2017 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
AUTONOMOUS GROUND SYSTEMS (AGS) TECHNICAL SESSION
AUGUST 8-10, 2017 - NOVI, MICHIGAN

Automotive Smart Vehicles & Functional Safety Applied to DoD Ground Vehicles

David A. LaRue: PhD
Sr. Technical Specialist
FEV North America
Auburn Hills, MI

Tom Tasky
Director Electronic
FEV North America
Auburn Hills, MI

Stephan Tarnutzer
VP Electronics
FEV North America
Auburn Hills, MI

Jerry Lane
Great Lakes Systems & Technology LLC
Macomb, MI

ABSTRACT

The application of advanced FEV Automotive Smart Vehicle© methods and technologies while maintaining functional safety compliance and how it applies to similar features, requirements and capabilities across the fleet of DoD combat and tactical vehicles will be discussed. The requirement of technologies for DoD autonomous ground vehicle including leader follower, automated convoy operations, and intelligent applique kit' are common to those specified in the automotive industries. Intelligent vehicles can be advanced and implemented in an expeditious manner through FEV Smart Vehicle technologies, techniques and methodologies while maintain compliance to required functional safety. The application and impact of ISO 26262 (2011) as well as Mil-Std. 882(E) to the implementation of the advanced technologies and techniques in support of full operational vehicle autonomy can hinder development. Leveraging the FEV Automotive Smart Vehicle reduces the time and cost for safety compliant implementation of these advanced technologies and techniques even where VI and AI strategies are required through the optimization of system and sensor fusion of ISO safety certified components and systems. DoD Ground Vehicles can leverage this evolution of vehicle intelligence, autonomy and safety normally only supportive of the automobile industry.

INTRODUCTION

FEV Smart Vehicle© is a method and process developed by FEV and includes the design, development and implementation of technologies for Infotainment, Telematics, ADAS (Advanced Driving Automated System) and AD (Autonomous Driving) technologies and techniques while maintain compliance to required functional safety standards as well as cyber security challenges. Infotainment systems are becoming the central and operational communication hub in many vehicle designs.

These hubs support numerous communication protocols such as CAN (Controller Area Network), LIN (Local Interconnect Network), Automotive Ethernet, FlexRray, MOST (Media Oriented Systems Transport), SPI (Serial Peripheral Interface), SCI (Serial Communication Interface), UART (Universal Asynchronous Receiver/Transmitted), and USB. It also includes various wireless protocols such as LTE (Long Term Evolution) and DSRC (Dedicated Short Range Communication) Wi-Fi (Wireless Fidelity), NFC (Near Field Communication, GSM (Global System for Mobile), CDMA (Code Division Multiple Access), Bluetooth as well as other RF (Radio Frequency) type communication over an almost infinite range of frequencies in support of Cloud Connectivity based applications as well as FOTA (Flash Over The Air) all while supporting Cyber Security through various means such as encryption. In addition to the technologies/techniques of AD operation and the communication protocols supporting these operations, FEV Smart Vehicle also supports AI (Artificial Intelligence) and VI (Virtual Intelligence) strategies, while maintaining compliance to various safety standards (e.g. ISO26262; 2011, Mil Std. 882 (E), IEC 61508, edition 2; 2010)\

