“Penny, Your Check Engine Light is On,” or How On-Board Diagnostics (OBD) Principles Can Improve Military Vehicles - Rob Weiss, CEO & President, Gearhead Vet Enterprises LLC

A reoccurring theme in the nerd-tastic situation comedy, Big Bang Theory, is every cast member noticing the Check Engine Light (AKA Malfunction Indicator Lamp, or MIL) is always on in Penny’s car. Like many drivers today, Penny continues to ignore the light until bad things happen. How is this relevant to the OMFV, Stryker, or HETS? While they don’t have a MIL or exhaust catalytic converters like civilian vehicles OBD is about early warning for **all** things that can go wrong with a vehicle’s powertrain.

Applying the principles of OBD, and the related Service Information Requirements (SIR) to military vehicles will enhance mission readiness. A military tactical vehicle and the civilian line haul truck, 4x4 pickup, or delivery driver have many of the same required functionality:

1. It needs to perform its mission dependably and robustly in the presences of noise factors
2. The diagnostic system should automatically store pass/fail status data, and indicate when a still-passing system is trending toward failure
3. It needs to keep operating once a fail condition exists, and give operator maximum warning while preserving sufficient usable function until it can be repaired
4. The diagnostic system must pinpoint the fault precisely, with a minimum of false failure (Type I error), or false passing (Type II error) decisions
5. The diagnostic system should pinpoint the failure down to a line replaceable unit (LRU), and by and large, should not depend on the operator, an external procedure, or a fancy off-board tool to make the correct diagnosis. As one OBD certifier used to say, “It’s called ON-Board, not OFF-Board, Diagnostics.”
6. The service documentation must be clearly written to enable the quickest possible repair, and any lessons learned/updates must be clearly communicated.

In my 20 years of developing, validating, certifying, and verifying OBD systems at four different Original Equipment Manufacturers (OEMs) and two Tier 1 Suppliers, I have come to learn OBD is really a systems integration discipline. Because one must understand the complete powertrain and interactions with related subsystems, e.g., Heating Ventilation and Cooling (HVAC), chassis, fire control (for military), etc., to have an effective OBD system.

The Diagnostics function must be involved at every stage of Vehicle design, not be an afterthought at the end of a development program

Some OBD-relevant design features must be approved in advance of hardware freeze on a vehicle program; many need to be approved before software freeze. Diagnostic design goes hand in glove with service and maintainability. In fact, aiding rapid repair of a malfunctioning vehicle was the impetus behind OBD in the first place.

Emission standards and certification are about a vehicle that is working to design specifications. OBD is there when something goes wrong.

OBD Hierarchy

All powertrain-related inputs and outputs (I/O) for an Engine, Transmission, or Powertrain Control Module (ECM/TCM/PCM), should be diagnosed. This includes both hardwired I/O and inputs coming over the powertrain backbone from other modules. Diagnostics cascade from basic to complex. There are three levels of monitoring in a typical OBD hierarchy: Circuit/out-of-range (OOR) faults, performance/rationality faults, and system monitors. There also service-only diagnostics.

- Circuit monitors are the simplest and the fastest, with no entry conditions other than key being on, and take 5-10 seconds to make a pass/fail decision. For the most part they run as soon as the control system is powered up and continuously
- Performance monitors are typically once-per-trip, especially temperature-based monitors that required a stable, ambient environment. Some may run multiple times during a drive. They take longer to run (5-10 minutes, on average), and the circuit diagnostics of the monitored input must pass or the performance monitor is enabled, i.e., to check an in-range signal, it must first be in-range.
    - My Chevrolet Volt patent for a cold-start temperature performance monitor individually compared each temperature sensor in the hybrid system (power inverter phase and motor temperature thermistors) to an average of engine coolant and transmission fluid temperatures sensor outputs. Previous monitors of this type were round-robin approaches where the hybrid system temperature sensors were each compared internally to the average of all the sensors. The upside of this approach is it did not depend on external engine sensors from other powertrain modules coming over a network. The downsides were: 1) if more than one sensor (out of four, in the base design) was skewed in-range the diagnostic fell apart, and 2) every sensor had to be present on every vehicle using this algorithm since the inputs were hard-coded in software. My approach was modular. Since the compare was to external independent sensors, it could work with a variety of temperature sensor configurations. In other vehicles, for example, there might be a virtual, not physical, electric motor thermistor. Or, a cheaper application might only have thermistors on two of the three inverter phases. The calibrator could tune the diagnostic to work with whatever sensors were present, which made it more useful for a variety of vehicles, not just one.
- The system level monitors often require multiple inputs, as well as actuators to run. These take the longest, sometimes across multiple key cycles, with the most complex entry conditions. A system monitor, or complex rationality, that makes a fail decision before all the supporting diagnostics have made their respective decisions will often lead to an incorrect repair. It makes its decision based on garbage data.

