access to vehicle data and what level of access should be enabled.
- Can allow simultaneous access by multiple users with different purposes that can be secured, tiered, limited and authorized by the automaker and car owner — whether the connection is wireless or continues to be wired through the underdash J1962 connectors. In other words, access to vehicle data would be governed.

Of critical note here, all of the proposed new advanced interfaces would be jointly managed by automakers and the aftermarket, except one — the ExVe. Why that is problematic will soon become apparent.

“The new interfaces could also be potential game-changers for J-boxes and other connected diagnostic tools,” Potter explained. “EPA and CARB currently require the J1962 connector for OBD-II diagnostics. Just four of the 16 pins in the J1962 connector are needed for OBD-II; the rest are not. The regulators also currently require that OBD-II data only be communicated on the CAN network within vehicles. Because CAN is the least secure and most easily attacked of all onboard communication networks, that may not always be the case.”

Bottom line: Non-OBD-II data could be moved to the gateway SVI. For that matter, OBD-II data could too, at some point. Consider these three possible scenarios:

- What functionality on the J1962 VCI might be turned off by automakers, and when? — As of today, any and all functionality not mandated, such as OBD-II information, to be on the SAE J1962 connector could be removed at the discretion of any or all automakers. Being more security-conscious, any of them could remove non-OBD-II proprietary diagnostics, including remote diagnostics, from that connector and deliver it via an advanced interface instead. Dealer and aftermarket facilities in this scenario would both get data in the same manner, but current J1962 tools, J2534 boxes and other devices may no longer be viable.
- What if J1962 VCI functionality is limited or even eliminated?” — As the future rolls on and wireless connectivity to vehicles becomes standardized and more universal, EPA and CARB may well decide, “Wireless works for us,” rather than continue to support outdated insecure technology. It might take years, or it could happen sooner. But experts say more secure and functional alternatives will push everything to being done wirelessly with the vehicle. Again, should this occur, both dealer and aftermarket facilities would be on the same competitive playing field.
- What if all non-OBD-II software reprogramming fixes were delivered to both dealers and the aftermarket via OTA updates from an automaker’s centralized, secure location? — This could kill J1962 by itself. Taken to the extreme, if automakers didn’t provide any proprietary diagnostics to dealers, they arguably wouldn’t have to provide them to the aftermarket either. All that would be necessary is the diagnosis of what to replace and adjust. Think about all the tools,

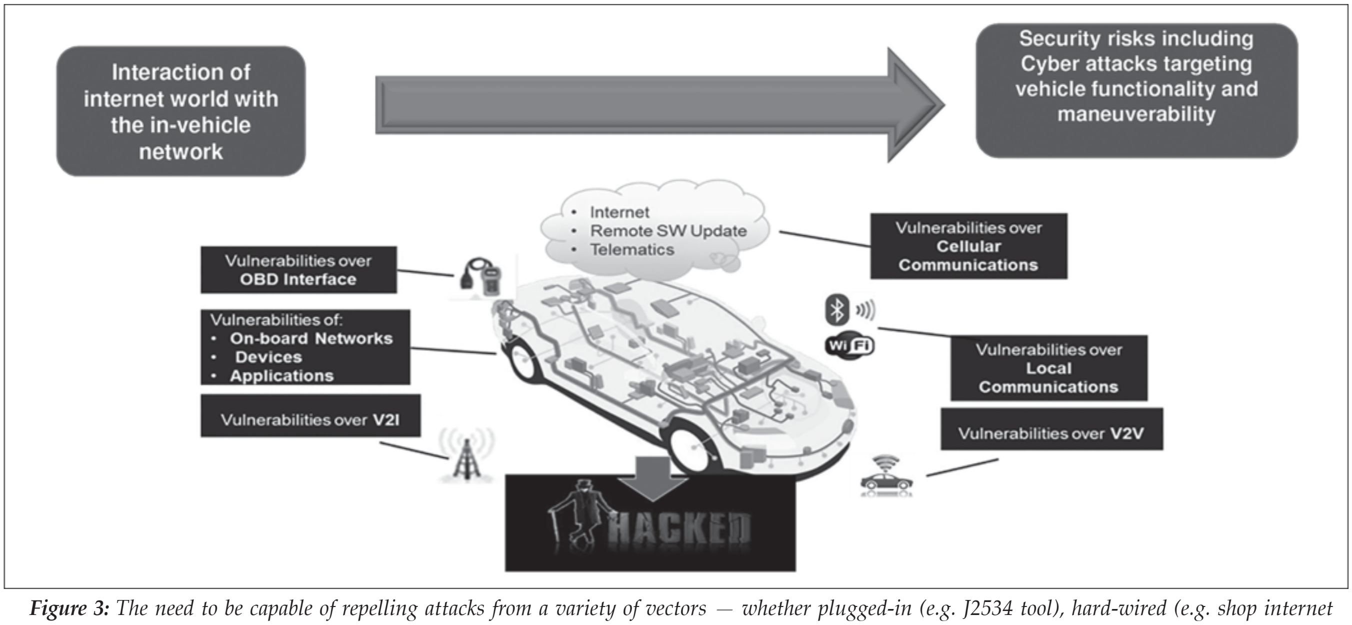
equipment, businesses and people that are on the line. Like the struggle to retain access to software at the USCO, this is a potential threat the aftermarket may not see coming either. Feeling lucky?