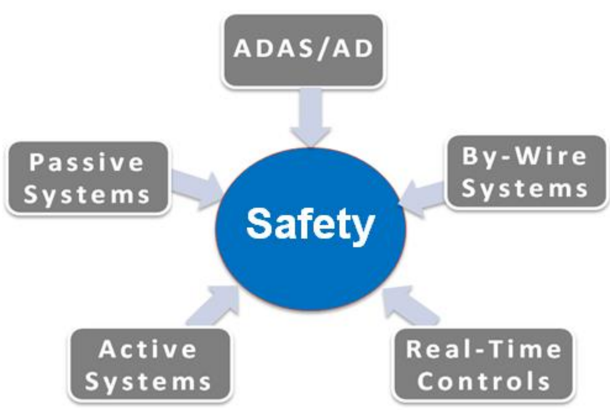

Illustration 1

In comparison, the first aircraft autopilot was developed by the [1] Sperry Cooperation in 1912. These systems at their introduction as well as today are not intended to replace the pilot, but to assist them in the operation of the aircraft allowing the pilot to focus on broader aspects of operation such as monitoring the weather, trajectory and other operational systems, as well as to reduce pilot fatigue in longer duration flights. As the aircrafts sense and control systems evolved, so did the autopilot. The technology currently exists for full autonomous operation of an aircraft, and within the next decade we will likely see these types of aircrafts being introduced into the commercial realm for various operations. Similar to the automotive industry these systems leverage the use of various technologies and techniques in support of both the autopilot system as well as autonomous operation. Autonomous operation should not be confused with remote operation such as the technique used in drone or UAV (Unmanned Arial Vehicle) operation.

Looking at advanced technology applications in the automotive space, the Cadillac's Night Vision was originally introduce on the DeVille in 2000 using a thermal imagery sensor which detected infrared radiation, displaying an image thru the HUD (Heads Up Display) onto the windshield. This image would have to be processed and acted upon by the vehicle operator. This feature was subsequently canceled following the 2004 model year.

ABS (Anti-Lock Brake Systems) as of 2004 have been mandated as standard equipment on all new passenger cars sold in the US (United States). [2] Anti-skid brake systems first turned up on aircraft in the late 40's. One of these purely mechanical systems, the Maxaret was adapted to the British Jensen FF in 1966. These vehicles were not available in the US. It was recognized early on that these type systems would need to have fast acting electronic controls. Despite the claims of a famous German carmaker, the first electronic four-wheel anti-skid system was introduced by Ford in late 1969. The Ford Sure-

Track system by Kelsey-Hayes was available on the Thunderbird and Continental Mark III. The Sure-Brake system for Chrysler's 1971 Imperial prevented the front wheels from locking up in order to maintain steering control during a full-brake or panic braking event.

The advent of electronic controls, help to push functions such as ABS into the mainstream and as previously mentioned are now a required feature on all new vehicles in operation on American roadways. Today's vehicles use throttle and brake by-wire capabilities, where there is no longer a mechanical connection to these functions. By-wire uses various sensors to determine the operators request and electronically pass this input to an ECU (Electronic Control Unit) where the request is verified and acted upon. This type control has two unique challenges over older mechanical systems; first how do I know the request received by the ECU is that requested by the operator and secondly how do I know the action taken by the ECU reflects the operators request. Even with older mechanical systems a failsafe approach was required. Older throttle control systems would use redundant springs on the throttle plate of the carburetor of the throttle body so if the mechanical linkage were to break the vehicle would return to idle, even if one of the two springs were to fail. Today's cars use a similar process where there are two or more redundant sensors used to verify the operator's request. These two inputs are compared to each other to be sure they both match the expected values based upon the request from the operator. Sensor type, slope and other key measurables are defined as to reduce what is referred to as a "common mode fault" as required by the safety standards that apply.

Today's vehicles can include in excess of over 100 ECUs communicating over a number of buses, supporting various communication protocols. Additionally it is not uncommon to have fully electronic (by-wire) throttle, brake, PRNDL (Park Reverse Neutral Drive Lever) and steering functions. Current safety systems leverage the technologies of vision (optical and infrared), RADAR (Radio Detection And Ranging), LiDAR (Light Detection And Ranging), proximity (or ultra-sonic) and GPS (Global Position System) type sensors. These sensors and by-wire controls work in conjunction with digital maps provided in the navigation systems (or via cloud connectivity) allowing for various levels of autonomous operation; ultimately to the NHTSA (National Highway Transportation Safety Administration) Level 4, or SAE (Society Automotive Engineers) Level 5, which is full autonomy. These ADAS & AD functions include FCW (Forward Collision Warning) RCW (rear Collisions Warning), Blind Spot Detection/Warning, LCW (Lane Keep Assist), LDW (Lane Departure Warning), CTA (Cross Traffic Alert), Parking Assist, TSR (Traffic Sign Recognition), ACC (Adaptive or Active Cruise Control), C2I (Car to Infrastructure), C2C (Car to Car), AEB (Automatic Emergency Braking), Pedestrian Detection/Warning, and many others. In addition to these systems, many vehicles also use captive type steering and brake interfaces which are used to alert the driver. This, together with the world's need to be connected, also has driven a need to support various HMI (Human Machine Interface) and Apps through; Linux, QNX, iOS & Android).