When a civilian car returns with an unaddressed issue, the technician often starts changing out random parts just to get the car fixed so the customer doesn't file a 'lemon law' complaint. This is the 'parts cannon' approach and is not recommended.

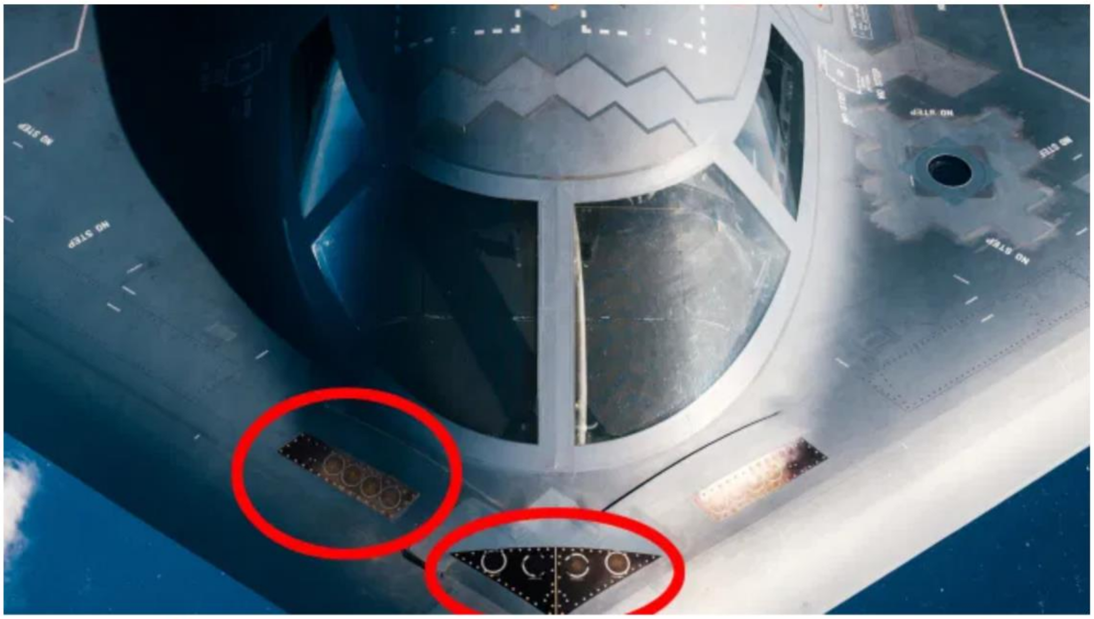
- Service-only diagnostics are designed to aid the technician in finding root cause and avoid the 'parts cannon.' They can also be used to indicate aggressive operation, e.g., multiple RPM limiter actuations. Sometimes a 'clunk' or other transient can appear like a mechanical fault to the operator when it really is a controls fault. And when there is no fault code present, the technician is left guessing.
- Another diagnostic I helped design was a battery system performance monitor. Hybrid vehicles have regenerative braking, i.e., braking resulting from charging the electric drive motor during

deceleration. Regenerative braking is blended with standard friction brakes to provide a smooth stop. However, an abrupt reduction to regenerative braking effort due to conditions within the hybrid system, e.g., charge current too high, can cause a sudden reduction in braking effort which can be disconcerting to the driver. The transient can feel like a mechanical brake or transmission problem, e.g., rough downshift. My team designed a service diagnostic that pointed to a normal hybrid battery protection routine, and thus avoided needless brake and transmission repairs.

