Written questions to Daniel Lange (Faster IT)

EMIS hearing of 16 June 2016

The questions are answered by Daniel Lange (DL) and by Felix Domke (FD).

Overview of questions

No.	Question
1	What is the reason why car manufacturers install functioning emission reduction systems in their cars, which they partly deactivate by software?
2	What parameters are used in order to programme a car's Electronic Control Unit (ECU)? What strategy is pursued by the car manufacturers?
3	Please elaborate on the reporting mechanisms in ECU software development and optimisation of Emission Control Technologies (ECTs). Typically how many people and what types of people (software developers and other ICT experts, engineers, management, etc.) are involved, in particular in the programming of the ECU, and how is the process documented: does the documentation indicate who programmed what part of the software and who gave the order? Are ECU manufactures optimising ECUs according to OEM's specifications or are they only optimised in-house by the OEMs? How is it possible that so many software developers did not go to the public ("whistleblowers") while working on an illegal software?
4	Can you explain how the reverse engineering of the ECU manufactured by Bosch (and typically installed in Volkswagen cars) was performed and what did it reveal? What means (time/technical/financial) did this reverse engineering require? Are there other results of reverse engineering of ECUs as regards ECTs of diesel vehicles?
5	From the technical point of view, under which conditions you would see necessary to use devices to deactivate or reduce the effectiveness of emission control systems, and how likely are those situations? Do these conditions relate to the known ECTs for diesel NOx reduction (SCR and LNT) in the same way if they are used alone, or are there differences if combined with EGR?
6	Can you provide us with a possibly accurate definition of a "defeat device"? When and from whom did you find out for the first time about the possible use of defeat devices by a European or any other car manufacturer?

No.	Question
7	According to your experience and knowledge what are the reasons for optimisation of ECU with regards to the effectiveness of ECT in diesel vehicles? If the ECU optimisation renders ECT ineffective during all or most of the driving of the vehicle under average normal conditions and outside laboratory testing, as revealed by ongoing investigations in the EU (FR, DE, UK), are those optimisation falling under the category of defeat devices?
8	Is it possible to distinguish between test results from cars with normally functioning software systems and test results from cars with defeat devices (or raise reasonable suspicions)?
9	Is it possible to develop a "cheat device" that can be used as a cycle beating technology in RDE-tests? If not, why not? If yes, how could it be prevented? Will more rigorous and well-designed type approval procedure be sufficient to prevent the use of defeat devices? Could including a specific test for detection of various defeat devices during the type-approval, conformity of production and in-service conformity tests be a solution? How difficult would it be to develop a software test as part of the type approval system?
10	In connection to the previous question and answers, would you support the view that defeat devices can be detected by currently available instruments and testing methods, or would you share the view that more sources are necessary to invest in defeat devices screening in the test laboratories? Or would you see the current problems rather in the way how the test laboratories carry out the tests (e.g. test cycles) in comparison to robust on-road testing enabling to verify defeat strategies?

Individual answers

1	What is the reason why car manufacturers install functioning emission reduction systems in their cars, which they partly deactivate by software?

DL: Using the emissions reductions systems comes at a cost, e.g. the consumption of DEF (Diesel Exhaust Fluid, brand name "AdBlue") or the wear on the catalytic material inside the catalytic converter or the piling up of soot and ash inside a particulate filter. The emissions reduction systems are designed to (as closely as possible) meet the allowed emissions in the regulated gases and particles when fully operational. This may go to the point of some cars being barely drivable when in emissions testing mode ("dyno mode"). The emissions reduction systems are primarily optimized to meet the tests. These tests, esp. the NEDC (New European Driving Cycle[1]), do not reflect the bandwidth of real world usage scenarios. Thus car manufacturers have to optimise for other usage scenarios as well. And in the past there was little incentive to do so and still keep an optimum in emissions of the regulated gases.

1 "New" as in last updated 1997.