Despite and in support of the complexity of today's vehicles, a keen and continued focus on safety is an absolute necessity, regardless of any mandate for compliance. Understanding the risk associated with autonomous operation, the challenges and limitations of the technologies used as well as the potential for threats outside the vehicle environment must be understood and quantified early and throughout the products development life-cycle.

SAFETY STANDARDS

This paper, as well as FEV's Smart Vehicle are based on ground type systems. Generally these systems and their integration require compliance to at least one of the following safety standards; ISO 26262, IEC 61508 or Mil Std. 882. The automotive industry based on volume is the largest consumer and advocate for these safety standards. Originally, commercial safety critical systems such as electric or hybrid vehicles would develop these systems to IEC61508 as there was no specific standard for these type applications. In parallel to the design and development of electric and hybrid vehicle applications in compliance to the IEC standard, ISO had taken the IEC standard and updated it specific to the automotive industry for vehicle applications less than 3500kg, which was formally released in 2011. Even prior to the formal release of ISO 26262, many of the North American OEMs were working to compliance with pre-release or draft copies of the standard, abandoning the IEC standard.. With exception of a few legacy vehicles or systems there is currently little direct use of IEC 61508 within the automobile industry today. ISO 26262 has just recently completed an update scheduled for release in late 2017 or early 2018. This new update has increased content and examples specific to ADAS and AD systems and has also included parts specific to Motorcycles, Micro-Controllers, and Commercial Applications (heavy Trucks and Buses). In addition to the ISO standard, SAE J2980; May 2015: Surface Vehicle Recommended Practice, Considerations for ISO 26262 ASIL Hazard Classification is very helpful in supporting and performing the Hazard Analysis and Risk Assessment required of ISO 26262.

There are certainly differences in the approach and requirements when comparing Mil Std. 882, to IEC 61508 and/or ISO 26262. Despite these differences the intent of all three (3) standards is in the support of functional safety with a key attribute to that in being understanding how a system might fault and what the specific consequences or risks of such a fault might be. In short, each standard assists in the development or metrics which are used to direct the user in the type design, analysis, diagnostic, monitoring and mitigation techniques required to either avoid a fault or failure or to always maintain the vehicle in a safe state.

The safety demonstrated through the limited use of early ADAS systems has not gone unnoticed. Insurers, legislators and the automotive industry itself have recognized the effectiveness of these systems many of which are being mandated for use in future production vehicles. This as well as the volumes consumed in the automotive industry has driven component manufacturers to take notice as well. The integration of these technologies couldn't have happened at a better time as there was already considerable focus on needed compliance to ISO 26262. The end result is many of the micro-controllers, sensors, and their accompanying systems can be purchased pre-certified to a specific ASIL (Automotive Safety Integrity Level).

The ASIL is similar to the SIL (Safety Integrity Level) value defined and used within IEC 61508 as well as the Risk Values associated with Mil Std. 882. Though there is no direct relationship between any of these values the underlying requirements in design, analysis and integration are quite similar. It is also important to note, that though a system may be certified to an ASIL D (as example) this certification is only valid when the system has been properly integrated.

LEVERAGING FEV SMART VEHICLE

The FEV Smart Vehicle is a highly modularized system which supports the Benchmarking, System Architectural Design, Requirements Development, Functional Safety/Cyber Security, Controls Development (HW & SW Function), Component & System Integration/Calibration, Test & Validation as well as Test System Design of all aspects of the systems and components in support of Infotainment, Telematics, ADAS and full autonomous vehicle operation all with full compliance to applicable safety standards.

FEV Smart Vehicle allows for the seamless integration or removal of functions and features throughout the vehicles architecture, while maintaining compliance to applicable safety standard and in support of cyber security needs. This is done in part by FEV's deep knowledge of most all automotive OEM's design and architectural designs and strategies, including their unique HW/SW design as well as bus communication. This knowledge drives the company's highly optimized solution approach from simple to complex and static thru full VI application and strategies.