Real World Examples

*February 23, 2008 B-2 Spirit "Spirit of Kansas" bomber (S/N: 89-0127, Air Vehicle 12) crash at Andersen Air Force Base (AFB), Guam.

The B-2 "Spirit" fleet is based at Whiteman AFB in Missouri, but often deploy to forward locations all over the world. Conventional aircraft have multiple "pitot" probes and vanes to gather air data. To preserve the stealth characteristics of the flying wing, air data is generated from an array of 24 flush Port Transducer Units (PTUs) near the nose of the aircraft (see picture). On this day a heavy rainstorm had occurred and humid conditions were present on the Pacific island, filling three of the 24 PTUs with moisture. This caused their pressure data to significantly differ from the other 21 sensors, at a much larger delta than would normally be associated with sensor-sensor variation. This delta triggered an air data recalibration procedure. The procedure was performed and the new bias offsets were stored in the Flight Control System (FCS) non-volatile RAM (NVRAM). The problem is the air data calibration procedure 'learned' bad data for the three PTUs in question, and no in-range diagnostic was present to flag the gross discrepancy (the air data recalibration procedure is triggered when any sensor is more than +/- 0.05" Hg away from the array average. The three PTUs in this case varied by as much as -0.262" Hg from the average).



A close-up shot of the B-2 during AAR (Air to Air Refueling) shows the air data ports of the stealth bomber. (Original image: Staff Sgt. Iordan Castelan).

An unofficial procedure, known by some maintainers but not others, was to turn on heating elements on startup PRIOR to performing the air data calibration procedure to avoid learning 'bad' offsets. Had the maintenance team done this, the three sensors' output would have likely come into agreement with the others, and recalibration would not have been necessary. The pre-heat step was not documented in an official Technical Order. The so-called pitot heat is designed to melt ice in very cold temperatures, not dry out condensation on the ground. Leaving the heater on too long on the ground would damage both the PTU assembly and the surrounding stealth surface coating. Thus the aircrews were not supposed to turn on the heat until just before takeoff.

When the heaters were activated, the three PTUs went back to normal readings, but were now providing significantly different output on takeoff because of the moisture-based incorrect offsets. Being an inherently unstable, fly-by-wire flight control system, the control inputs are made automatically based on pilot and environmental inputs. During takeoff rollout, a Yellow Master caution light indicated the air data system had some discrepancies but showed green status by the time the copilot examined the FCS screens. Since the caution was yellow, not red (which would have triggered an immediate abort), it went out during rollout indicating a properly operating FCS, and the aircraft had exceeded 100 knots indicated airspeed (KIAS), the crew continued the takeoff roll. The pilot rotated the nose 12 actual knots slower than required, and 1,450 shorter roll than normal. The FCS detected an erroneous nose down attitude, and thus commanded a sharp 1.5g pitchup correction upon takeoff. The aircraft was flying too slow and went into an unrecoverable stall shortly after takeoff. The crew could not get the nose lowered in time and ejected when the left wingtip struck the runway. Several things went wrong here:

- The preflight air data recalibration procedure was incomplete
- There was no apparent offset/bias rationality check; system allowed gross offset to recalibrate. A fault code for gross offset/bias condition should have been set, and the PTU recalibration procedure should have been disabled.
- Contributing factors: The indicated airspeed being 12 knots higher than actual at rotate, or 9% high, 1) shortened the 100 knot go-no go decision point, and 2) shortened the takeoff roll by 1,450 feet. The crew did not cross check the actual takeoff roll from distance remaining placards, which were present, to known takeoff distances for that location.
- A topic for future investigation would be how did three out of 24 skewed sensors have such an outsized effect on the FCS performance? It would seem these three, known as "Gust Alleviation PTUs," may have had a greater weight than other PTUs on airspeed, angle of attack (AOA) and other key calculations. If so a Design FMEA (DFMEA) should have highlighted this effect. Also, another point for investigation would be if these three sensors were more susceptible to moisture intrusion/collection than other PTUs on the wing/body.
- Three of four air data computers have to agree for the FCS system to be valid. Momentary disagreement between the FCS computers likely generated the Yellow caution lamp. But then the lamp extinguished. What most likely occurred is at least three computers agreed, <u>but all four were basing their calculations on the same skewed PTU inputs</u>. So the calculations were not truly independent. This can happen in the automotive world as well. Do your analog inputs have independent analog-to-digital (A2D) converters, or do they share a central A2D logic circuit? Are they discrete inputs, or are they transmitted over a network bus? Are the wiring

run lengths within the sensor specification, and are they properly routed and shielded? A thorough DFMEA will identify potential issues here.

