JCB's 3.0-L 430 Dieselmax Stage V engine is equipped with a "one-can" DPF/DOC and boasts auto-stop technology to further reduce emissions.

loader product marketing manager.

The Cummins engine will be equipped with an auto shutdown feature and the combination of the new engine and transmission will deliver a claimed 10% improvement in fuel consumption. A wide-core cooling pack, previously an option on the 457, will become standard on the Cummins-powered loader.

The 457 will continue to be powered by a 192-kW (258-hp) **MTU** engine in Tier 4 Final territories such as North America, as the MTU engine meets the emissions standard without the use of a DPF.

JCB will also use Stage V Cummins engines in its 437 and 427 models. The 437 gets a power boost at Stage V, from 136 to 145 kW (183 to 195 hp). The 427 will be equipped with a 123-kW (165-hp) Cummins motor. Both machines also adopt a five-speed Powershift transmission and auto shutdown, while the 437 also comes with a low power mode.

The smaller 407 and 409 loaders will continue to use JCB Diesel by **Kohler** engines to meet Stage V, though now with the addition of a DPF. Power outputs are unchanged, though auto shutdown has now been included. The 407 will also come with a "whisper quiet" **Rexroth** hydraulic pump to reduce overall noise levels. An Eco Drive Mode has also been incorporated in the hydrostatic driveline, to make up to a 16% fuel saving at higher speeds.

For the smallest 403 model, JCB will offer a choice of the current 26-kW (36-hp) engine, alongside a Smart Power 19-kW (25-hp) version, for those customers seeking ultimate fuel economy.

Dan Gilkes

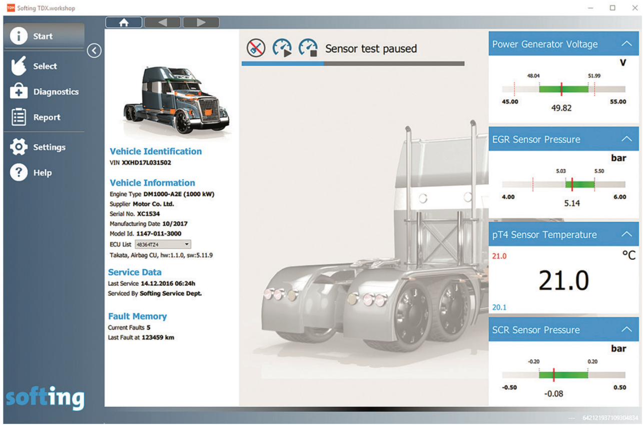
CYBERSECURITY | COMVEC PREVIEW

Protecting a cyber-physical remote diagnostic communication system against cyberattacks

The increasing complexity of microcontroller-based E/E (electrical/electronic) systems that control heavy-duty trucks, buses and non-road mobile machines and their powertrain components (diesel engines, emission control systems and transmissions) comes with increased self-diagnosis functions and diagnosability via external test equipment.

Technicians in the development, production and service depend on diagnostic test equipment that is connected to the E/E system of the vehicle/machine and performs diagnostic communication. Examples of use cases of diagnostic communication include diagnostic data acquisition, (guided) fault finding and flash reprogramming.

The physical connection between diagnostic test equipment



Sensor test paused

Vehicle Identification
VIN XXHD17L031502

Vehicle Information
Engine Type DM1000-A2E (1000 kW)
Supplier Motor Co. Ltd.
Serial No. XC1534
Manufacturing Date 10/2017
Model Id. 1147-011-3000
ECU List 48364TZ4
Takata, Airbag CU, hw:1.1.0, sw:5.11.9

Service Data
Last Service 14.12.2016 06:24h
Serviced By Softing Service Dept.

Fault Memory
Current Faults 5
Last Fault at 123459 km

Figure 1: Screenshot of a generic diagnostic tester.

KWP 2000	ISO 14230
HD-OBD	SAE J1939-x
WWH-OBD	ISO 27145
UDS on CAN	ISO 14229-3 and ISO 15765 (DoCAN)
UDS on IP	ISO 14229-5 and ISO 13400 (DoIP)

Table 1: Examples of standardized diagnostic communication protocols.