FEV's work through all aspects of ground vehicle development as well as their respective applicable standards which they have to support, allow the comapny an understanding which in turn gives it the insight necessary to draw a relationship between these standards allowing the use of COTS (Commercial Off The Shelf) systems readily available for integration into defense ground based vehicles/systems. The result in leveraging technologies and techniques pre-certified to the ISO standard is reduced cost in the integration of proven compliant sensors, components and systems as well as greatly expedited integration timing. Additionally, many of the technologies and techniques used in the automotive industry are available to support HIL (Hardware in the Loop), MIL (Model in the Loop) and SIL (Software in the Loop) systems as well as SW (Software) and HW (Hardware) integration development and validation. To further support the rapid prototyping of ground based systems there are libraries readily available that might otherwise need to be developed (e.g. sign recognition), even where regional differences in size and color exist. These libraries not only support the simulators companies might use but the actual controls recognition and execution needed in the actual implementation of the product.

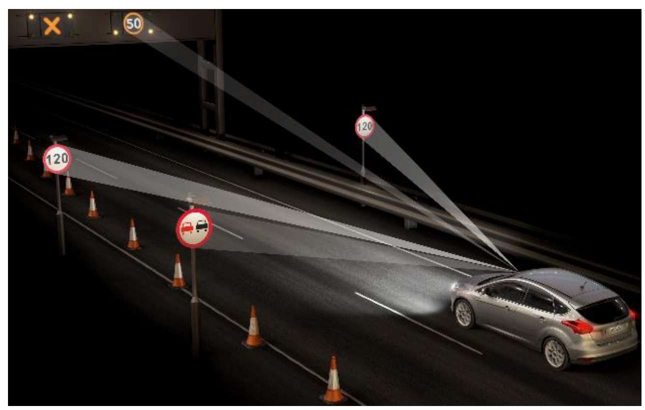

Illustration 2

FEV Smart Vehicle also supports ANN's (Artificial Neural Networks) which is a type learning task of an application in [3] Deep Learning (also known as deep structured learning or hierarchical learning). This compounded with the company's continued work in AI and VI allow the systems themselves to improve in function, capability, and performance over time without any direct operator or user input. The use of cellular networks allow VI systems to learn not only from themselves but also from other similar systems.

This learning frequently programmed in these systems support all aspects of operation, function, monitoring, and mitigation. Hence, overall functions as well as general fault mitigation strategies evolve over time, working to maintain as much overall operational function while still supporting failsafe operation mitigation actions within the required FTTI (Fault Tolerant Time Interval) assigned by the hazard (based upon ISO 26262 as example).

The FTTI is the time period between when a fault presents itself until when the vehicle is brought to a safe state. The FTTI period defined is required regardless as to the complexity of the overall systems as well as any strategy which may allow the system to progress thru multiple mitigation actions in order to bring the vehicle to a safe state. A typical FTTI time line is similar to the image below

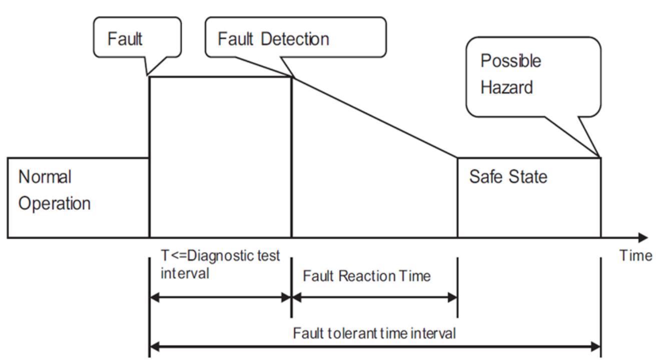

Illustration 3

When applied to vehicle powertrain controls, leveraging the use of those systems used in ADAS/AD allows not only for predictive control in the improvement of mileage and increase in range but alsoreduction in overall vehicle emissions. These improvements are further optimized through the use of a network center as well as VI strategies applied which allow for real-time adjustment to these controls to further optimize on the success of this type of controls strategy.