2	What parameters are used in order to programme a car's Electronic Control Unit (ECU)? What strategy is pursued by the car manufacturers?

DL: The software inside an engine ECU is mostly programmed to emulate models of physical processes. So a module may e.g. estimate the consumption of petrol by counting the injections. This number, together with estimated pressures in the air intake and measured temperatures before and after the engine block may then be used to calculate a raw NO_x emissions value. Which in turn may impact the amount of DEF being injected.
The software inside the ECU is often partially created by modelling the physical processes from scientific research and physical testing. The models are then adopted to engine specifics through configuration and calibration (tuning). This process involves iterative physical testing. And the reduction of physical tests is one of the foremost cost down measures in vehicle development. Automotive engineers are always complaining they do not have enough hardware of upcoming vehicles and engines to test. So the calibration/tuning phase has come under pressure in the last decade to be less iterative and e.g. use more up-front simulation work instead.
The whole approach to engine software development can probably be best explained historically. Physical implementations of control technology have been gradually replaced by software. And then these implementations continued to grow but kept the inherited pattern of model + configuration + calibration.

3	Please elaborate on the reporting mechanisms in ECU software development and optimisation of Emission Control Technologies (ECTs). Typically how many people and what types of people (software developers and other ICT experts, engineers, management, etc.) are involved, in particular in the programming of the ECU, and how is the process documented: does the documentation indicate who programmed what part of the software and who gave the order? Are ECU manufactures optimising ECUs according to OEM's specifications or are they only optimised in-house by the OEMs? How is it possible that so many software developers did not go to the public ("whistleblowers") while working on an illegal software?

DL: The development of an engine ECU requires the close co-operation of the core engine developers, software engineers, configuration engineers, various testing function (engine, full vehicle, regulatory compliance, …), purchasing, legal departments and the target (launch) markets usually represented via sales & marketing functions. Typically multiple hundred people are involved in engine development on the side of an OEM (car manufacturer) and a similar amount of people at various suppliers, usually including the manufacturer of the ECU, external developers, testing companies / facilities and companies involved in vehicle certification for the target markets. The process is documented at minuscule details e.g. every change needs a change request document and various levels of approval, every software release is accompanied by change documentation and test results from automatic and/or manual test runs. It is always possible to identify who requested a change, who authorized it, who implemented it and who tested / signed it off.
Due to the principle explained in Q2 above (model + configuration + calibration) of ECU development ECU manufacturers need to adjust the model or the model capabilities (e.g. variable mappings) quite frequently so there is a constant back and forth between the ECU manufacturer and the OEM. The OEM can set variables (=turn knobs) but when it needs new variables or changed behaviour it specifies a change request against the ECU manufacturer so that a new

knob to set is implemented and exposed as a configurable variable. Usually a few "resident engineers" are on-site with the OEM and take part in joint test-drives to facilitate the back-and-forth.
Whistleblowers do not have a sufficient legal protection in Europe. See the inability/unwillingness of the European Community member states to grant asylum to Mr. Snowden. So while I believe many people will have had doubts and may have tried internal ways to get their companies to comply with the intent of regulation (and not barely the letters or not even that), risking the excellent salary at an OEM for an extended stay under legal scrutiny and away from their families didn't seem a sufficiently compelling option.

4	Can you explain how the reverse engineering of the ECU manufactured by Bosch (and typically installed in Volkswagen cars) was performed and what did it reveal? What means (time/technical/financial) did this reverse engineering require? Are there other results of reverse engineering of ECUs as regards ECTs of diesel vehicles?

