IEEE P1616a WG
Phone: +1 910-692-5209
Email: mvedr@ieee.org

IEEE
Celebrating 125 Years
of Engineering the Future

TOM KOWALICK
CHAIR
TONY HUFFMAN
Vice-Chair
MATTHEW D. SMITH
Secretary

THE NATIONAL TECHNOLOGY TRANSFER ADVANCEMENT ACT (NTTAA), IEEE EDR GLOBAL STANDARDS and 49 CFR 563

SUBMISSION FOR THE RECORD

DATE: November 9, 2012

FROM: Thomas M. Kowalick
Chair, IEEE EDR Global Standards
IEEE-1616-2010 and IEEE-1616a-2010
mvedr@ieee.org
910-692-5209 N.C. residence

ISSUE: NHTSA's 'BLIND-SPOT': BALANCING TECHNOLOGY FORESIGHT UNCERTANTIES AND CONSUMER PROTECTION IN RIN 2127-AK86: MANDATORY EDR REQUIREMENTS

The NHTSA "safety only" mandate ignores consumer protection, consumer acceptance and privacy issues. Simply put, NHTSA erroneously requires quantitative evidence that a sizeable problem exists (regarding tampering of EDRs and odometer roll-back) before it will act.

In reality, NHTSA would in fact be creating a sizeable problem by mandating EDRs in light vehicles without providing owners of the vehicle basic consumer protection.

The owner of the vehicle, not the automaker should control access to this device (EDR) since it is widely known that In-vehicle electronic modules are subject to tampering, spoliation of evidence, un-detectable surveillance, un-authorized access, misuse of data, and mischief.

Thus, common sense dictates that more emphasis is needed on sealing access to the data at the federally-mandated On-Board Diagnostics (OBD-II) download connector port, located under the dash in virtually all modern vehicles, therefore establishing a chain of custody and preventing tampering.

NHTSA should adhere to the National Technology Transfer Advancement Act (NTTAA) and incorporate by reference IEEE-1616a-2010 into 49 CFR 563: Event Data Recorders.

The IEEE EDR standards offer vehicle owners, fleets, rentals and lessor's accountability, protection and security.

Use of IEEE standards would not be inconsistent with applicable law and would improve motor vehicle safety by preventing a consumer backlash towards implementing this technology. Use of IEEE EDR standards would not be impractical.

The IEEE EDR standard provides a promising countermeasure addressing the safety promise and challenges of 21st Century in-vehicle automotive networks and vehicular electronics. Specifically, vehicle owners must "own" the EDR data, become "aware "of EDRs existence and functioning and must "control access" to the EDR data in their vehicles.

Given these goals OIRA should amend 49 CFR 563: Event Data Recorders by adding the following:

ADD this section:

§ 563.13 Motor Vehicle Event Data Recorder Connector Lockout Apparatus

(MVEDRCLA).

Each manufacturer of a motor vehicle equipped with an EDR shall ensure that a motor vehicle event data recorder connector lockout apparatus (MVEDRCLA) as standardized by the Institute of Electrical and Electronics Engineers Standards Association (IEEE 1616a-2010) to protect the security, integrity, and authenticity of the data that are required by this part is attached to the vehicle's SAE J1962 (ISO/DIS 15031-3) vehicle diagnostic link connector (DLC) at the point of motor vehicle sale, including leased and rented vehicles.

DEFINITION: Connector Lockout Apparatus (CLA) is a device or mechanism to secure a vehicle diagnostic link connector (DLC) as standardized by IEEE-1616a-2010.

IEEE Automotive '*BLACK BOX KEY*' Standard

Protects the security, integrity and authenticity of vehicle crash data

The 21st Annual Conference: Computers, Freedom & Privacy: "The Future is Now"

14-16 June 2011

Georgetown University Law Center

600 New Jersey Ave NW, Washington, D.C

Thomas Michael Kowalick
Chair, IEEE 1616 and IEEE 1616a / Global Standards for Motor Vehicle Event Data Recorder (EDR)
IEEE - Vehicular Technology Society / IEEE - Standards Association
President of AIRMIKA, Inc., Southern Pines, North Carolina, USA
mvedr@ieee.org

Abstract— **The Institute of Electrical and Electronics Engineers (IEEE), the world's leading professional association for the advancement of technology, completed IEEE 1616a in 2010, a new standard based on IEEE 1616, the first universal standard for motor vehicle event data recorders (MVEDRs), similar to units found on aircraft and trains. An adjunct to IEEE 1616, the new standard helps to provide greater consumer protections by improving the effectiveness of these automotive "black boxes" with new lockout functionality designed to prevent data tampering, such as Vehicle Identification Number (VIN) altering and odometer fraud. It also addresses concerns over privacy rights by establishing standards protecting data from misuse. This paper explains how the IEEE 1616a-2010: Motor Vehicle Event Data Recorder Connector Lockout Apparatus (MVEDRCLA) enhances cyber security of automotive electronic control systems and in-vehicle digital network data.**

Keywords – chain of custody, consumer protection, consumer acceptence, crash data, crash data recorder (CDR), cyber security of electronic control systems, data transfer, data transmission, diagnostic link connector (DLC), diagnostic programs, diagnostic testing, EEPROM, electronic control unit (ECU), electronic scan tools, event data recorder (EDR), nonvolatile memory data, OBD2 or OBDII, odometer clocking, odometer fraud, odometer spun, odometer tampering, onboard network data security, power control module (PCM) and/or electronic control unit (ECU) flashing, privacy, road vehicle engineering, road vehicles, SAE J1962 connectors, vehicle components, vehicle crash data, vehicle identification number (VIN) tampering and/or theft.

