SIH PS No - AK211

BH60M and BH100 with Electronic Transmission

Description of the problem

The Engine, Transmission , equipment dash board system and brake controls equipped with embedded, digital control Electronic Control Units(ECU) for parameters monitoring, display, store and control application. These ECU's are programmable type for changing the configuration depending on power train combinations, customer requirements and field conditions.

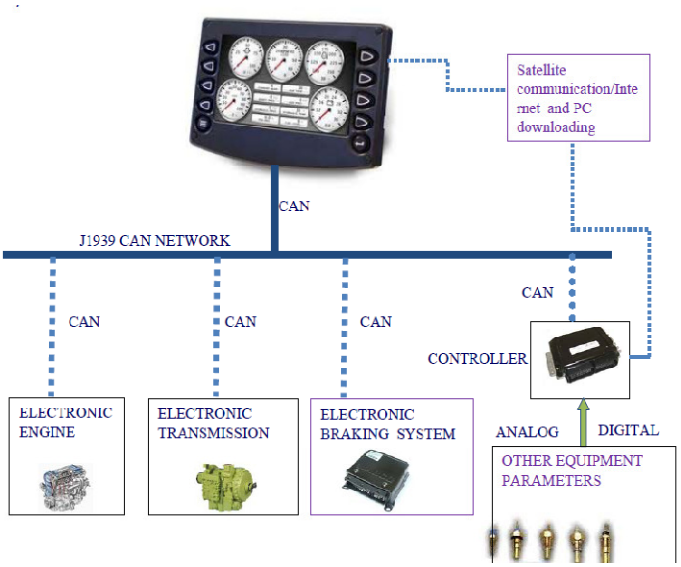
The ECUs are capable of sending vital/critical data of the equipment over CAN J1939 2.0B communication protocol. A data logger with J1939 2.0B protocol having connectivity with GPS/GPRS/Internet, if fitted, is capable of sending the vital data of the equipment to remote systems/computers.

Objective of the project

The equipment may be tried for hacking for-.

1. Un-authorized access of the ECUs.
2. Retrieving of equipment vital/critical data with geo locations.
3. Making malfunction/un-intended function of ECUs by injecting virus causing potential damages to Engine and Transmission.
4. Altering of pre-loaded sequences to change the way of working of Transmission.

Block Diagram for Case Study:



1. The equipment ECUs(Electronic controller unit) are connected in parallel through SAE J1939 CAN network. At the heart of any modern vehicle's interconnected systems is the Controller Area Network bus, or CAN bus. The CAN bus is a single, centralized network bus on which all of a vehicle's data traffic is broadcast. The CAN bus carries everything from operator commands such as "engine/transmission control" or "apply the brakes", to readouts from sensors reporting engine temperature or pressure. The advent of the CAN bus brought about improvements in efficiency and a reduction in complexity while also reducing wiring costs.
2. **Inherently Insecure**: The CAN bus is a 30-year old architecture that was developed for various valid reasons, but security certainly was not one of them. Automakers at the time could not possibly envision the risk of vehicles being hacked decades into the future, nor could the governing bodies that mandated the CAN and OBD standards. The CAN architecture was designed to be lightweight and robust, and those qualities it accomplishes very well. However, CAN contains numerous vulnerabilities that are inherent in its design.
3. **Lack of Segmentation and Boundary Defense**: Network segmentation is a fundamental part of secure system design. If a network is not segmented, a trivial vulnerability in a non-sensitive system component can be exploited to grant access to the rest of the network, including its most critical and sensitive parts.
4. **Lack of Device Authentication**: Another way in which the CAN bus is inherently vulnerable to attackers is the lack of device authentication on the network. The Controller Area Network – as the name implies – is a network of different controllers. Each controller serves a different function.

Some controllers are used to broadcast data onto the bus; an example would be the engine control unit constantly sending a CAN message onto the network containing the current engine speed (RPM) (OpenXC, 2015). This data, once broadcast onto the bus, becomes available to all other vehicular components on the CAN bus whether they require that information or not. Other controllers on the CAN bus constantly listen for specific messages; an example of this would be the controller for the gauge cluster, which constantly listens for RPM messages on the bus so it can update the vehicle's tachometer accordingly. However, the system does nothing to prevent unauthorized devices from joining the CAN bus and broadcasting messages out to any listening controllers. This inherent vulnerability is an attacker's dream. By gaining access to the CAN bus, an attacker can send spoofed messages over the bus. Because CAN utilizes its own native protocol, a would-be vehicle hacker must take the time to learn the CAN protocol before being able to launch an attack.

Users :

BEML and Coal & Non Coal companies (Overseas and Domestic)

Technology that can help address the issue:

New Software and hardware development/ logics

1. Protecting each segment with a proxy and a firewall will greatly reduce an intruder's access to the other parts of the network.
2. The Critical Controls recommend that network level authentication should be used to limit which devices can operate on the network.
3. An implementation of Network Access Control (NAC) and a client certificate infrastructure

Outcome expected:

1. Explore the robustness of the current system and bring out the weak points by hacking into the control software and data stored in ECU.
    a. Un-authorized access of the ECUs.
    b. Retrieving of equipment vital/critical data with geo locations.
    c. Making malfunction/un-intended function of ECUs by injecting virus causing potential damages to Engine and Transmission.
    d. Altering of pre-loaded sequences to change the way of working of Transmission.
2. Security measures to prevent remote access to vehicle electronics.

********** End of Document **********