Wired CAN /CAN-FD (ISO 11898)
Wired Ethernet (IEEE 802.3 - 100BASE-TX)
Wireless LAN (Wi-Fi, IEEE 802.11)
Bluetooth (BT)
Cellular (3G GSM, 4G LTE, 5G), e.g. for Telematics
RF Link for dTPMS
Satellite Digital Audio Radio Services (SDARS)

Table 2: OSI model physical and data link layer protocols.

TOP LEFT: JCB; ALL OTHER IMAGES: SOFTING AUTOMOTIVE ELECTRONICS

and a vehicle/machine is provided by a diagnostic connector that comes with pins for K-Line, CAN and Ethernet. In addition, today's vehicles are equipped with several wireless access points, such as telematic control units (TCUs), global positioning systems (GPS), Bluetooth or wireless LAN (Wi-Fi).

The wireless and remote connection between a diagnostic tester and a fleet of vehicles can be considered a technical masterpiece, but only if new challenges such as closing security gaps are mastered. This article analyzes the components of the cyber-physical system (CPS) for remote diagnostic communication and provides measures to improve the resilience against cyberattacks.

A cybersecurity panel taking place on September 11 at the **SAE** COMVEC 2019 event in Indianapolis also will cover this topic and other cyber-related concerns. The session will be moderated by Larry Hilkene, chief product cybersecurity engineer at **Cummins** Inc., and include the author from **Softing Automotive Electronics**. (A list of technical sessions can be found at www.sae.org/attend/comvec/program/technical-sessions.)

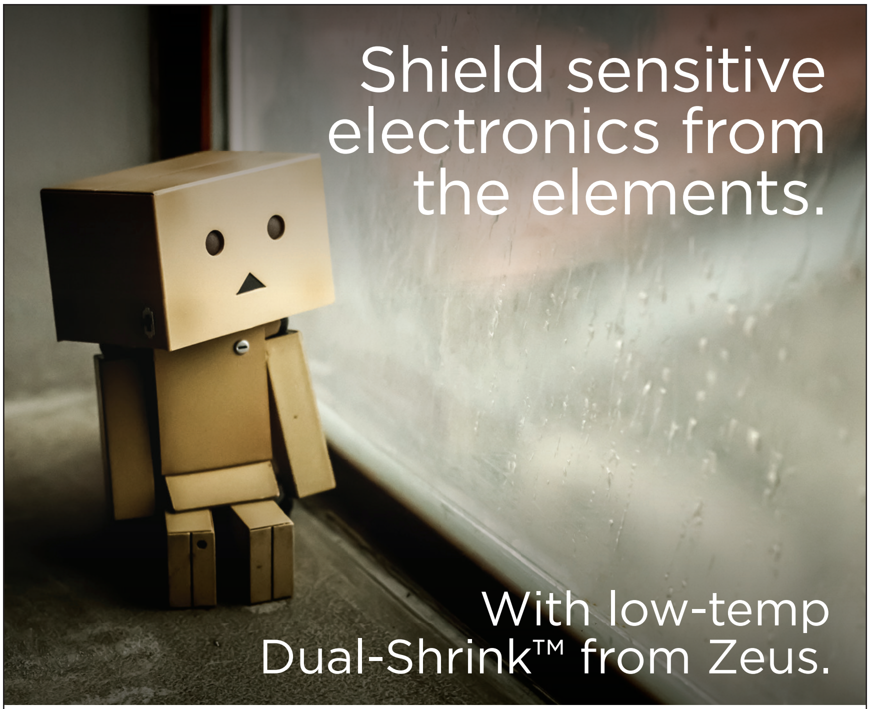
Automated functions require real-time detection, fast repair

Like any other function, the diagnostic functions of a vehicle or machine must be specified, planned, designed, developed, tested and released. External test equipment, in this context referred to as diagnostic tester, helps the technician to do his or her job right—for example, to develop the correct setting of Diagnostic Trouble Codes (DTCs), to program control units in the production line or to find a fault in the aftersales service. Figure 1 shows the screenshot of a diagnostic tester as an example.