I. MANDATING EDR PERFORMANCE STANDARDS

During a joint press conference on February 8, 2011, the USDOT Secretary and NHTSA Administrator announced plans to consider three requirements in future passenger vehicles and light trucks: 1) mandatory brake override systems, 2) standardized keyless ignition systems and 3) **mandatory event data recorders.**[1]

*Event Data Recorder (EDR) means a device or function in a vehicle that records the vehicle's dynamic, time-series data during the time period just prior to a crash event (*e.g., *vehicle speed vs. time) or during a crash event (*e.g., *delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data do not include audio and video data.*[2]

According to the World Health Organization (WHO), someone dies in a motor vehicle crash once every minute, and road crash fatalities have claimed 30 million lives globally since 1896.[3] As millions of drivers today face ongoing automotive recalls for electrical and onboard computer issues, MVEDRs are playing an increasingly critical role in the analysis of the scientific data collected from these vehicles. IEEE 1616a provides another extraordinary layer of protection by ensuring the integrity of data collected is not compromised, while providing stronger consumer protections and preserving privacy rights.

The newest member in the IEEE 1616 collection, IEEE 1616a-2010 aims to preserve the data quality and integrity needed to meet federal collection standards, while protecting consumers' privacy.[4] Built on more than a decade of MVEDR research and development by organizations including federal agencies, industry trade associations, and global automotive, truck, and bus manufacturers, newly added safeguards in IEEE 1616a address the following areas:

[1] See http://fastlane.dot.gov/2011/02/nhtsa-nasa-toyota-study-finds-no-electronic-causes-of-unintended-acceleration.html

[2] See http://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Rules/Associated%20Files/EDRFinalRule_Aug2006.pdf

[3] See http://amro.who.int/english/dd/ais/be_v25n1-acctransito.htm

[4] See http://standards.ieee.org/news/2010/1616a.html

Data tampering – modification, removal, erasure, or otherwise rendering inoperative of any device or element, including MVEDRs;

VIN theft – duplication and transfer of unique VIN numbers, a process known as "VIN cloning", enabling stolen cars to be passed off as non-stolen;

Odometer fraud – rolling back of vehicle odometers, resulting in the appearance of lower mileage values; and

Privacy – prevention of the misuse of collected data for vehicle owners.

As of 2011, there are approximately 243 million passenger vehicles in the U.S. As early as 1996, auto manufacturers began installing MVEDRs as part of car and light truck airbag modules. Triggered by certain conditions, such as changes in vehicle speed, MVEDRs collect a variety of data during crash and near-crash events. Data typically collected includes speed at time of impact, steering angle, whether brakes were applied, and seatbelt usage during the crash. However, the National Highway Traffic Safety Administration (NHTSA) will require MVEDRs to meet specific data collection standards. [5]

A. Why we need crash information

Crash information is critical to understanding causation leading up to the crash, occupant kinematics and vehicle performance during a crash, and post-crash events. Manufacturers, engineers, policy makers, researchers, and others rely on crash information to improve vehicle design, shape regulatory policy, develop injury criteria, detect vehicle defects, and resolve investigations and litigation. Motor vehicles have markedly transitioned from mechanical machines with mechanical controls to highly technological vehicles with integrated electronic systems and sensors. Modern automobiles generate, utilize, and analyze electronic data to improve vehicle performance, safety, security, comfort and emissions. Surrounding a crash, capture of a subset of vehicle data on an MVEDR makes important information readily available. The degree of societal benefit from MVEDRs is directly related to the number of vehicles operating with an MVEDR and the ability to retrieve and utilize these data. Having standardized data definitions and formats allows the capture of vehicle crash information. There has been dramatic growth in the volume of sophisticated electronic components installed in today's generation of motor vehicles, including an estimated 90 million vehicles using MVEDR technologies.

IEEE MVEDR standards will help minimize traffic-related fatalities, reduce instances of theft and insurance fraud, and help improve vehicle, emergency response, and roadway design, providing consumers with a greater level of protection.

The P1616 Working Groups of IEEE recognizes the value of improved crash information in improving the knowledge of what happens before, during, and after a motor vehicle crash. Such insights will provide major benefits to society and significantly improve the science of motor vehicle crashes. This IEEE EDR standards define a protocol for MVEDR output data compatibility and export protocols of MVEDR data elements

B. End Users of Crash Data

The impact of improved crash data goes beyond just understanding the dynamics of a crash; it affects a myriad of important societal and business functions. With that in mind, the Working Group solicited input from a range of end users to help identify important data element and critical uses of motor vehicle crash data.