FD: For the particular ECU of the Volkswagen Sharan (MY2012) that was analysed, a Bosch EDC17, the goal was to find both the mechanism that was used to detect the test cycle, as well as the effect of that detection on emission control.
The analysis revealed - slightly simplified - that the method of detection was to monitor the driven distance over time (since engine start), and comparing that with the expected distance (at a given time) when driving a test cycle (NEDC in this EU5 car, but further analysis of other market's cars showed similar treatment for corresponding test cycles). Further, a few environmental variables have to be in the correct range as well, most notably fuel temperature.
It also revealed that detection of the test cycle, on this particular SCR-equipped car, would cause the SCR system to be forced back into a "full model" ("NH3 storage model" with on-board efficiency checks enabled), whereas the car by default – due to parameters being set appropriately – operates in a "simplified model" (that does not take NH_3 storage into account, and has all efficiency checks disabled), which was configured to limit DEF dosing. The result is that the car operates more clean in detected test situations than in most non-test situations. (Further analysis showed that other parameters outside the SCR system, for example EGR, are also affected by the switch.)
In general, reverse engineering an ECU can be performed in the following way:

1. The first step is to obtain a binary image of the used firmware (i.e., the software in the computer-readable format that it is stored in the ECU). This can either be retrieved directly from an ECU (often by using existing diagnostic features), or it can be obtained from a software update for the ECU (which are sometimes made available to end-users).
2. The second step is to convert the binary (computer-readable) image into human-readable text. A program called "disassembler" can reverse one of the final steps (the "assembler" stage) of the translation from the original source code and the binary. However, the "disassembler" cannot recover all details that have been present in the original source code (i.e. the form that was used to initially develop the software) – for example all names, comments and some higher-level structures are lost in the process and cannot be retrieved automatically, and must be reverse-engineered by hand, sometimes helped by semi-automated tools.
3. The third step is to understand enough of the software structure from the disassembly to find individual functionality. For the Volkswagen ECU, FD initially targeted find-

ing the SCR functionality. Helpful pointers are error codes that relate to SCR (which can be found in the disassembly), or standardized measurement methods (OBD-II functionality).

4. To help this step, live data of the internal variables can be obtained from the vehicle during operation. Usually the diagnostic functionality available over the OBD-II bus does not only allow to read standardized measurements, but also allows to read ECU-specific data ("read-memory-by-address"). This allows to capture most internal ECU state, and allows to verify if important functionality (that has been reversed in the previous step) has been understood correctly by comparing expected with actual outputs.
5. Once enough of the functionality is understood, a hypothesis of a defeat device can be verified. For example, the hypothesis for the Volkswagen ECU was, after observing that it usually operates in the "simplified SCR model", that the car switches to the "full model" during a test cycle. The goal then was to find conditions that would force the software to switch to the full model. Analysing the possible conditions that would cause such a switch lead to the discovery of a function that would lookup "time since engine start" to a minimum and maximum value (using two piecewise-linear curves), which were compared to the actually driven distance. Plotting these curves against the NEDC reference curves showed a close fit. A prediction was made that when these conditions are satisfied, the car would switch to the main model, increase DEF dosing, and finally produce fewer NO_x in otherwise similar driving conditions.
6. Finally, this prediction must be verified. In the Volkswagen case, it's possible to satisfy all conditions by driving a reasonably correct NEDC cycle within a specific temperature window. Live data (as well as tailpipe measurements) were collected from such a test, and the hypothesis of the "switch" was successfully verified. Further driving cycles with targeted, intentional deviations from the required conditions at specified times, while monitoring the internal ECU data, ensured that the criteria were understood correctly and were not a just co-incidence.

It must be stressed that even with a full understanding of the exact conditions that are used to "switch" the motivation behind these conditions can't be shown. The result of reverse-engineering an ECU cannot be the detection of a defeat device; it can only show which exact conditions exist that cause a reduction in the ECT efficiency. It's up to the car manufacturer to find (or fail to find) a sufficient technical explanation why the found conditions are necessary for engine protection and/or safety, and don't represent a defeat device as described in the law.

5	From the technical point of view, under which conditions you would see necessary to use devices to deactivate or reduce the effectiveness of emission control systems, and how likely are those situations? Do these conditions relate to the known ECTs for diesel NOx reduction (SCR and LNT) in the same way if they are used alone, or are there differences if combined with EGR?