Time Doesn’t Wait on any Technology

As a growing industry concern, security goes well beyond J2534. Of note, both the J1962 VCI and J2534 devices are vulnerable to being hacked, according to both automaker and aftermarket experts.

While the SAE Committee expects the J2534-3 and -4 elements of v.05-00 to be adequately resolved, it is possible they won’t be. It’s also possible that other technologies emerge that replace the need for J2534 devices — or even scan and other connected diagnostic tools. That could turn the viability of the aftermarket on its ear.

“The J1962 connector as well as any electronic vehicle communication interface — a scan tool, J2534 box, laptop, dongle or some other device — are prone to attack and capable of being hacked,” shared Mohan Sethi, MAHLE Aftermarket’s head of Product Management & Business Development “These devices lack adequate built-in cybersecurity defenses. If a J2534 tool has been infected with malware, then every vehicle and device that J-box is then connected to is at risk, until the attack is remedied. In addition, the industry has, and is, developing better solutions. The buildup and rollout of telematics; connected and intelligent vehicles and transportation systems; and automated driving has begun. The industry simply cannot wait forever. It needs complete solutions now.”


Interaction of internet world with the in-vehicle network
Security risks including Cyber attacks targeting vehicle functionality and maneuverability
• Internet
• Remote SW Update
• Telematics
Vulnerabilities over Cellular Communications
Vulnerabilities over OBD Interface
Vulnerabilities of:
• On-board Networks
• Devices
• Applications
WiFi
Vulnerabilities over Local Communications
Vulnerabilities over V2I
Vulnerabilities over V2V
HACKED

Magneti Marelli S.p.A

Figure 3: *The need to be capable of repelling attacks from a variety of vectors — whether plugged-in (e.g. J2534 tool), hard-wired (e.g. shop internet service), or wireless and remote (e.g. OTA software updates) is an essential attribute of next-generation VCIs. Vehicle security must be a surety.*

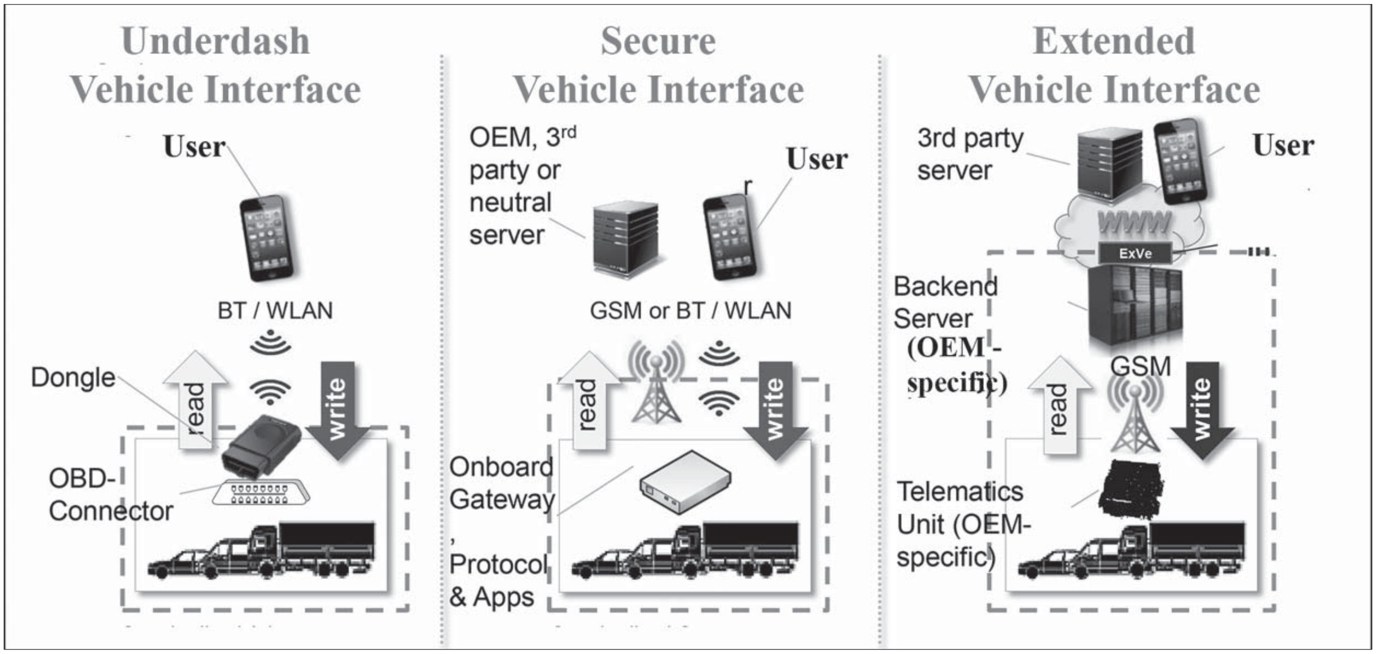
As a result, Sethi said the industry should expect how software updates are delivered to shift over time. “For example, consider the rise in use of OTA software reprogramming by automakers. OTA software updates are just another pass-through vector to the vehicle’s communication networks — different from J2534 pass-through devices — albeit wirelessly, robust and more secure. Tesla Motors already does this, using OTA software updates instead of reprogramming by using J2534 and J1962 devices. BMW AG, Daimler AG and Hyundai Motor Co. have also begun to use OTA updates on a limited to regular basis, and several other automakers are about to.”