Both individual crash events and aggregate data have value for end users, depending on the application and data used.

Some users and uses include the following:

– Automotive industry: Data-driven design of vehicles, using larger numbers of crashes across a continuum of severity; early evaluation of system and vehicle design performance; and international harmonization of safety standards.

– Insurance industry: Help to identify fraudulent claim, costing more than $20 billion annually; improve risk management; expedite claims and decrease administrative cost. Insurers require accurate crash data for subrogation of claims and recovery of expenses.

– Government: Promulgating and evaluating standards; identifying problem injuries and mechanisms; stipulating injury criteria and investigating of defects. State and local officials require crash information to identify problem intersections and road lengths, to determine hazard countermeasures, and to evaluate the effectiveness of safety interventions.

– Researchers: Human factors research, such as the man-machine interface; crash causation, the effects of aging and medical conditions, and fatigue; biomechanics research on human response to crashes, harmonized dummy development, and injury causation.

— Medical providers: On-scene field triage of motor vehicle crash victims; improved diagnostic and therapeutic decisions; automatic notification of emergency providers; better organization of trauma and EMS system resources.

— The Public: Better policies, vehicle design, emergency response, roadway design, and driving habits; lowered insurance costs, decreased possibility for fraud; fewer crashes and more efficient systems.

In the United States, an estimated 90 million motor vehicles already use some type of event-recording equipment that collects not only acceleration and deceleration speed but also braking and steering data.

Proponents of standard data recorders hope the crash data they collect will be a useful complement to accident information gathered from victims and eyewitnesses.

C. EDR Controversry

However, the implementation of event data recorders (EDRs) has not been without controversy. The United States Department of Transportation (USDOT) Docket Management System (DMS) contains over 1000 submissions reflecting the

[5] See http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=49:6.1.2.3.29&idno=49

pros and cons of a decade-long debate amongst automakers, government regulators, safety and privacy advocates, and the public.[6]

D. Evolution of EDR Technology

In the beginning EDR technology was built into a sensing diagnostic module in each vehicle that controls the air bag deployment. The initial product liability motivation for the generation of a retrievable record was to defend against claims that the air bag system had malfunctioned and caused personal injuries and the safety motivation was to enable improvements to the deployment system. Once the data was compiled for these purposes, it evolved to re-analyze the data in broader terms to promote a better understanding of vehicle and operator behavior before crashes (Causation).

E. 49 CFR 563: Event Data Recorders

The National Highway Traffic Safety Administration (NHTSA) Rule on Event Data Recorders (49 CFR 563) does not address issues generally within the realm of state law, such as the following:

– the ownership of EDR data

– how EDR data can be used/discovered in civil litigation

– how EDR data may be used in criminal proceedings

– whether EDR data may be obtained by the police without a warrant

– whether EDR data may be developed into a driver-monitoring tool

– the nature and extent that private parties will have or may contract for access to EDR data.

There is no Federal law clarifying the rights of a vehicle owner to control access to or ownership of the recorded data and, in the absence of Federal direction, States have begun to create different standards of access and ownership and rights for recorded data.

These issues are being addressed by state legislatures.[7]

F. Types of MVEDRs

There are many types of recorders. Some continuously record data, overwriting the previous few minutes until a crash stops them, and others are activated by crash-like events (such as a sudden change of velocity or angular momentum) and continue to record until the crash is over. EDRs can record whether or not brakes were used, the speed at the time of impact, the steering angle, and whether seat belts were worn during the crash. While EDR information can be useful in determining the cause of a crash, a lockout gives you the reassurance of knowing that you have control of crash data. The "black box" will still work exactly as it is designed to.

G. Control of Data Access

However, with a motor vehicle event data recorder connector lockout apparatus (MVEDRCLA), the vehicle owner (and only the vehicle owner) determines when and who sees the data and, thus controls how it is used. Ownership of EDR data is a matter of state law. Generally, the owner of the vehicle is considered to be the rightful owner; however, courts can subpoena crash data. The IEEE-1616a-2010 amendment seeks to maintain privacy, prevent tampering, avoid odometer fraud, limit data access, and enhance safety by using a MVEDRCLA.

While many vehicle purchasers are not aware these devices are in their vehicles, most are unaware of the nature and potential use of the information collected by their EDR. Data collected by EDRs, without the driver's knowledge, has been used in civil and criminal cases in several states and in Canada. At least one automotive insurance company is considering basing policy rates on EDR data. Auto manufacturers could use EDR data to void warranties. The possibilities are endless.

Several states have already passed laws requiring disclosure of the existence of an EDR in a vehicle, and protection of a driver's privacy by requiring the owner's permission or a court order before downloading the EDR data. It is generally agreed that the owner of a vehicle also owns the EDR data as they have purchased the technology when they bought their vehicle. When consumers drive off the lot with a new car, they own more than just the vehicle; they own the information their vehicle generates and stores.