DL: There is a well known definition for AECDs (Auxiliary Emissions Control Devices) in US regulation ("*Auxiliary Emission Control Device* (AECD) means any element of design which senses temperature, vehicle speed, engine RPM, transmission gear, manifold vacuum, or any other parameter for the purpose of activating, modulating, delaying, or deactivating the operation of any part of the emission control system." from 40 Code of Federal Regulations (CFR) 86.1803-01)

The European directive made this the basis for describing the "defeat device" directly as "'*defeat*

device' means any element of design which senses temperature, vehicle speed, engine speed (RPM), transmission gear, manifold vacuum or any other parameter for the purpose of activating, modulating, delaying or deactivating the operation of any part of the emission control system, that reduces the effectiveness of the emission control system under conditions which may reasonably be expected to be encountered in normal vehicle operation and use[.]"
from REGULATION (EC) No 715/2007)
The US American wording makes it more simple to explain: AECDs may be necessary to protect the engine during a startup phase (of may be 30 seconds or a minute) and in extreme conditions (e.g. when overheating). If they are increasing emissions (EI-AECDs – Emission Increasing AECDs) they must be declared and justified during vehicle certification. Now much around the Diesel emission scrutiny for Opel, Daimler, Renault, Fiat or Peugeot is around EI-AECDs that are very "generous" with arguing for engine protection in a way that they work fully only in the incidental temperature window used for testing (usually 20-30°C) and reduced the emissions treatment outside a manufacturer specific temperature window that lies around that testing temperature window.
EI-AECDs should be the exception (as in <1% of the vehicle operation) and the EU regulation finds the excellent wording "under conditions which may reasonably be expected to be encountered in normal vehicle operation and use". We seem to just lack the ability (or willingness) to enforce this.
EGR cools the engine (as there is less combustible material in one intake stroke compared to a Non-EGR operation) and thus helps to reduce the NO_x formation right at the source. There are issues with "too much EGR" e.g. around drivability, particulate mass production and water depositing in the intake but here again "switching off" is the cheap route, solving the problem by good engineering the better route but obviously more costly and time consuming.

6	Can you provide us with a possibly accurate definition of a "defeat device"? When and from whom did you find out for the first time about the possible use of defeat devices by a European or any other car manufacturer?

DL: "'*defeat device*' means any element of design which senses temperature, vehicle speed, engine speed (RPM), transmission gear, manifold vacuum or any other parameter for the purpose of activating, modulating, delaying or deactivating the operation of any part of the emission control system, that reduces the effectiveness of the emission control system under conditions which may reasonably be expected to be encountered in normal vehicle operation and use[.]"
from REGULATION (EC) No 715/2007)
Now this definition is not good. Because VW tries to evade confessing to a defeat device in Europe by nitpicking on what a defeat device specifically is, see
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/transport-committee/volkswagen-group-emissions-violations/oral/27791.pdf.
As stated in my introductory talk, I suggest to get out of the "arms race" with the automotive industry and rethink the approach to emissions regulation to be more generic, hugely simplified, neutrally controlled and thus vastly more efficient and much harder to evade. Regardless of whether that evasion has happened deliberately or accidentally.

7	According to your experience and knowledge what are the reasons for optimisation of ECU with regards to the effectiveness of ECT in diesel vehicles? If the ECU optimisation renders ECT ineffective during all or most of the driving of the vehicle under average normal conditions and outside laboratory testing, as revealed by ongoing investigations in the EU (FR, DE, UK), are those optimisation falling under the category of defeat devices?