Sethi explained the rationale. OTA updates are:

- Less expensive to develop and deploy (think of updates to your home computer).
- Free of third-party service information vendors and device manufacturers.
- Enable data to be more easily securitized by automakers and other developers.
- Independent on J2534 devices for uploading into vehicles.
- Convenient and provide improved customer use experiences.

“Ethernet in automobiles is another emerging technology that can be either wired or wireless in nature,” Potter advised. “I know of one automaker planning to introduce vehicles in MY2018 equipped with an advanced, built-in, internal gateway interface with Ethernet capabilities. Only OBD-II data will be communicated over the old J1962 VCI. The new gateway would allow Ethernet communications to securely pass through to the vehicle’s communication networks, and be converted into CAN or any other onboard vehicle communication protocols, either wirelessly or via personal computers connected to the vehicle. Like OTA updates, wireless Ethernet could eventually eliminate the need for a J2534-box when reprogramming software.”

“For the immediate future, however, Ethernet architecture lacks a clear, uniform defined global standard — the nemesis typical of emerging technologies,” he added. “What is happening in the U.S. can be at loggerheads with Europe, Asia or other markets; even global standards organizations disagree. For instance, automobile Ethernet here is predominantly two-wire based, whereas Ethernet for personal computers are four-wire


Underdash Vehicle Interface
User
BT / WLAN
Dongle
read
write
OBD-Connector
Secure Vehicle Interface
OEM, 3rd party or neutral server
User
GSM or BT / WLAN
read
write
Onboard Gateway, Protocol & Apps
Extended Vehicle Interface
3rd party server
User
WWW
ExVe
Backend Server (OEM - specific)
GSM
read
write
Telematics Unit (OEM-specific)

ETI

Figure 4: The underdash J1962 VCI (left) is little security and is easily hacked. Both the SVI model (center) was developed before the ExVe model (right). Both have stringent security protocols all users must successfully pass before being granted access to the vehicle. Note that the SVI concept specifies that the aftermarket and automakers jointly control and monitor access to vehicles. Note that unlike the SVI, ExVe specifies only automakers control and monitor access to vehicles.

or eight-wire based, which allows faster and higher data volumes to be transferred. Other automotive markets have moved beyond two-wire. We're lagging.

"The auto industry in the United States needs to get in step with what's happening here in other industries and in the rest of the world," continued Potter. "Too often, when meeting with automakers, suppliers and others about wanting access to vehicles, the one thing that is always thrown back in our faces is, 'That will be unsecure.' That's closed-minded. It's critical to go beyond our business cultures and past practices to wherever the information and know-how we need is, whether it's for Ethernet, security, encryption, artificial intelligence or other needs we have."