H. Large Market of the IEEE MVEDRCLA

A large ever-expanding market exists consisting of:

– registered owners of over 243 million passenger motor vehicles;

– military vehicles and federal, state, county, and local government vehicles;

– vehicle OEMs and new car dealerships that lease vehicles;

– automotive insurance companies that seek to prevent other parties from access to data;

– automotive rental companies that cannot permit odometer tampering; institutional fleets such as schools, colleges, and universities;

– business fleets include leasing, construction, plumbing, heating, food distribution, shipping, utilities; and others such as police, fire, EMS, taxi, etc.

I. Odometer Fraud

An NHTSA report notes:

"Odometer fraud is the illegal practice of rolling back odometers to make it appear that vehicles have lower mileage than they actually do. This has historically been considered a significant problem for the American consumer. While any vehicle sold on the used car market could have been the object of odometer tampering, the problem has been considered to be

---

[6] See www.regulations.gov and search the term "event data recorder" for EDR dockets

[7] State Initiatives: Arkansas Code 27-37-103, California Code 9950-9953, Colorado Statutes 12-6-4, Connecticut Public Act 07-235, Maine Statutes 29A-1-17-3, New Hampshire Statutes 357-G, New York Laws 4A16 416-B, Nevada Statutes 484.638, North Dakota Code 51-07-28, Oregon House Bill 2568 (644), Texas Statutes 547.615, Virginia Code 46.2-1088.6 and Washington 46-35.010.

most prevalent among late-model vehicles which have accumulated high mileage in a relatively short period of time. Vehicles in fleets, such as lease fleets, rental fleets, or business company fleets typically fall into this category. When sold on the used car market, vehicles whose odometers have been rolled back, or "spun," can obtain artificially high prices, since a vehicle's odometer reading is a key indicator of the condition, and hence the value, of the vehicle."

See: http://www.nhtsa.gov/Odometer-Fraud

J. The Diagnostic Link Connector (DLC)

Many light-duty vehicles, and increasing numbers of heavy commercial vehicles, are equipped with some form of MVEDR. These systems, which are designed and produced by individual motor vehicle manufacturers and component suppliers, are diverse in function and proprietary in nature, however, the SAE J1962 (ISO 15031-3:2004) vehicle DLC has a common design and pinout, and is thus universally used to access event data recorder information. Data access via the DLC can be accomplished by using scan tools or microcomputers and network interfaces.

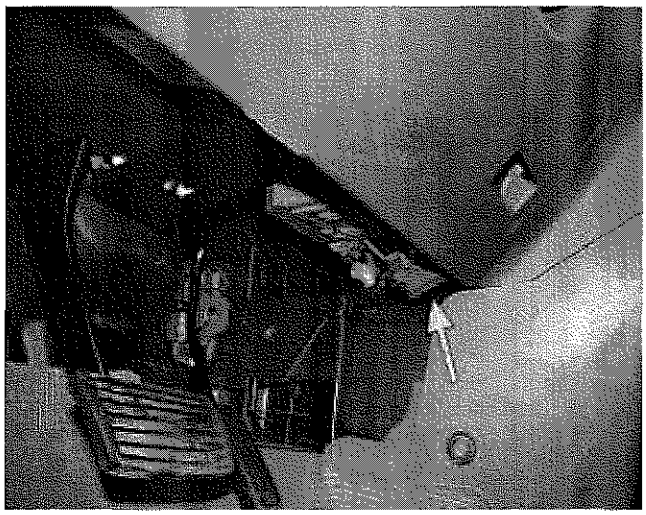
This same DLC and network interface is also used for re-calibrating electronic control units on a vehicle. Such ECU applications can include restraint controls, engine controls, stability controls, braking controls, etc. The IEEE-1616a-2010 standard defines a protocol to protect against misuse of electronic tools which use the DLC to erase, modify or tamper with electronic controller or odometer readings, or to improperly download data. Implementation of MVEDRCLA provides an opportunity to voluntarily achieve DLC security by standardizing a MVEDRCLA which will act to prevent vehicle tampering, which can include odometer fraud, illegal calibrations leading to emissions violations and theft of personal data.

Adoption of IEEE 1616a-2010 will therefore make the common MVEDR/DLC data more secure and credible while still permitting accessibility to legitimate end users. The continuing implementation of MVEDR systems provides an opportunity to voluntarily standardize data output and retrieval protocols to facilitate analysis and promote compatibility of MVEDR data. Adoption of the standard will therefore make MVEDR data more accessible and useful to end users.

Having standardized data definitions and formats allows the capture of vehicle crash information. This standard recognizes the value of improved crash information in improving the knowledge of what happens before, during, and after a motor vehicle crash. Such insights will provide major benefits to society and significantly improve the science of motor vehicle crashes.

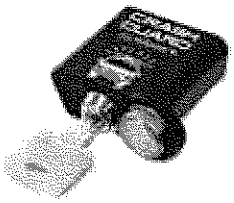
K. Opportunities and Challenges

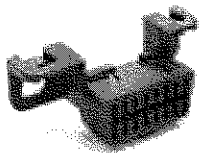
The past four decades have witnessed an exponential increase in the number and sophistication of electronic systems in vehicles. A vast increase in automotive electronic systems, coupled with related memory storage technologies, has created an array of new safety engineering opportunities and subsequent consumer acceptance challenges.