Note: In colloquial language it is often said that the diagnostic communication takes place between the tester and the vehicle/machine. That is not actually correct. For reasons of accuracy, we presume that the diagnostic communication at a specific point in time takes place between the tester and exactly one control unit (ECU). SAE J1939 goes one step further and defines Controller Applications (CAs) that consist of control unit firmware, for example for diagnostic purposes.

In simple terms, there is a TST-to-ECU and an ECU-to-TST connection. The communication protocol between the tester and the ECU is referred to as the diagnostic communication protocol. Examples of common and standardized diagnostic communication protocols are listed in Table 1.

Diagnostic communication protocols are mapped to the Open Systems


Shield sensitive electronics from the elements.
With low-temp Dual-Shrink™ from Zeus.

Safely encapsulate your critical components.

We know there are certain sensitive electronics and components that require coatings with tight, moisture seals, strong chemical resistance, and lower recovery temperatures. Low-temperature Dual-Shrink™ offers comprehensive environmental protection without harming equipment.

Five decades of extrusion experience have made us a leader in the heat shrink industry. As we continue our commitment to supplying products that emphasize safety and performance in harsh environments, let's see what we can develop together.

Call for a consultation or visit *zeusinc.com/ltds* for free samples and get started today.

ZEUS®
Turning polymers into possibilities.

AMERICAS: +1 803.268.9500
EUROPE: +353 (0)74 9109700
ASIA/PACIFIC: +(86) 20-38254909
support@zeusinc.com | zeusinc.com

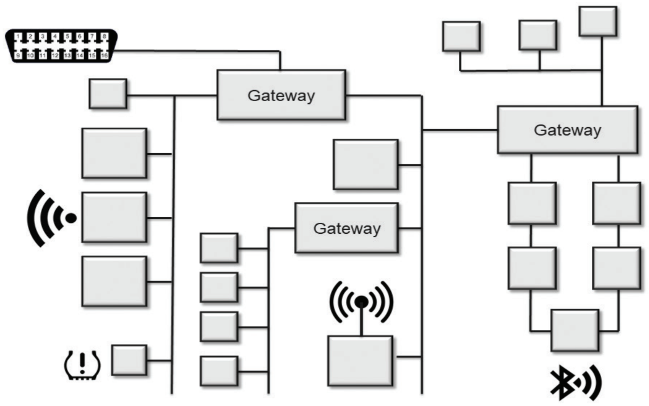


Figure 2: Wired and wireless access points to the E/E system of the vehicle/machine.

Interconnection Basic Reference Model (OSI model) and organized in OSI model layers. On the OSI model application layer, the tester sends a diagnostic service request to the ECU and the ECU answers with a positive or a negative response.

Each diagnostic communication protocol also comes with an OSI model physical and data link layer such as CAN, Ethernet or Wi-Fi. Table 2 lists a selection of the currently used OSI model physical and data link layer protocols for diagnostic communication.

Figure 2 shows a simplified in-vehicle network with access points as they are listed in Table 2.

Especially with the increase of automated functions, reliable self-diagnosis functions must be implemented. The detection of malfunctions in real time and methods/procedures for the fastest possible correction or repair must already be considered in the planning phase of safety-relevant automatic functions. Remote diagnostic communication is part of the game, and in order to fix malfunctions caused by software bugs, the update of control unit firmware by OTA (over-the air) flash programming is required.

Figure 3 and Table 3 show a simplified cyber-physical system for remote diagnostic communication.

Increasing resilience against cyberattacks

For diagnostic communication, the tester is connected to the control unit (actually to its CA) and sends a diagnostic service request to it. If supported, the control unit will send a positive response and process the requested action—for example, start internal (test) routines, send diagnostic data, or prepare for/process flash reprogramming.

Each component of the CPS as it is described in Figure 3 / Table 3 can be attacked by a malicious hacker. Especially the wired and wireless data links pose a security risk.