Potter cited two examples:

- The International Consumer Electronics Show (CES) — The Las Vegas CES is a multi-industry show where know-how has traction. Just a few years ago, no one in the automotive repair industry attended it. Yet it is where telematics, connectivity and other emerging technologies this industry now needs were already being discussed and successfully implemented years ago. Some, but not enough of stakeholders attend now to grow knowledge, expertise and relationships with IT experts from Apple, Google, Amazon, NVIDIA and other tech giants that we can leverage. They have shown the value of using open and proven industry standards and methods, rather than traditional proprietary means, to build more secure, encrypted and standardized vehicle access for all legitimate stakeholders. Simply put, doing things a dozen different ways isn't user-friendly, and often, it's confusing and less secure.
- Intelligent Transportation Systems (ITS) Plenary Meetings —Globally, the industry is headed toward managed ITS; this includes service repair shops and suppliers. Security and encryption design is being done right in the international ITS community today. This past summer, the 2016 CONVERGE meeting in Berlin showcased the new ISO 21217:2014 standard, which describes open standards communications architecture and the use of reference security protocols to safeguard ITS nodes, such as vehicles, control centers, shops and traffic signals, based on the principles of bounded, secured and managed domains. This new ISO standard is far superior to what we have domestically today. It's know-how we need.

"ETI member firms build the automotive tools, equipment, devices and third-party service repair information products that bridge automakers and service repair facilities," Potter said. "Our customers are in both groups, and we've enjoyed an open, honest collaboration with them. We realize automakers have been behind the curve regarding vehicle security and encryption, for which solutions are complicated and expensive. On the other hand, the global IT and ITS communities are well ahead of the auto industry in the areas of security and encryption. We need to use our relationship with them to grow our capability."

"That's why we've been telling automakers for a few years now: 'Get rid of your individual proprietary systems. They add unnecessary complexity to servicing vehicles, and frankly aren't as good as those developed and in use today by the ITS and IT industries.' We've urged automakers to adopt the new robust systems developed by these two communities, which use state-of-the-art security and encryption mechanisms and employ standardized but more sophisticated and secure vehicle interfaces. They work, and that serves everybody's interests. After all, we're all in the security business now."

Global Standards Organizations Are at Loggerheads Re: Advanced Interfaces

Two new vehicle communication interface concepts have taken the lead in being considered as replacements by the ISO and the SAE standards groups. One is the Vehicle Interface Methodology concept by the Society of Automotive Engineers (SAE), more commonly known as Secure Vehicle Interface (SVI). The other is the Extended Vehicle concept (ExVe), proposed by the ISO. In short:

- The Secure Vehicle Interface model has been described in detail in previous articles and presentations published by Motor Magazine, the Equipment and Tool Institute, as well as other media and organizations. At this time, the SAE supports the SVI, while it has a neutral position on ExVe. Officially, the SAE is neither for nor against ExVe, but it is not developing any associated standards for ExVe either.
- The Extended Vehicle model is under the jurisdiction of an ISO technical committee (ISO TC/22 SC31 WG6), which is managing two projects developing standards — 20077 (ExVe Methodology) and 20078 (ExVe Web Services). The ISO does not support the SVI; it isn't even neutral. ExVe is backed by Audi/VW, BMW, Fiat, Opel, PSA Peugeot Citroën, Fiat, Renault-Nissan and other ISO members. Of note, the ISO has scheduled ExVe for adoption near the end of 2017, with publication and implementation slated for early 2018.

SVI vs. ExVe: Similarities and Differences Worth Noting

Both new interface alternatives are secure, allow for multiple users simultaneously, and can integrate emerging telematics, connected and automated driving technologies. But they differ significantly in how and what level access to vehicle data, software and information is determined, controlled and monitored. In the SVI alternative, control of access is shared jointly by the aftermarket and automakers. In contrast, in the ExVe alternative, as currently written, only automakers have control of access to vehicle data, software and other information. Déjà vu?

Automakers, on an individual proprietary basis and at their sole discretion would be able to develop and implement ExVe systems that would, de facto, control all third-party access to vehicle Information — including access by the aftermarket. Whether a manufacturer of tools, equipment, parts or supplies; a service or repair professional; a vocational tech school, instructor or aftermarket trainer; regulator; or consumer — this difference is crucial and warrants your immediate attention.

Both new VCI architectures facilitate simultaneous access to data by "approved" multiple users and level of access to data being tiered to a user's bona fide "need to know," determined by each automaker. For example, an insurance company wouldn't necessarily need or get the same level of access that a service/repair technician might or that an automaker's development engineer would.