Virtually every passenger car and light truck manufactured in or imported to the North American market since model year 1996 includes an Environmental Protection Agency (EPA) mandated DLC to allow access to engine and emissions diagnostic data.

This onboard DLC (OBDII) is regulated by the Code of Federal Regulations (CFR) (40 CFR 86.094-17(h)) and revisions for subsequent model years. It is standardized by the Society of Automotive Engineers (SAE) Vehicle Electrical Engineering Systems Diagnostic Standards Committee. The physical configuration of the output plug is specified under SAE J1962-2002 and through the International Standards Organization under ISO 15031-3:2004 and is increasingly used as an access point to other in-vehicle electronics systems, subsystems, computers, sensors, actuators and an array of control modules including the air bag control module.





AN IEEE 1616A MVEDRCLA AND SAE J1962 DIAGNOSTIC LINK CONNECTOR

The onboard DLC is also used as a serial port to retrieve data elements from on-board systems, subsystems, modules, devices and functions that collect and store data elements related to a vehicle crash such as a restraint control module (RCM) and event data recorder (EDR). Thus, the onboard DLC provides a portal for capture of an increasing volume of sophisticated sensor data regarding the operating condition, operation and behavior of vehicles, and in particular the operation and behavior of vehicles involved in crashes. Consumers continue to be interested in safety advancements but remain concerned about issues of privacy, tampering, and misuse of vehicle crash data. It is important to protect a variety of crash-sensing and diagnostic memory modules. Increasingly, data from these devices have been used in civil and criminal court cases nationwide, including cases dealing with vehicular homicide in which speed was an issue.

L. Tampering

Tampering involves the deliberate altering or adulteration of information, a product, or system. Tampering means to modify, remove, render inoperative, and cause to be removed, or make less operative any device or element design installed on a motor vehicle or motor vehicle power-train, chassis or body components which results in altering federal motor vehicle safety standards (FMVSS). Tamper-evident describes a device or process that makes unauthorized access to the protected object easily detected or determined after the fact. Tamper resistance is resistance to tampering by either the normal users of a product, or system by others with physical access to it. Access Control refers to a means of recording time and date that a vehicle's Diagnostic Link Connector (DLC) was sealed or unsealed.

A variety of electronic tools are manufactured and marketed to re-engineer vehicle networks, reset odometers and tamper or erase vehicle data via this port which is generally unsecure and prone to misuse of the original safety and emissions diagnostic related purpose. Unauthorized access, whether malicious or inadvertent, must be prevented in order to protect the integrity of connected devices, vehicles, and systems.

M. A Short List of Online Links for Tampering Tools

Publicly advertised tools that have the ability to clear "locked data" from crash records in Event Data Recorders (typically SRS ECUs):

1. http://www.uuctech.com/Products/VW-AUDI-Airbag-Reset.html
2. http://www.tradekey.com/product_view/id/811757.htm
3. http://www.codecard.lt/carprog/carprog-airbag-with-all-software-39-s-and-adapters-needed-for-airbag-repair-and-programming/prod_345.html
4. http://www.adkautoscan.com/Production/R101.htm
5. http://autocheery.en.made-in-china.com/product/reOQqGocbJiB/China-Honda-SRS-OBD2-Airbag-Resetter-for-Honda-with-TMS320-.html
6. http://www.mtaplus.cz/navody/vwgroup_airbagreseter.pdf
7. http://www.codecard.lt/ford-airbag-reset-tool-please-find-it-as-carprog-software-/prod
8. http://www.codecard.lt/carprog/software/carprog-airbag/s5-5-gm-airbag-reset-tool-by-obdii/prod_88.html

The NHTSA's National Center for Statistics and Analysis Research Note DOT HS 811 363 cites that there were 5,505,000 vehicle crashes in 2009. The major technical problem is that all of these 2009 vehicles crashed with un-sealed in-vehicle networks, although not all of these vehicles included an event data recorder function or device whereby post-crash data could be analyzed.

However, as the nation's vehicle fleet is updated more and more vehicles include electronic systems or sub-systems and the Diagnostic Link Connector (DLC) will remain the primary communications and download port to the majority of electrical and electronic data accessible via the Controlled Area Network (CAN) infrastructure.

N. The IEEE Technical Solution

The exact technical problem is locking down this port to avoid mischief and misuse including tampering.

Since the DLC is easily located and clearly visible to first responders such as law enforcement, emergency medical technicians and others it can be easily established if the port was sealed or unsealed by taking a photograph that includes time and date. Many cell phones include photo capability. Otherwise, a law enforcement official may note on an accident report if the DLC was sealed.

Once this fact is established, despite the best efforts of everyone involved, it may be possible that a hacker could defeat the locking mechanism by numerous methods ranging from blunt physical force to ripping out the entire wiring assembly and thereby removing the evidence that the port was sealed. However, this is not a simple or quick process for a number of reasons. First, the DLC is usually tightly fitted amongst a number of other devices within the vehicle cabin whereby the attacker could not get to the side or the rear of the DLC. Second, the wiring harness is very tightly packaged and concealed and would require extreme blunt force to detach by physical force since there are a large number of wires (up to 16) that retain the DLC.

