

Securing the software loading process in cars



Figure 1: Annual arctic driving event in Sweden, demonstrating BorgWarner's torque transfer systems

More and more of the mechanical systems in modern cars are being replaced by electrical control systems in order for car manufacturers to provide improved fuel efficiency and new features such as self-parking cars and other driver assisting features. To support this dramatic shift the number of Electrical Control Units (ECU:s) in modern cars has increased significantly in recent years. It is not unusual that a modern high-end car has up to a hundred ECU:s in total.

Cars are rapidly becoming more computerized

This change has steered the control systems in cars to become more and more similar to computers where software plays a major part in the performance of the vehicle. Because of the increased importance of the software in vehicles there is a need to be able to maintain this software even after it has reached the consumer, by providing the possibility of fixing bugs and adding new features. This is achieved by performing software loading or *flashing* in car workshops during the regular service of the vehicle, in a similar way as, for example, the operating system on a personal computer receives several updates during its lifetime.

Software updates of cars are needed in reality

Real world examples of these kinds of software updates can easily be found in daily newspapers, e.g.:

“Renault, which was on Monday afternoon hauled in front of a government-appointed commission to explain the emissions results for its cars, has now offered owners of certain diesel vehicles a software update to improve its pollution control system. Up to 700,000 vehicles could be eligible for the modifications.”

“Chrysler had already issued a patch in a software update for its vehicles last week, but announced it with a vague press release on its website only. A recall, by contrast, means all affected customers will be notified about the security vulnerability and urged to patch their software.”

Control of the software loading process is lost

However, by providing other parties the ability to modify the software of the on-board ECU:s, there is a risk that the software loading sequence is not done in a correct manner. In the worst case, this could result in an ECU that stops working and therefore needs to be replaced, at a high cost, both for the consumer and vehicle manufacturer.

International standard for the software loading process

The International Organization of Standardization (ISO) has presented an international standard for diagnostic communication in road vehicles called Unified Diagnostic Services (UDS), providing a framework for a software loading sequence. The UDS standard enables a unified approach to how the software loading sequence should be performed, independent of vehicle

manufacturers' specific preferences, thus providing a more secure flashing sequence with minimized risk of corrupting the software on the ECU.

BorgWarner PowerDrive Systems

BorgWarner PowerDrive Systems in Landskrona develops and manufactures torque transfer systems for customers like Volkswagen, Audi and Volvo (Figure 2). The torque transfer systems developed enable all-wheel drive or cross-differential drive for improving the traction while driving. The control of these systems is performed by an ECU.

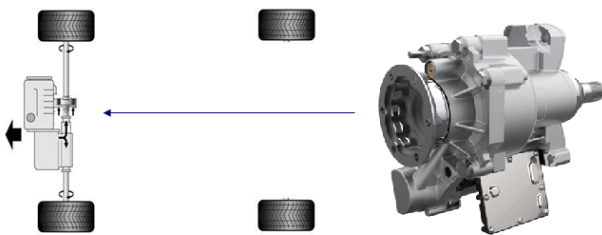


Figure 2: Torque transfer system developed by BorgWarner PowerDrive Systems to enable cross differential drive in front wheel driven vehicles.

Verifying compliance of ECU:s

In order to improve the reliability of the software loading process to the ECU:s used in their systems, BorgWarner PowerDrive Systems needed a way to verify the compliance of ECU:s, to the UDS-standard. This project was able to develop a framework for testing the bootloader¹ software in commercial ECU:s from several different manufacturers according to the UDS-standard, regarding the software loading sequence. By introducing variations of the standard software loading sequence, that are permitted within the UDS-standard, as well as non-acceptable sequence errors, the stability and robustness of the ECU can be tested and improved as bugs are identified.

Identifying weaknesses in both externally and internally developed ECU bootloader software

By being able to write generic test cases that could be run on several different

ECU:s, various requirements and recommendations in the UDS-standard could be tested. In this project weaknesses were identified in both internally and externally developed bootloader softwares.

BorgWarner PowerDrive will continue to use and develop this project to improve the internally developed software as well as quality test externally developed ECU bootloader softwares.

Author:
Richard Pendrill

The complete description of this project can be found in:
Pendrill, R. (2016). "Automation of UDS-based flashing for software testing purposes in CANoe", Master's thesis TEIE-5370, Division of Industrial Electrical Engineering and Automation, Lund University, Sweden
(http://www.iea.lth.se/publications/MS-Theses/Full%20document/5370_full_document.pdf).

1. Bootloader – software which handles the software loading process.