Finally, the two new proposed architectures under consideration each provide enhanced security protocols and measures. Individual onboard electronic control modules (ECUs) could continue to have their own security (each with electronic keys a vetted user would need to provide). But access to a vehicle would be routed through different master gateways.

Specifically, SVI methodology requires the gateway module to be installed internally onboard vehicles, which would use security protocols to govern access either via the underdash port, onboard telematics systems (e.g. OnStar) or other wireless communications. ExVe methodology differs by requiring gateway security measures for initial access to be located outside of the vehicle within the automaker's cloud server.

ExVe Could Shape the Future of Tools, Equipment and Vehicle Service

In essence, ExVe redefines the vehicle as we known it — a vehicle with four wheels, a few doors and an engine — into a virtual entity. The concept combines that vehicle with extensions that include a manufacturer-owned ExVe cloud server and its proprietary communications between the vehicle and server.

With this new vehicle definition, the automakers would have the option to perform all enhanced diagnostics for electronic systems via their ExVe cloud server exclusively. If exercised, the current underdash connector would only have access to legislated OBD-II emissions-testing data, but not diagnostics or repair. And likely, that would change in time.

The ExVe standards and methodology allows all electronic communications for identifying problems with vehicle components (e.g. in-vehicle network diagnostics) to be controlled by the automakers — not the vehicle owner. In particular, ExVe methodology has the potential to render the current all-makes aftermarket scan and other diagnostic tools obsolete, in addition to impacting other aftermarket products and services.

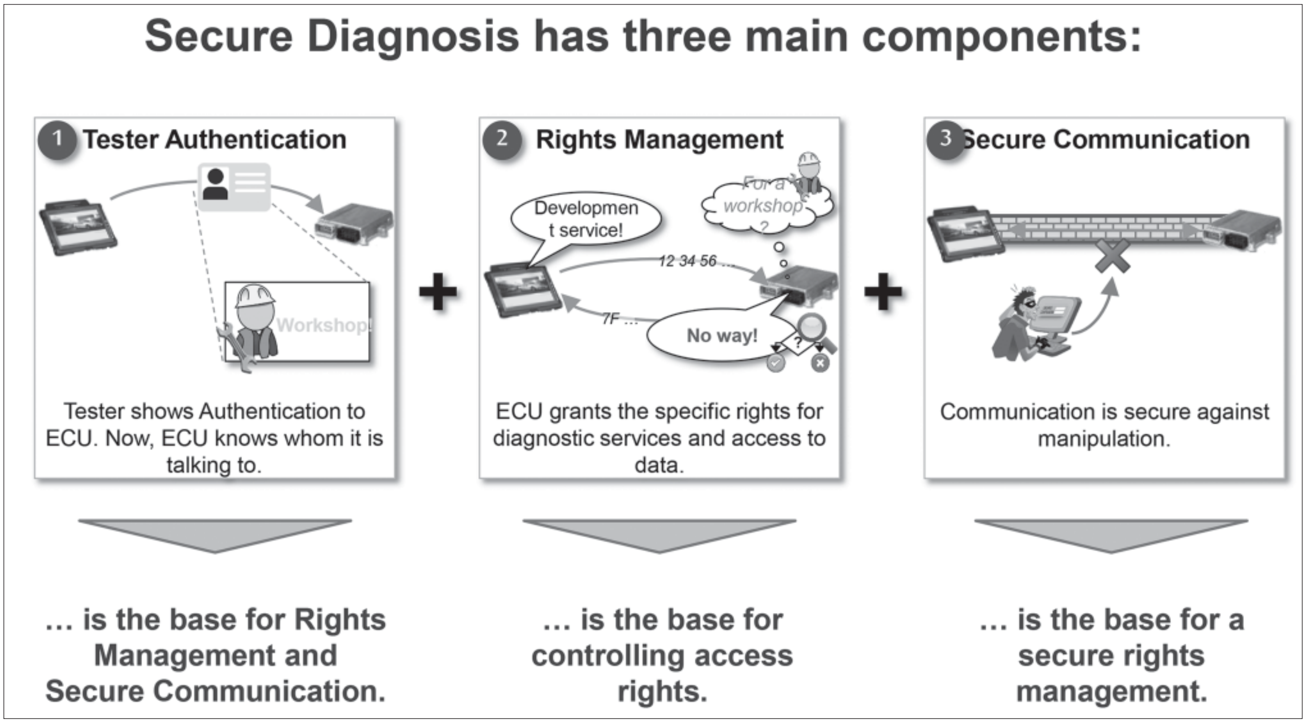
ExVe Puts the Automaker-Aftermarket Competitive Balance at a Tipping Point

Today's legislation and regulatory environment clearly requires automakers make available the same level of diagnostics as provided to their franchised dealer network for a non-discriminatory price. Without adequate safeguards that protect the aftermarket and public interest, ExVe allows only automakers to control, monitor and dish out access to vehicle data, software and information as each sees fit.