The major point of the process is to provide evidence at the time of the crash. Thus, establishing a chain of custody at crash time is essential to securing digital data probative value.

II.

III. EDR Generic Risks

- Confidentiality
- Integrity
- Availability
- Authenticity

A. CONFIDENTIALITY

CONFIDENTIALITY is defined as the "property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes, or other entities"([ISO/IEC 2382-8: 1998], 08.01.09).

The assumption that EDRs only provide data linked to a specific vehicle, but not a specific driver, ignores the data privacy issues outside the vehicle.

Although it may seem feasible to avoid privacy issues by restricting the recorded data to a minimal set of sensor and status data and to only record a time span of about one minute around the crash event – it is highly probable that next generation memory module technologies will increase the recording time, therefore making privacy issues unavoidable.

Increasing numbers of people will obtain access to EDR data. The minimum requirement to access EDR data is physical access to the vehicle's interior and the SAE J1962 connector. Therefore, access to EDR data will always be possible unless a technical countermeasure is utilized.

The DRIVER and OWNER will always have physical access to the EDR device (via the SAE J1962 Diagnostic Link Connector (DLC) common on all light vehicles.

This is a problem if the owner can access data that would indicate a crash in which the vehicle was involved and where a driver other than the owner was involved in the crash.

For example, a car rental company or transport fleet could regularly access data to find out about the crashes by drivers. Even if the rental company does not sue the driver immediately, the company (or even a group of cooperating rental companies) could use the data to keep a 'black list' of drivers involved in crashes.

Since the USDOT/NHTSA is mandating EDRs in light vehicles it is highly likely that lease, fleet and rental vehicles will have EDRs. Therefore, since drivers are supposed to notify the company about any crash, accessing the EDR data would only change the situation for those drivers who had not informed the company about the crash.

Although this might be an issue in the case of low-priority (unreported to law enforcement) crashes, access to the data by the OWNER in this scenario, especially the COMBINATION OF EDR DATA AND PERSONAL DATA requires the consent of the DRIVER and would need to be explicitly agreed in the rental contract.

The combination of EDR data with driving records creates data records that require consumer data protection to avoid creating 'black lists'.

The potential to 'misuse' EDR data will greatly increase.

Following a crash, many vehicles are taken to a workshop where access to the EDR data is possible. Workshops can sell data to car or insurance companies for statistical purposes, or sell data for marketing purposes. A rare/extreme motivation for workshops to download EDR data is blackmailing of drivers or owners which is more likely to occur with high-profile crashes.

After a crash, it may be possible that neither driver nor owner is capable of controlling physical access to the vehicle. Therefore, an opportunity does exist for third parties to access EDR data from the vehicle, although they may have no rights to access them. It is technically possible to gather EDR evidence since the port is unprotected.

B. INTEGRITY

INTEGRITY is defined as the "property of data whose accuracy and consistency are preserved regardless of changes made" (data integrity, [ISO/IEC 2382-8:1998], 08.01.07). For systems (like the EDR itself), integrity means "the quality of a data processing system fulfilling its operational purpose while both preventing unauthorized users from making modifications to or use of resources and preventing authorized users from making improper modifications to or improper use of resources" (system integrity, [ISO/IEC 2382-8: 1998], 08.01.17).

The most obvious threat to an EDR is the manipulation of the data. After a crash, a driver or owner of a vehicle may be interested to tamper EDR data in order to avoid prosecution. Manipulation / Tampering may take several forms, like replacing all data with a forged set of records, changing only selected records, or even changing only selected entries within a record.

From an IT security point of view, all manipulations / tampering of data is considered as unauthorized – however, it still happens. An attacker may delete data from the EDRs event storage creating the impression that the crash did not happen at all.

An attacker may overwrite incriminating data in a way that suggests that the EDR or its attached sensors did not function correctly, thus making the EDR data useless for prosecution. An attacker may consistently change EDR records in a way that suggests that the accident did happen, but the driver did not violate any driving regulations.

For example, an attacker can change the vehicle speed prior to a crash to a lower value, indicating that the vehicle was being driven within the permitted speed limit. Such manipulations are the most complex ones, because not only the speed needs to be changed, but also the acceleration/deceleration values, time values, and other data need to be changed consistently.

Forging / Tampering / Manipulation is most likely following a crash, unless an attacker has exact knowledge of a pending crash and seeks to influence the post-crash analysis of

that crash data. Therefore, most manipulation of data will occur following a crash before it has been downloaded (and secured as evidence) by an authorized party.

Once the EDR data has been secured as evidence by time stamping and digitally signing the downloaded records, manipulation will be useless, since any record presented in court would have to compete with credibility with the original record already downloaded and introduced into the legal process by the appointed trustworthy expert. Therefore, we can assume that manipulation of EDR data is only a threat during the 'window of opportunity' between the crash itself and the point in time where the EDR is secured as evidence. In Hit & Run cases the 'window of opportunity' is larger. There is also a threat of manipulating data prior to selling the vehicle.