DL: Managing the emissions of a modern Diesel engine under all environmental and vehicle usage conditions is a complex task. Obviously “reducing complexity” by switching off emissions treatment (say) below 17°C is an easy way out of this complexity and not detected during certification testing (as that happens at ~20-30°C). So time pressure, cost pressure or lazy engineering are possible reasons for such short-cuts. Bad management is the reason for unrealistic time pressure, cost pressure and badly led engineering teams.
As such emissions increasing codes are active “under conditions which may reasonably be expected to be encountered in normal vehicle operation” the are legally a defeat device.

8	Is it possible to distinguish between test results from cars with normally functioning software systems and test results from cars with defeat devices (or raise reasonable suspicions)?

FD: Test results can raise reasonable suspicions, but alone are not sufficient to prove the existence of a defeat device.
Each ECT has a number of key parameters that can be monitored over time to allow a deduction of whether the system is activated or not; a list of non-exhaustive examples is: for EGR, this would be the EGR rate itself, for LNT, it would be the combustion lambda value (indicating regeneration), and for SCR, it would be the amount of injected DEF.
There are other parameters that allow to characterize the efficiency of the applied techniques; for EGR, this is the raw emission rate (NO_x concentration before exhaust treatment systems), for LNT and SCR this would be the ratio between NO_x concentration before and after the treatment system.
It's important to note, however, that these values are only comparable under identical engine operating points, and often also depend on medium and long terms effects that can be hard to observe. This makes it difficult to directly compare two situations and understand whether the efficiency of the exhaust treatment was intentionally decreased, or was just decreased because of physical limits. Controlling as all relevant parameters is required to produce tests results that can be quantitatively compared. If controlling a parameter is not directly possible, the effect must be understood (for example, a particle filter regeneration must be detectable) and tests must be repeated in case such a parameter caused a deviation from a previous run.
In general, the approach to find defeat devices using tests is to look for non-continuous relationships between input parameters and emissions, where a small change in input parameters results in an unnaturally large change of output parameters.
As a simplified example, if a car produces about 10% more NO_x at a 5% higher engine load, that can probably be explained by the different operating conditions due to the higher engine load. However if the same car produces about 500% more NO_x at a 5% higher engine load, even though all other parameters are (within a reasonable range) constant, it indicates that the car operates in a different mode.
This alone is not necessarily an indication of a defeat device, however, as there are various legitimate reasons to operate temporary in non-emission optimized operating points. One example is

a particle filter regeneration that requires high exhaust temperatures which will result in additional fuel burnt. But also hard safety limits that are required for proper engine operations can cause such abrupt changes. (It must also be noted that it's well possible to build more sophisticated defeat devices that do not cause abrupt changes, but instead gradually transition from one mode to another.)
If such suspicious behaviour is found, the exact conditions that cause the behavioural change must be characterized. One way is to look at the ECU software, for example with reverse-engineering, another method is to do more directed (A/B) testing to eliminate unused but possible detection criteria. Once the exact switch criteria has been found, the motivation for the criteria needs to be found. If the criteria can't be explained with a physical necessity, the car manufacturer needs to be able to explain why the criteria was necessary and does not resemble a defeat device.
DL: As stated in my introductory remarks, I would turn the process around. The OEM submits each software release for certification and specificities all changed and explicitly all AECDs (see Q5 for a definition) and their justification. Not specifying an AECD or not submitting the software release at all leads to immediate voiding of the vehicle approval and a significant fine per affected vehicle. As all software releases are stored with the (national) governing institutions no arguments about software content can ever arise again. And the tedious and error-prone work of reverse engineering is avoided for all cases but to prove a software found in the field is identical to a submitted software release version. Which is rather trivial.

9	Is it possible to develop a “cheat device” that can be used as a cycle beating technology in RDE-tests? If not, why not? If yes, how could it be prevented? Will more rigorous and well-designed type approval procedure be sufficient to prevent the use of defeat devices? Could including a specific test for detection of various defeat devices during the type-approval, conformity of production and in-service conformity tests be a solution? How difficult would it be to develop a software test as part of the type approval system?