- Given the aircraft system age, corporate knowledge regarding the effect of the PTU array and AIRDATA recalibrations were not fully understood. Wing personnel believed the AIRDATA recalibration procedure was essentially a glorified version the aforementioned altimeter reset, when in reality, "the FCS uses sensed air pressure from the PTUs…to calculate aircraft airspeed, angle of attack (AOA), angle of sideslip (AOS), and altitude…"

Why does your $40,000 SUV have more robust diagnostics than an irreplaceable $1.4b strategic aircraft or a multi-million dollar ground combat vehicle?

1. Every input sensor is required to be continuously monitored for circuit failure and at least once per driving cycle for full in-range failure conditions. Modern vehicles have pressure sensors that adapt and correct based on comparisons to other pressure sensors at startup, but also have diagnostics that set a fault if the measured offset exceeds a diagnostic threshold.
2. Every input needs to be assessed for what level of action needs to be taken in case of a failure. So-called 'default actions' can be as mild as shunting to another backup sensor or calculated value or can be as major as shutting the powertrain down, depending on the failure severity.
3. The MIL illuminates to notify the driver, but the diagnostic system takes the default action automatically.

*Ground Vehicle Service and Repair. Army Managers at this year's Michigan Defense Expo (MDEX2020) revealed an Army study that combat support vehicles' engine performance varied up to +/- 70 horsepower from specification for multiple reasons:

- Mechanics swapped engine/powertrain control modules (ECM/PCMs) among similar vehicles to keep them running, even though the software and calibrations do not match the installed vehicle
- Unauthorized ECM/PCM modifications from off-base vendors that improve engine power output

Modern powertrains and suspensions are designed as an interdependent system. Significantly changing one performance parameter without a comprehensive system analysis leads to increased emissions and reduced durability. Increasing the engine power sounds great, but then the transmission or transfer case torque capacity may be exceeded, leading to part failure. Running the wrong engine map can clog exhaust manifolds with soot or put increased load on turbochargers.

In the civilian world this is called 'tampering.' To combat this each calibration release has a part number-checksum combination, called a Calibration Identifier and Calibration Verification Number (CAL ID/CVN) pair. Once each quarter, every automaker sends a list of valid released CAL ID/CVN pairs to government agencies. When vehicles come in for annual registration checks the CAL ID/CVN transmitted by the vehicle is compared to a list of valid pairs submitted by manufacturer. An aftermarket tuner can ensure the CAL ID is the same as before, but if any byte in the ECM memory map is altered, the CVN is also altered. This process detects intentional tampering as well as manufacturer mistakes, which do happen. Running changes do not occur in the military as often as they do in the civilian world, so the expected CALID/CVN pair for the engine and transmission control modules (ECM/TCM) can be written to a central Body Control Module during production, updated during a valid upgrade, and used to detect invalid changes.

Full environmental validation is critical

Typical automotive development programs develop and validate in “four corners” environmental conditions; extreme heat, cold, altitude, and humidity. In one circumstance during -40 Deg Celsius winter testing, I had to modify a diagnostic threshold due to transmission fluid starting to gel and causing a startup diagnostic to false fail. The effects of the humid/rain condition B-2 crews encountered during Guam deployments were not well understood by factory and Whiteman AFB staff, and previous lessons learned were not communicated. At Whiteman, the aircraft are all parked in hangars, out of the elements. When they deploy, they are parked outside on the ramp in most cases.

Predictive Maintenance

Another key consideration today is predictive maintenance. For those military vehicles and engines that have civilian applications, the approach is typically to remove the unneeded aftertreatment components and disable any diagnostics associated with them. But that is not the only thing omitted in the military application. Referring back to the early servicing issues with disparate approaches, there is now a standardized list of data items that must be made available to all so-called generic scan tools like the ones that can be purchased at any auto parts store. These are called ‘legislated diagnostics’ and they are defined by OBD regulations supported by a Society of Automotive Engineers (SAE) Standard so every vehicle has the same baseline of repair data available. This set of data has very little in the way of predictive capability. It stores codes and displays real time values of a defined number of data items. It stores one “freeze frame” snapshot of data for a single fault. It tells the user if a diagnostic has failed but gives no indication of a passing diagnostic that’s on its way to failure.