With a USDOT/NHTSA EDR mandate a large base of installed EDRS (90+ million) will trigger development of sophisticated manipulation tools, especially if such a manipulation can be programmed in software. Electronic tools exist to manipulate EDRs and to alter digital odometers.

C. *AVAILABILITY*

AVAILABILITY is defined as the "property of data or of resources being accessible and usable on demand by an authorized entity" ([ISO/IEC 2382-8:1998], 08.01.17).

Threats to EDR data are similar to the INTEGRITY threats because they have similar affects, although they can have different causes. The EDR or some of its sensors could malfunction. The EDR could be severely damaged in the crash. The power supply to the EDR could be cut.

D. *AUTHENTICITY*

AUTHENTICITY deals with the origin and genuineness of data. In EDR issues AUTHENTICITY has its own set of threats relative to EDR security architecture. EDR data is used as evidence in disputes, and therefore its authenticity must be guaranteed to a degree acceptable by courts.

EDRs raise critical issues including: who should have access to the data stored; under what circumstances access should be granted; whether EDRs are tamper-proof; and whether they are resistant to accidental spoliation.

Access to EDR data is possible by anyone having physical access to the vehicle interior and plugging an electronic tool into the SAE J1962 connector. The court or any higher authority must be convinced that the data presented to it can be linked unambiguously to an event and a certain vehicle.

AUTHENTICITY needs to be protected during the data transition from the EDR to the court. The current design of EDR architecture and data model provides a link between the EDR and the vehicle. However, the EDR itself would not provide a digital signature of any kind to prove that the data originates from the EDR.

As the records are not signed by the EDR, everybody in the chain could modify it. Such modifications would be hard to spot if the original record is not integrity-protected. EDR data needs to be sealed at the time of the crash. EDR data can be sealed at the time of the crash by utilizing an IEEE standardized Connector Lockout Apparatus (CLA).

If not sealed at crash time, it is crucial to keep the time window between crash and download of the EDR data as small as possible. Signing the records by the EDR itself cannot be implemented without a significant overhead for a security infrastructure. However, sealing the EDR data at the time of crash via a CLA is both technically feasible and economically sound. Reliable proof of AUTHENTICITY of EDR data is achieved via an IEEE 1616a CLA. Tampering motor vehicles may be the privacy crime of the future. Cars today are as much products of computer electronics as they are automotive engineering. Because they contain and rely upon so much high-tech circuitry, cars are increasingly becoming vulnerable to computer hackers who may be able to manipulate vital components while in use, according to researchers.

IV. ONGOING RESEARCH

A. *Hacking Vehicles Paper*

In a recently published research paper (Experimental Security Analysis of a Modern Automobile 2010 IEEE Symposium on Security and Privacy) computer security experts at the University of Washington and the University of California, San Diego, concluded that hackers who access a car's computers "can leverage this ability to completely circumvent a broad array of safety-critical systems...including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on." The research claimed:

> Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced a range of new potential risks. In this paper we experimentally evaluate these issues on a modern automobile and demonstrate the fragility of the underlying system structure. We demonstrate that an attacker who is able to infiltrate virtually any Electronic Control Unit (ECU) can leverage this ability to completely circumvent a broad array of safety-critical systems. Over a range of experiments, both in the lab and in road tests, we demonstrate the ability to adversely control a wide range of automotive functions and completely ignore driver input– including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on. We find that it is possible to bypass rudimentary network security protections within the car, such as maliciously bridging between our car's two internal subnets. We also present composite attacks that leverage individual weaknesses, including an attack that embeds malicious code in a car's telematics unit and that will completely erase any evidence of its presence after a crash. Looking forward, we discuss the complex challenges in addressing these vulnerabilities while considering the existing automotive ecosystem. Someone, such as a mechanic, a valet, a person who rents a car, an ex-friend, a disgruntled family member, or the car owner–can, with even momentary access to the vehicle, insert a malicious component into a car's internal network via the ubiquitous OBD-II port (typically under the dash). The attacker may leave the malicious component permanently attached to the car's internal network or, as we show in this paper, they may use a brief period of connectivity to embed the malware within the car's existing components and then disconnect.

It also was determined that infiltrators could conceivably hide any trace of their hacking and "completely erase any evidence of its presence after a crash." Numerous news stories and articles report that cars can be hacked.

B. VERONICA II: Vehicle Event Recording based on Intelligent Crash Assessment.

VERONICA II is to specify the technical and legal requirements for a possible implementation of Event or Accident Data Recorders in vehicles in Europe. Of major importance is the definition of the trigger sensitivity in order to capture not only hard crash data but also data from collisions with 'soft objects', i.e. vulnerable road users which represent a relevant part of road users and victims in accidents.

http://ec.europa.eu/transport/road_safety/pdf/projects/veronicaii.pdf

C. Government Accountability Office (GAO)Report

A United States Government Accountability Office (GAO) Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate (GAO-09-56) titled HIGHWAY SAFETY: Foresight Issues Challenge DOT's Efforts to Assess and Respond to New-Technology-Based Trends recommends that DOT (1) develop an approach to guide decision-making on new, fast moving trends that can affect highway safety; (2) evaluate whether new data systems and analytic techniques are needed to provide information on such trends; and (3) employ specific strategies and schedules in communicating with Congress about these and other trends. DOT disagreed with the first of these and did not comment on the other two. GAO continues to recommend all three.