To summarize, automakers would be able to decide which third parties — including tool companies, researchers, white hat hackers, consumer advocates and others — will be granted access to vehicle service information, data and software. Secondly, ExVe would enable automakers to also limit or curtail the degree of access and use by third parties. For instance, automakers could also leverage ExVe to restrict access or limit the level of access to information. In addition, automakers could amend the current "read and write" software functionality available to the aftermarket to "read only." While these and other possible decisions may well suit an automaker's interests, they do not serve the interests of the aftermarket, consumers or the public. If all access to information is routed solely through the automakers, consumers and every aftermarket sector will be affected.

While the impact will vary between sectors, the market viability of some, such as the aftermarket scan tool market, could be compromised. Consider these examples of how certain aftermarket sectors could be impacted:

- Tool and equipment manufacturers could face losing direct



Secure Diagnosis has three main components:

1 Tester Authentication

Tester shows Authentication to ECU. Now, ECU knows whom it is talking to.

… is the base for Rights Management and Secure Communication.

2 Rights Management

ECU grants the specific rights for diagnostic services and access to data.

… is the base for controlling access rights.

3 Secure Communication

Communication is secure against manipulation.

… is the base for a secure rights management.

Concepts and Services Consulting

Figure 5: *Security is an omnipresent concern and will evolve to meet new challenges as they arrive. So expect encryption protocols and other security measures to become the norm, from parts to tools to vehicle to the transportation systems they operate within.*

sales of multiple-make, multiple-model scan tools, J2534 reprogramming devices and other diagnostic equipment/tools, the effects of which would cascade into other segments. ExVe could potentially enable automakers to absorb the aftermarket's entire scan tool business, let alone other diagnostic elements.

- Parts manufacturers and resellers could be required to build-in manufacturer-specific security key and seed protocols into replacement parts before the ExVe cloud connection "allows" the part to operate on the vehicle.
- Independent service and repair shops and their technicians may see competitiveness eroded, their cost of doing business increase due to added ExVe fees and other impacts, such as new security-related PC requirements, shop cybersecurity prerequisites, or other measures before getting ExVe access.
- Vocational schools, instructors and aftermarket trainers, who already deal with constrained and meager resources, could face increased costs for access to the essential resources and information needed to teach aspiring and upgrade current technicians' troubleshooting and diagnostic competencies.
- Consumer's choice of service facility and repair affordability may be eroded. Many vehicles in operation now are 11 to 12 years old, with each new model year bringing more electronics and software. ExVe standards do not include any surety safeguards to prevent an automaker arbitrarily discontinuing support for certain older vehicle models, akin to computer companies that end support of older operating systems. What assurance do consumers have that their older vehicles will continue to be safely and fully serviced?

Show Me the Money!

Huge revenue dollars are at stake. Controlling access to vehicle data via ExVe provides automakers with a means to gain and monetize some of the aftermarket's traditional core business. A recent survey by the National Automobile Dealers Association (NADA) demonstrates this. NADA reported the total value of the U.S. automotive service business is $310 billion annually —$84 billion provided by franchised dealerships and the remaining $226 billion provided by the aftermarket or the do-it-yourself crowd.

Studies by market research firms support the NADA statistics. First Research reports U.S. automotive maintenance services alone, performed by more than 160,000 establishments, generate annual revenue of $100 billion and gross profit margins in the range of 25+ percent. Markets & Markets pegged the current market value of the aftermarket scan tool business at more than $1 billion annually, and projected it to reach $1.8 billion by 2018. Potter also shared that when canvassed, several of ETI's largest diagnostic tool manufacturers agreed with these valuations.

Capturing some (if not all) of the aftermarket's value generators represents a huge opportunity for automakers. Control of access to data, software and other information via ExVe would provide the potential for automakers to gain and monetize some of the aftermarket's traditional core business. Clearly, the aftermarket doesn't find that appealing.

Collaboration, Regulation or Legislation — Pick Any Two

History has shown us that collaboration between automakers and the aftermarket has often been able to successfully resolve conflicts and competitive differences to best serve consumers and the public interest. But there have also been instances where legislation, regulation or another pathway was required.

