Manipulations on EURO V and VI trucks by suppression of AdBlue injection

Status report from Swiss heavy-duty truck controls

Background

In early 2017, it was discovered that many EURO V-compliant vehicles, and possibly some EURO VI-compliant vehicles, on the roads, especially in Poland and Germany, had been manipulated. According to German media reports, up to 20 per cent of vehicles had been manipulated.

The vehicles had been equipped with what are known as AdBlue emulators, which stop AdBlue injection without the engine management system being able to detect the failing. The vehicles concerned were for the most part from Eastern Europe. The emulators are installed by the drivers or the vehicle owners; the problem does not stem from the manufacturers. The reason for the manipulation is to save costs amounting up to approximately 2,000 euros per year and per vehicle. Heavy vehicle charges (toll fees) are also saved, provided they are designed with the environment in mind, as is the case, for example, in Switzerland.

The situation in Switzerland

The Swiss authorities decided to act, as it was quite likely that Switzerland was also concerned. To that end, they provided the police and customs forces with the basic technical information needed to detect the manipulations, especially in the case of hardware manipulations. Suspect vehicles are immobilized and inspected. If necessary, they are escorted for inspection to professional workshops that have better brand-specific testing devices.

The measures were introduced in February 2017. Since then, about 100 vehicles have been discovered nationwide, nearly 40 of them at the biggest and most important heavy-duty truck control centre alone, in Erstfeld, at the north-south junction of the Gotthard ramp, i.e. the most heavily travelled transit route in Switzerland. The centre controlled about 4,000 vehicles during that time, for a detection rate of about 1 per cent. Most of the vehicles came from various Eastern European countries and Italy.

This Informal Paper has been prompted by one finding: to date, only EURO V-compliant vehicles have been caught, and only in hardware manipulations. In most cases, the vehicles had emulators, but some had a hidden in-built potentiometer that lowered the external temperature of the AdBlue system to approximately -19° C, meaning the system no longer injected AdBlue. However, no manipulated EURO VI-compliant vehicles have been caught so far, and there have been no cases of software manipulation alone, even though the necessary tools are available on the Internet.

A workshop on this subject organized with the police and representatives of vehicle importers produced no further findings of tangible use to law enforcement agencies. It simply established that, from the technical point of view, it is also possible to manipulate a EURO VI system. Professional manipulation of EURO VI systems is reported to be more difficult and therefore probably also more expensive (around 1,000 euros for EURO VI systems as opposed to less than 100 euros for EURO V systems). According to the importers, however, software manipulations may well not be detected in every case, even using brand-specific testing apparatus.

Questions:

- 1. Can technically equipped and trained police and customs officers detect manipulations of EURO VI systems using multi-brand testing devices?
- 2. Are brand workshops in principle able to detect pure software manipulations using <u>brand-specific</u> testing devices?
- 3. Have any pure software manipulations been detected in other countries?
- 4. Are there any technical strategies for countering such manipulations?
- 5. Do the manufacturers' dealer networks receive any support for detecting manipulations, and, if so, what information might be useful for police and customs officers and how could it be made available?