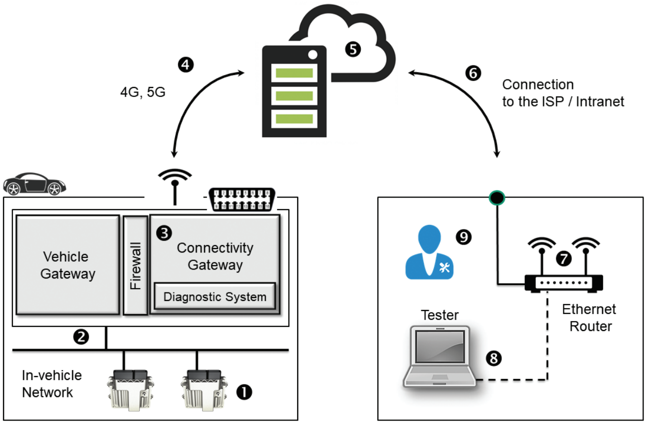
To improve the resilience of remote diagnostic communication between external test equipment and a vehicle/machine against cyberattacks, it is imperative to understand and analyze the functionality and vulnerability of each communication system component, including the wired and wireless communication channels.

Numerous papers, studies and guidelines, even standards, such as SAE J3138, SAE J3005 and SAE J3061, have been published since the automotive industry became aware of the cybersecurity issue a couple of years ago. Since then, cybersecurity has been a moving target.

Due to the limited resources provided by the E/E system and due to real-time requirements of many processes within a vehicle, it is not possible to implement the full set of available measures known from the IT industry. It is reasonable that each CPS component supplier installs its own cybersecurity line of defense to protect itself from being blamed for a successful attack, but the resilience of the entire CPS can be rated and improved only if the vehicle manufacturer specifies, validates and verifies the entire system and the associated processes.

There is no such thing as 100% security. Thus, the improvement of the resilience against attacks is a must, whereby cybersecurity measures are effective enough if the effort of hacking them is unrewarding.

A very powerful measure to increase the resilience is the implementation of cryptography. Both the communication between control units (in-vehicle communication) and the



❶	Electronic Control Unit	Engine Control Module (ECM) or Transmission Control Module (TCM)
❷	In-Vehicle Network	High-speed CAN (HSC), low-speed CAN (LSC), CAN-FD, LIN, FlexRay, Automotive Ethernet (BroadR Reach)
❸	Connectivity Gateway	incl. wired and wireless data links and an integrated diagnostic system
❹	V2C Connection	Vehicle-to-Cloud connection, radio data link, cellular 3G GSM, 4G LTE or 5G
❺	Cloud Environment	Cloud server
❻	Cloud to Intranet Connection	Connection between the cloud and the intranet of the user, for example via Internet Service Provider (ISP)
❼	WiFi Infrastructure	Wi-Fi infrastructure network at the user´s premise (e.g. authorized dealer with service workshop), Ethernet router with cable modem or DSL modem
❽	Diagnostic tester	Diagnostic tester application with graphical user interface (GUI) and guided procedures
❾	Staff	Development engineer, service technician, worker, data analyst, fleet manager

Figure 3 and Table 3: Components of the cyber-physical system for remote diagnostic communication.

ALL IMAGES: SOFTING AUTOMOTIVE ELECTRONICS

Implementation of a gateway that protects the in-vehicle network (e.g. by a firewall)
Implementation of UDS on CAN or UDS on IP
Encryption of the in-vehicle communication
Encryption of diagnostic communication (messages and data)
Protection of the flashware with an RSA signature
Combination of positive responses with conditions (e.g. engine rpm = 0 or vehicle in safe state)
Authentication with password length of at least 11 characters and the character set {0,9…a,z…A,Z} and symbols
Authorization
Implementation of a secure firmware over-the-air (FOTA) process
Authentication of signature/ Signature of data for authentication
Implementation of UDS and Service 0x28 = Authentication
Dynamic increase of time-outs after a specific number of failed attempts or blocking the system completely after (e.g.) three consecutive false attempts.
Geo Fencing
3G (UMTS) and 4G (LTE) Radio Data Link Security: EPS-AKA
WiFi Security: WPA 2, in future WPA 3
Protection against Social Engineering Attacks
Intrusion detection and self-healing mechanisms

Table 4: Examples of measures to increase the resilience against cyberattacks.

diagnostic communication can be encrypted.