For example, legislation prompted the 2013 Massachusetts Memorandum of Understanding, which ended the prolonged "Right to Repair" debate within the industry. The recent U.S. Copyright Office (USCO) decisions were regulatory, and upheld the aftermarket's ability to serve as a public watchdog.

Since ExVe was first proposed, aftermarket members on the ISO ExVe Committees have repeatedly requested clarifications and explanations from automaker members and other proponents. These concerns pertain to access to data, software and information; what limits if any would be imposed; costs, fees and other financial impacts; consumer safeguards; privacy; and others. Rather than voluntarily providing answers to these requests, proponents have stonewalled the aftermarket. Meanwhile, the ISO's adoption deadline for ExVe is now less than a year away. Time is of the essence.

The aftermarket has continually shown support for the concept of automakers offering access to their web services for many viable use cases at a reasonable, nondiscriminatory fee. A positive example is GM offering aftermarket access to "On-Star" data via a contracted vendor. However, current relations between the aftermarket vehicle care industry and some vehicle manufacturers validates concern whether all manufacturers will make their proprietary ExVe system efficient, viable and affordable for aftermarket entities. It isn't without precedence and has become a growing point of contention.

Certainly, many automakers embrace the aftermarket and understand what an important role the aftermarket plays in keeping customers loyal to vehicle brands. But there are also some automakers that view the aftermarket as competitors, and have been difficult and expensive to negotiate with until the threat of, or actual, litigation, legislation or regulation has forced a mandated solution.

Nonetheless, aftermarket members of the ISO remain hopeful for a mutual and voluntary collaborative resolution of ExVe concerns. That of course requires an active, in-good-faith dialogue between ExVe proponents and the aftermarket. Although time is short, it's the aftermarket's preferred pathway; it's also the least costly way for the industry to move forward together.

It Takes Two to Tango

At the ExVe meeting held in June 2016 in Gothenburg, Sweden, the Automobile Club of Germany (ADAC), an aftermarket member of ISO, suggested a modified ExVe model as a "fair and reasonable" path forward. The essential difference from the original model put forward by ExVe proponents was a change from the single cloud server being controlled by automakers only, to a neutral shared cloud server in joint control of automakers and the aftermarket.

Essentially:

- Vehicle data, software and information would be distributed by automakers to their certified partners, while the aftermarket would distribute the same (in quality and scope) to its authorized independent workshops, at reasonable and non-discriminatory cost and conditions.
- This suggested ExVe alternative is similar in nature to the SVI model, with the exception that the requests for access to vehicles would start at the cloud server, not at the master gateway inside the vehicle.
- In addition, vehicle owners would (1) control data transfer to the service provider(s) of their choice; and (2) have the right to know what vehicle data is transferred to any other entity.

The automaker-dominated ISO ExVe Committee rejected the ADAC's proposal outright, with little meaningful explanation or discussion. Aftermarket members then reiterated earlier requests for clarifications, explanations and details with little response, Aftermarket members then formally requested a Risk Analysis. Within the ISO, this formal request requires a formal written response at a future ISO meeting.

The ADAC's suggested modification of ExVe is a step in the right direction. Without a workable compromise, it is untenable for the aftermarket to accept ExVe, as currently proposed. The risks to the aftermarket business are just too high. The aftermarket hopes the Risk Analysis provides the basis to continue collaborating toward a voluntary, nonlitigious ExVe solution that works for the entire industry. But if the Risk Analysis negates a workable ExVe compromise being reached, expect the aftermarket to choose a less collaborative path.

Simply put, the aftermarket has too much invested to not advocate on behalf of itself, the rest of the industry, consumers and the general public. History has shown us that while the evolution of vehicle data and communication interfaces has put the aftermarket and automakers at loggerheads before, ultimately workable solutions were reached. For example, the "Who owns the data?" issue spawned right-to-repair, which was settled by the formal MoU agreement. The more recent "Who owns the software?" ruling by the U.S. Copyright Office, upheld mutual access to vehicle software.

"Who controls access to vehicles?" is the latest challenge. Whether the automakers now supporting ExVe, as it's currently written, will compromise remains to be seen. But be clear: While the aftermarket supports a collaborative "win-win" solution over the "nobody wins" alternative, it will not be shut out. ■

MACS Service Reports is published monthly by the Mobile Air Conditioning Society Worldwide. It is distributed to members of MACS Worldwide and is intended for the educational use of members of the automotive air conditioning service and repair industry. Suggestions for articles will be considered for publication, however, MACS Worldwide reserves the right to choose and edit all submissions.

Unless otherwise noted, all photos/art by author.