There are a host of projects where FEV has demonstrated its competency in these areas; one of which involves platooning for commercial vehicles. The initial system supported longitudinal control of commercial vehicles with a following distance of 0.4 seconds at highway speeds. This resulted in a 3rd party determination that the lead vehicle had improved fuel economy of +5% while the trailing vehicle saw an increase in fuel economy of just over 10%. Though safety was demonstrated with these parameters (target trailing distance of 0.4seconds), it was found the closure trailing distances had an adverse effect on engine cooling resulting in extended use of the cooling fan which reduced efficiency and also resulted in increased driver fatigue operating at these close distances.

Similar systems are being demonstrated with lateral steering controls as well, proving upon the functional capability of the current longitudinal systems.

Illustration 4

This system also leverages the data streamed to the network center (cloud and connected vehicle back-end) from all vehicles in operation, allowing qualification of other driver routes as well as real-time information regarding traffic, construction and weather. This data is used to assist in setting the speeds and trailing distances of other platooning vehicles as well as to warn them of situations that may exist further down their route as well as the continued advancement in the overall operational functions of the base system currently.

FEV has further demonstrated the capability of FEV Smart Vehicle thru the accelerated development of a non-mechanical LiDAR sensor head. Performance of the standalone device was in many areas experienced capabilities superior to that of far more expensive units. The development and benchmarking alone though of great use, can be further optimized thru the FEV Smart Vehicle approach whereby this system was developed and assigned compliance of the system to the safety integrity level specific to the applicable safety standard(s) for which it had been developed. This allowed the end or future user to follow a workbook of requirements which where followed and properly documented and supported the specified tasks (requirements) throughout the design life cycle that helped to ensure compliance to the applicable safety standard. As safety is an iterative process the vast majority of this effort could still be reused as part of the "Impact Analysis' even where major components or functions may have changed.

The value in the use of this process grows exponentially especially where fusion of data is to be leveraged. Through the fusing of LiDAR, RADAR, and Vison as well as possibly high-definition maps (on-board or cloud based), the individual operational and functional characteristics of these technologies can be significantly improved. With FEV Smart Vehicle, integration of these stand-alone technologies is reasonably seamless. Further, through the fusing of these technologies, outputs can complement each other reducing false positives (targets), improve collective operation in various types of environmental loading, e.g. sun, rain, snow, etc. allowing confidence in the extended use technologies despite other than desirable loading. Even where techniques or manufacturers may change, much of the FEV Smart Vehicle methods allows sensor fusion to beadjusted and reused with only minimal development.

Additionally, with FEV's continued support and development of various secure DSCR modules for V2X (Vehicle to Anything) allows a system solution to any ADAS/AD need including secure FOTA communication with our without various encryption needs. FEV already demonstrated such V2X applications in Owasso, MI. This specific application not only helps to expedite traffic by giving priority to first responders and their vehicles thru heavy traffic of congested intersections but V2I information is filtered and provided to vehicles equipped with V2V capability that greatly improves situation awareness and hence safety for these cars. This applies not only in the actions and resultant sub-action resultant from their intended use, but also when reviewing dynamic vehicle data regarding the evasive maneuvers such as braking, accelerating, and steering where results show a less aggressive, more controlled mitigation to the situation presented. The data also showed a great benefit when used to support the vehicle's predictive controls which can be supported thru a DSRC (V2V) or similar communication (LTE, 5G, other) protocols to receive data. This has shown not only improvements in predictive engine, predictive transmission, and predictive braking controls (which present great opportunity not only in improving some of the key financial motivations of reduced fuel consumption and reduced exhaust particulates) but also reduction and improved control on traffic flow. Such system can quickly and easily be integrated onto any vehicle type through the FEV Smart Vehicle and also blended with existing systems and functions while still supporting compliance to applicable safety standards.

REFERENCES

[1]Lt. Colonel, W. Scheck, "Lawrence Sperry: Autopilot Inventor and Aviation Innovator", Aviation History magazine, November 2004.

[2]J. Koscs, "Anti-Lock Brakes: Who Was Really First", Haggerty, 9 April 2013.

[3]D. Graupe, "Deep Learning, Neural Networks; Design and Case Studies", World Scientific, 2016.