Another measure is the implementation of UDS (ISO 14229) as a diagnostic communication protocol. UDS comes with several security measures, meaning diagnostic services such as Diagnostic Session Control (0x10), Security Access (0x27), Authentication (0x28), Secured Data Transmission (0x84), and Tester Present (0x3E).

Table 4 summarizes effective measures to increase the resilience of the diagnostic communication against cyberattacks.

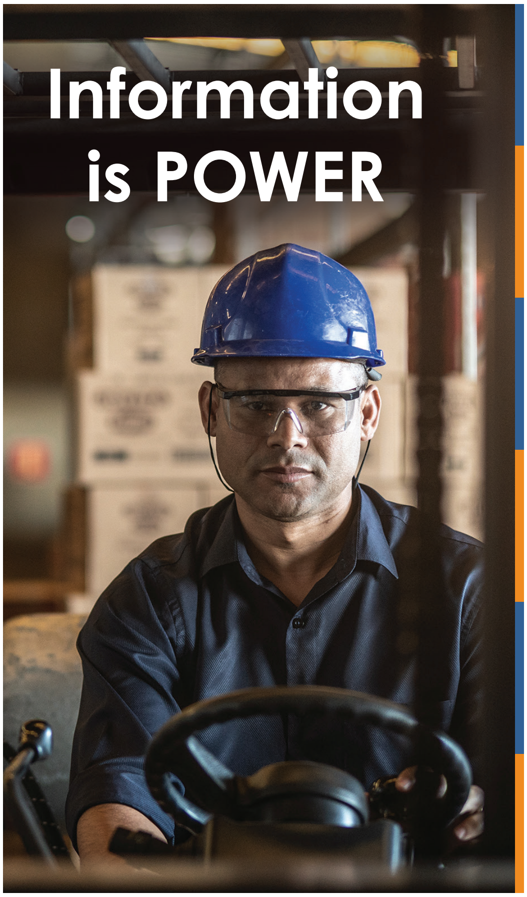
Intrusion detection by OBD

The UNECE 1998 Global Agreement was finalized under the leadership of the European Community, Japan, and the United States. The agreement establishes a process through which countries from all regions of the world can jointly develop UN Global Technical Regulations (UN GTR), for example regarding safety or environmental protection. GTR No 5 = Technical Requirements for On-Board Diagnostic Systems for Road Vehicles "prescribes the requirements for on-board diagnostic (OBD) systems to detect, and, if applicable, record and/or communicate failures of specific vehicle and engine systems that affect the environmental or safety performance of these systems."

Security threats can severely harm the functional safety and finally cause damage to the vehicle/machine or worse, to life and health of people. If a cyberattack affects the safety, it should be detected by the OBD system. The OBD system shall have the capability of detecting malfunctions that affect emissions, functional safety and security.

Reasonable measures must be taken to prevent unwanted intrusion and/or manipulation, detect malfunctions that affect safety, create a fail-safe situation in case of a detected cyberattack, and fight any unauthorized intrusion and manipulation.

Peter Subke, Director Business Development, Softing Automotive Electronics GmbH, wrote this article for *Truck & Off-Highway Engineering*. He is the author of an SAE "deep dive" book on diagnostic communication (www.sae.org/publications/books/content/r-474/) and will participate in the Cybersecurity session at SAE COMVEC 2019 in September.



maxAI™ 430*i*

Advanced Instrumentation
Engine Monitoring System

maximatecc continually looks for innovative ways to bring critical vehicle data to operators and to display it in the brightest, clearest, smartest designs possible. Introducing the maxAI 430*i* engine monitoring system, a rugged, all-in-one instrumentation display for vehicles put to the test every day in the world's most demanding applications — from small construction equipment to large specialty vehicles.

- Fast, easy customization
- Vibrant 4.3" TFT display
- 20 LED telltales
- Sleek, compact design

Contact info@maximatecc.com. maximatecc.com

maximatecc

Free Info at http://info.hotims.com/73020-707