Editors: Elvis Hoffpauir, Steve Schaeber
Production Designer: Laina Forcey
Manager of Service Training: Steve Schaeber

Mobile Air Conditioning Society Worldwide
P.O. Box 88, Lansdale, PA 19446
Phone: (215) 631-7020 • Fax: (215) 631-7017
Email: membership@macsw.org • Website: www.macsw.org

MACS Service Reports Quiz #MSR102016

Based on October 2016 issue of MACS Service Reports.
This test must be received within 30 days in order to be processed.
Fill out the information at left, and circle the correct answer for each question in the box below.

Mail or fax your completed test to: MACS Worldwide, P.O. Box 88, Lansdale, PA 19446; Fax: (215) 631-7017

Your Name: ______________________________

Company Name: ___________________________

Position/Title: ___________________________

Address: ________________________________

City: ___________________________________

State/Zip: _______________________________

Day Phone: (   ) ______________________

Fax: ____________________________________

E-mail: __________________________________

Is this your first MSR Test? (Circle one)
YES NO

All members of MACS Worldwide may copy and distribute copies of this test to their company employees. The MACS Service Reports Training Program is only available to members of MACS and their company employees.

Certificate of Achievement - If you pass 8 tests each year (Aug. - Aug.), scoring at least 80% on each test, you qualify for a Certificate of Achievement. If you qualify, MACS Worldwide will notify you by e-mail and you may order your Certificate of Achievement for $10.00.

Rec'd:

Score:

Init.:

1.	A	B	C	D
2.	A	B	C	D
3.	A	B	C	D
4.	A	B	C	D
5.	A	B	C	D
6.	A	B	C	D
7.	A	B	C	D
8.	A	B	C	D
9.	A	B	C	D
10.	A	B	C	D

1. A vehicle in the shop for an A/C repair needs to be recharged, but the underhood label is missing. Checking service information shows: "See underhood decal." Technician A says to call a local dealer and make the simple check. Technician B says to check the following year's service information. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B

2. A combination cooler is one which joins two heat exchangers stacked vertically in the front end cooling module "sandwich" that's headed by the A/C condenser in front and the radiator in back.

a. True
b. False

3.Remote air conditioning is a feature on many vehicles, including certain plug-in hybrids. To activate the Prius system, the following conditions must hold:

a. Vehicle power off & transmission in park
b. Doors closed and locked, and hood closed
c. Adequate battery capacity to run the A/C for about 10 minutes and still start the engine
d. All of the above

4. The leaky A/C system in a 2004 Mercedes E-Class has just been repaired with a new dryer, evacuation and recharge, but a manufacturer-specific code (P1999) is preventing compressor clutch engagement. Technician A says that a generic OBD scan tool will not likely be able to clear this code. Technician B says that the OEM scan tool can be used to check for and clear manufacturer-specific codes. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B

5. Technician A says that the manual HVAC system in the 2015 GMC Canyon uses a push-pull control cable for mode and temperature door operation. Technician B says that the best way to begin any job is by asking the customer about the vehicle's history. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B

6. A 2000 Nissan Xterra's compressor runs for about 20 minutes, then turns off. The diagram shows this (these) sensor(s) as possible cause(s):

a. Evaporator Temperature Sensor
b. Refrigerant Pressure Sensor on the Condenser
c. Triple Pressure Switch/Sensor
d. All of the above

7. Before performing A/C system repairs it's always a good idea to check for codes and TSBs first. Software updates are becoming increasingly more important in addressing A/C system performance and operational issues.

a. True
b. False

8. Technician A says that the on-board diagnostics on a 1999 Jeep Grand Cherokee can be accessed by pressing and holding, then releasing the A/C and Recirc buttons on the A/C control panel, where any trouble codes will be displayed. Technician B says that active (vs. historical) codes are indicated (if they are immediately logged) when the ignition is turned on, indicated by an "ER" in the right side temperature display. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B

9. Technician A says that many Chrysler products with dual zone Automatic Temperature Control have a pair of infrared temperature sensors built into the center of the HVAC control head between the temperature control knobs. Technician B says that these sensors are not repairable, but can be replaced individually with detail parts widely available in the aftermarket. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B

10. Technician A says that some HVAC case actuators can encounter a problem if you try to test the system without installing them, as they lose alignment when they operate outside their position in the case. Technician B says that with a dislodged blower speed control there's the possibility of heat damage to the case and / or module. Who is correct?

a. Technician A only
b. Technician B only
c. Both Technicians A and B
d. Neither Technician A or B