FD/DL: In general, RDE exercises more driving situations, which ensures that the ECT are fully operational and produce compliant behaviour over a much wider operational range. This could be seen to reduce the incentive of defeat devices since the ECT must demonstrably work in these more natural driving situations that are resembled by the RDE tests. However as long as there are still downsides of activating the ECT (e.g. increased fuel consumption, reduced vehicle agility), some incentive will remain to detect the cycle and behave differently in a non-test situation.
There are criteria that allow an RDE test to be easily detected (for example increased exhaust backpressure due to the PEMS device), and be treated differently from a normal driving situation. Further, even RDE tests are not exhaustive; many typical driving scenarios will not be part of the test. The nature of the remaining cycle detection criteria will make it harder to detect defeat devices when looking at the ECU from a black box perspective (i.e. observe inputs and outputs, but no internal state), because there are so many input variables that exhaustive testing of all combinations is impossible to do. This is true to some extend even with a simulation model of the ECU (i.e. the ability to simulate arbitrary driving situations purely in software); in that case, the ECU may even detect being simulated instead of operated in a real vehicle.
As said earlier: DL suggests to not mend the broken system by applying yet another fixture but to invest some time and brain power into simplifying regulations but strengthening enforcement. E.g. why not have every company, NGO, government body define as many RDE tests as they like. And vehicles need to perform in these according to specification and type approval. Regard-

less. The EU regulation would only define what an RDE test is and how the measurements are to be performed, documented and published. Use the big data approach and crowd sourcing, that's what they are good for. Now this means “conformity factors” would turn into “average real world performance” by type model. A EURO 7 (or 8) “Vehicle X” could score an average of 60% of the regulatory emissions maximum and may be more appealing than – say – a “Vehicle Y” that scores 85% on average. Also this way average fuel consumption values would be 1:1 in line with resulting emissions.
Notice the authorized measurement companies supporting national regulatory bodies have not found anything wrong with VW diesel engines or other OEM's products until after the ICCT study was published. They really have not qualified to be the exclusive gatekeepers in the next rounds of regulations.

10	In connection to the previous question and answers, would you support the view that defeat devices can be detected by currently available instruments and testing methods, or would you share the view that more sources are necessary to invest in defeat devices screening in the test laboratories? Or would you see the current problems rather in the way how the test laboratories carry out the tests (e.g. test cycles) in comparison to robust on-road testing enabling to verify defeat strategies?

FD/DL: Standardised testing procedures cannot be exhaustive and are always predictable by definition, which allows the OEMs and ECU manufacturer to target these tests with special conditions. They optimise for the wrong thing, to “beat the test” but not to fulfil the intent of the regulation.
One aspect of a solution in randomising parameters to make test detection less simple and more easy to spot. Another aspect is to require verifiable proof that all functionalities present in the ECU that affect emission control (AECDs) are properly documented as part of the type-approval process. For any limitations that reduce effectiveness of the ECT (such as temperature limits) it must be documented and verifiable why and how these limits were chosen.
This documentation and ideally the software and tools to build it should be publicly available.
We should not accept that intellectual property rights hamper our ability to scrutinise software that human lives depend upon. Only public research can validate both the documented limitations as well as the overall ECU behaviour. And if issues arise they can be neutrally assessed and not skewed to limit a perceived potential damage to national (economic) interests.
Publicising and neutral reviewing of ECU algorithms gets even more important as we turn to electric vehicles and autonomous driving. We should know what algorithms drive us at 100 km/h and what their boundary conditions are, how they have been validated and where corners have been cut. These reviews will save lives just as adhering to emissions standards would have saved many Europeans from contracting respiratory diseases. So this is an important field for proper regulatory action. Consider forming an experts work group to produce a EURO 7 (or 8) regulation that is simple, transparent, well enforced and unavoidable. By design. For the OEMs this will lead to clearer, simpler regulation and thus faster and cheaper type approvals. And a requirement to have their software development processes and quality control in order.