Existing Enhanced Diagnostics Have Predictive Maintenance Features for DoD Vehicles in Many Cases

Enhanced diagnostics are also referred to as service diagnostics, or manufacturer-specific diagnostics. A generic scan tool will not have access to these extra features. There are also service fault codes that a generic scan tool can display but will not have any further information, such as description. Enhanced diagnostics offer such things as: Status bytes for each fault code, multiple freeze frame captures with much more data than a legislated freeze frame, ability to reprogram the ECU, and conduct specialty service bay operations. Many OEMs install fault code status counters that indicate how close a diagnostic is to failing. These are stored in Non-volatile Random Access Memory (NVRAM), or electronically erasable read-only memory (EEPROM), which are the most persistent memory types. Disconnecting power does not erase the memory. When compared to baseline, the peak fail count is rewritten whenever exceeded by a higher number. If the baseline fail count is near zero, and the internal max counter is one tick away from failing, the technician should know that. In the civilian world, manufacturers are required to make online troubleshooting information available to independent repair shops in a reasonably priced subscription fee structure. The tools necessary to access the enhanced diagnostic information, along with any required training are available for purchase, again for ‘reasonable’ fees (although even ‘reasonably’ priced tools get very expensive).

From my conversations with both Army Program Managers and industry suppliers, many times the manufacturer is only obligated by contract to supply the ‘legislated’ or ‘basic’ diagnostic capability. The ECU may have the ‘enhanced’ information available, but the military technician cannot access it.

Summary and Recommendations:

- Involve Diagnostics Specialists at the Concept Design Stage, and at every major milestone review stage/gate
- Ensure the diagnostics requirements are well understood and clearly communicated to suppliers
- If the vehicle and/or engine is a military variant of a civilian vehicle, supplier capability presentation should detail existing enhanced diagnostics capability used by the supplier’s civilian service network
- A comprehensive System Design Failure Modes and Effects Analysis (DFMEA) will identify the fault and default states that require potentially additional effort. These are the 9 or 10 severity failure modes, and the high Risk Priority Number (RPN) fail modes that indicate more remediation and detection capability may need to be added
- Ensure the ECU has sufficient RAM and ROM space for diagnostic-related algorithms, particularly NVRAM and EEPROM, to capture all the predictive maintenance-related trackers
- Robust Diagnostic validation at all levels of the System “V”: Software, subsystem, and system. Too often a fault is validated just by a simulation bit flip, versus validating the threshold is achievable, and the pass/fail mechanism works correctly. I have seen many instances where software issues cause a counter to clip or reset, and the fault never matures

The person or group writing the Service Information and Troubleshooting guide must have a thorough understanding of all the fault codes and troubleshooting routines. The service information should effectively translate engineering-level diagnostic descriptions into easily understandable procedures. Along with this a robust change control system and method to updated service information needs to be developed.

OBD principles are really system integration tools, since the emission/diagnostic system crosses multiple ECUs, vehicle networks, and hardware. Proper application of the OBD and Six Sigma disciplines can uncover nested software and hardware issues, maximize robustness and improve in-field performance.

GEARHEAD VET

https://gearheadvet.com

(586) 601-4286

Sources Links:

https://theaviationist.com/2019/09/03/this-close-up-photograph-of-the-b-2-spirit-provides-a-fantastic-view-on-the-stealth-bombers-air-data-ports/

https://en.wikipedia.org/wiki/Northrop_Grumman_B-2_Spirit

https://www.stripes.com/news/report-faults-computer-in-guam-b-2-crash-1.79781

http://www.glennpew.com/Special/B2Facts.pdf

https://sma.nasa.gov/docs/default-source/safety-messages/safetymessage-2009-01-01-usafb2mishap.pdf?sfvrsn=d3a91ef8_4

https://www.af.mil/News/Article-Display/Article/123360/b-2-accident-report-released/