GAO-09-56 at www.gao.gov/new.items.d0956.pdf

D. National Academies / Transportation Research Board (NAS-TRB) Study

The U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) has requested that the National Research Council (NRC) appoint an independent committee with appropriate expertise to review past and ongoing industry and NHTSA analysis and research to identify possible causes of unintended acceleration and make recommendations on (a) NHTSA research, rulemaking, and defects investigation activities and (b) human, infrastructure, and financial resources required for NHTSA to assure the future safety of electronic throttle control and other electronic vehicle control functions. The project is being undertaken by the NRC's Transportation Research Board (TRB) and Division on Engineering and Physical Sciences' Board on Energy and Environmental Systems and Computer Science and Telecommunications Board. See: "MOTOR VEHICLE 'EDR' GLOBAL STANDARDIZATION AND RELATED ISSUES."

http://onlinepubs.trb.org/onlinepubs/UA/111610Kowalick.pdf

V. RECOMMENDATION

Rationale: Government agencies use externally developed standards in a wide variety of ways, including the following: Adoption: An agency may adopt a voluntary standard without change by incorporating the standard in an agency's regulation or by listing (or referencing) the standard by title. For example, the Occupational Safety and Health Administration (OSHA) adopted the National Electrical Code (NEC) by incorporating it into its regulations by reference. In summary, IEEE 1616a-2010 should be incorporated by reference into *49 CFR 563: Event Data Recorders* as follows:

ADD this section:

§ 563.13 Motor Vehicle Event Data Recorder Connector Lockout Apparatus (MVEDRCLA). Each manufacturer of a motor vehicle equipped with an EDR shall ensure that a motor vehicle event data recorder connector lockout apparatus (MVEDRCLA) as standardized by the Institute of Electrical and Electronics Engineers Standards Association (IEEE 1616a-2010) to protect the security, integrity, and authenticity of the data that are required by this part is attached to the vehicle's SAE J1962 (ISO/DIS 15031-3) vehicle diagnostic link connector (DLC) at the point of motor vehicle sale, including leased and rented vehicles.

[1]. A review of jurisprudence regarding event data recorders: implications for the access and use of data for transport canada collision investigation, reconstruction, road safety research, and regulation, prepared for the road safety and motor vehicle regulation, Transport Canada. http://www.carsp.ca/downloads/edr_jurisprudence.pdf March 31, 2005

[2]. U.S. Department of Transportation, National Highway Traffic Safety Administration, Final Rule, 49 CFR Part 563, Event Data Recorders, http://www.nhtsa.gov/Laws+&+Regulations/Vehicles Aug. 21, 2006.

[3]. Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis, Transportation Research Board NCHRP (Project 17-24), http://www.nhtsa.gov/DOT/NHTSA/NRD/Articles/EDR/PDF/Research/EDR_Technology.pdf December 2004.

[4]. Vehicle Data Recorders - FMCSA-PSV-06-001, Federal Motor Carrier Safety Administration, http://www.fmcsa.dot.gov/facts-research/research-technology/report/vehicle-data-recorders-dec05/vehicle-data-recorders-dec05.htm December 2005.

[5]. Institute of Electrical and Electronics Engineers (IEEE) global standards for Motor Vehicle Event Data Recorders (MVEDRS); IEEE 1616-2010 and IEEE 1616a-2010 at http://grouper.ieee.org/groups/1616a/ May, 2010.

[6]. GAO -09-56 Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate: HIGHWAY SAFETY Foresight Issues Challenge DOT's Efforts to Assess and Respond to New Technology-Based Trends. www.gao.gov/new.items/d0956.pdf October 2008.

[7]. Analysis of Event Data Recorder Data for Vehicle Safety Improvement, USDOT/NHTSA DOT HS 810 935 at www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/EDR/.../810935.pdf

Thomas M. Kowalick *is widely recognized as a leading researcher on EDR technologies. He is a member of the Author's Guild, and president of AIRMIKA, Inc., in Southern Pines, North Carolina. Kowalick serves as Chair of the Institute of Electrical and Electronics Engineers (IEEE) global project 1616 ® to create the world's first automotive 'black box' standard, he contributed to the development of the National Highway Traffic Safety Administration (NHTSA) web site for EDR research, and as a panel member on the National Academies of Sciences project studying EDRs. He is the author of FATAL EXIT: The Automotive Black Box Debate (John Wiley) and six other books specifically covering EDR history, standardization, legislation, regulation, legal issues and consumer protection. Kowalick is also author of the EDR segment in the McGraw Hill 2009 Yearbook of Science & Technology.*