Article citation info:
KMIEĆ, M., WEBER, M., ROMIJN, M. et al. Application of automotive safety design methodologies to the development of Euro 7 emission control systems including on board monitoring. *Combustion Engines*. 0000, **XXX**(X), xx-xx. https://doi.org/10.19206/ CE-141291

Mateusz KMIEĆ
Matthias WEBER
Marcel ROMIJN
Dave MATEWS

Combustion Engines
Polish Scientific Society of Combustion Engines

Application of automotive safety design methodologies to the development of Euro 7 emission control systems including on board monitoring

ARTICLE INFO

Received: 18 July 2021
Revised: 14 August 2021
Accepted: 16 August 2021
Available online: 15 September 2021

Euro7 and California HD-OBD present a shift of approach in emissions control. Legislative bodies concentrate on individual vehicle conformity to standards during its lifetime on top of type approval processes in test environment. The main change is NO_x trackers in software and sensors in the exhaust pipes of all vehicles. As a consequence of constant supervision not only single point faults are taken into account in the analysis, but also cumulative parameter drift of components due to aging. To achieve normative requirements and prevent emission standards violation during exploitation, methodologies known from automotive functional safety domain and SOTIF are used to evaluate and modify a propulsion system design. An illustrative example of analysis is presented in the paper.

Key words: *OBD, Euro 7, emission control, robust design, design evaluation*

1. Introduction

Today's automotive development cycles are around 3 years [1]; new legislation norms can extend to requiring 4 years. Looking into the future, currently negotiated norms have to be considered now; otherwise, it will not be possible to sell the product. The article discusses regulations that will appear in coming years and development methods that are now transferred from other domains into the OBD domain.

For three decades, the emission characteristics of internal combustion engines have been increasingly gaining attention – the focus on clean transportation resulted in several normative and legal requirements which the vehicles need to fulfill [2]. Due to the development of better measurement equipment and increased computing power of ECUs placed on board and detected differences between declared, accredited, and actual measured emission, there is an evolution of emission control design approaches.

The previous generation approach with regulations Euro 5/V, China 5/V and older USA regulations was to design and balance all emission controls to produce valid emission levels of all relevant pollutants. The design was verified on near-series production vehicles on a chassis or engine dyno according to emission cycles. The type approval was conducted with, at minimum, an aged catalytic converter (DOC, SCR, 3W-cat). During this test, CO_2 emission was verified as well.

Since the previous procedure misses real-life exploitation parameters, for current generation Euro 6/VI [3] and China 6/VI, it was decided to include PEMS (Portable Emissions Measurement System) to pre-series cars and verify the emission limits on a public road with RDE (Real Driving Emissions) driving, traffic, and ambient conditions. The procedure applies to measurement with also, at minimum, an aged catalytic converter. To ensure compliance in the In-Service Conformity with Euro 6/VI, US EPA and California ARB [4] demand that PEMS testing is performed on randomly selected series vehicles. Additionally, for Euro VI (heavy-duty), PEMS measurement has also been required with a similar principle as RDE. China VI for heavy-duty has similar requirements with minor differences in the measurement protocol.

As a next step in evolution, regulations have demanded additional means above adding PEMS equipment to have data on real-life emissions systems performance. The California ARB demands that data from the tailpipe NO_x sensor is sorted by engine load and then stored in the vehicle engine management system, readable by the OBDII scan tool. The California ARB can stop any random series vehicle on the road and read out the stored tailpipe NO_x data for analysis, therefore being able to read data from the history of that vehicle. China VI has a very similar requirement, except instead of long-term storage in the vehicle, the data is reported by telematics to a server of the Chinese authorities.

The latest evolution is the demand for OBM (On Board Monitoring) that is part of the proposals for Euro 7/VII [5]. Other than storing data from tailpipe sensors as California and China [6] are demanding, the Euro 7/VII proposal demands a diagnostic in the vehicle software that will trigger a warning to the driver if tailpipe emissions (averaged over a certain driving distance which is still to be defined by legislation) have exceeded a threshold limit. Firstly the tailpipe emission data collection by NO_x sensors will be obligatory. The other sensors are to follow.

Tailpipe monitoring of consumer vehicles serves two purposes:

– Detection of design flaws of the released system. If a significant number of field reports surpass the emission limits, the design was not robust enough, and the manufacturer will have to improve it. The design needs to consider all conditions during vehicle usage and its exploitation up to aging and mileage limit.
– Detection of emission failure of individual vehicles. Regardless if there is a single point failure or combina-

tion of parameter drift resulting in violation of thresholds- it will be detected, and the owner will be prompted. As a result, the owner will have to replace components or drivetrain until the limits are reached again or alternatively purchase a different vehicle.

The practical consequence of new Euro 7 with on-board monitoring design is compared in Table 1.

Table 1. Comparison of analysis depth required for Euro6 and 7 norms

Norm/analysis of the effect on emissions:	Euro 6/VI with OBD	Euro 7/VII with OBM
Aging	Emissions achieved for type approval only with aged catalyst system and mildly aged overall for in service conformity.	Emissions achieved with actual aging overall is monitored for every vehicle for the whole lifetime
Tolerances	Mostly limited to production tolerances (aging = 0)	Production and aging
Failure modes	Norm defined Single point failure/deviation	Multi-point cumulative failures/deviations
Diagnostic capabilities	Only norm defined elements have to be diagnosed	Diagnostic capability over all relevant components of a system- to allow identification and replacement of problematic element

To achieve the required depth of system analysis and reach design goals required with Euro 7 OBM norm, one needs to incorporate a structured design and analysis method. To fulfill the OBM while still offering pinpointing of the root cause, it is also necessary to have a system wide approach to Emission Diagnostics and not a Component or Subsystem Approach as used nowadays in the industry. A structured methodological approach is also recommended as the need for comprehensive knowledge to overlook the complete Emission Reduction System to the detail can only be found in a few Specialists. To assist these experts and enable other engineers to design a comprehensive and complete Emission Reduction System, we suggest using the well-established lifecycle, design, and analysis methods from Functional Safety.

Both Functional Safety/SOTIF and OBD domains have established methods that are fit for this purpose:

– FUSA/SOTIF:
  - Determining safety goals on vehicle level and propagating them down to individual system components, including performance criteria.
  - Comprehensive failure/deviation analysis methods: HARA, FMEA, FTA, FMEDA.
  - Introduce OBD lifecycle based on safety lifecycle of the project;
– OBD
  - Analysis of tolerances combinations and aging effects.

The paper aims to show that mentioned methods are fit for emission domain and emission system development compliant to Euro 7 OBD norm.

2. Method

To show the stated thesis, a simplified model of the emission system is used. The methodology bases on the proven in-use safety lifecycle defined in ISO 26262:2 is used [7].

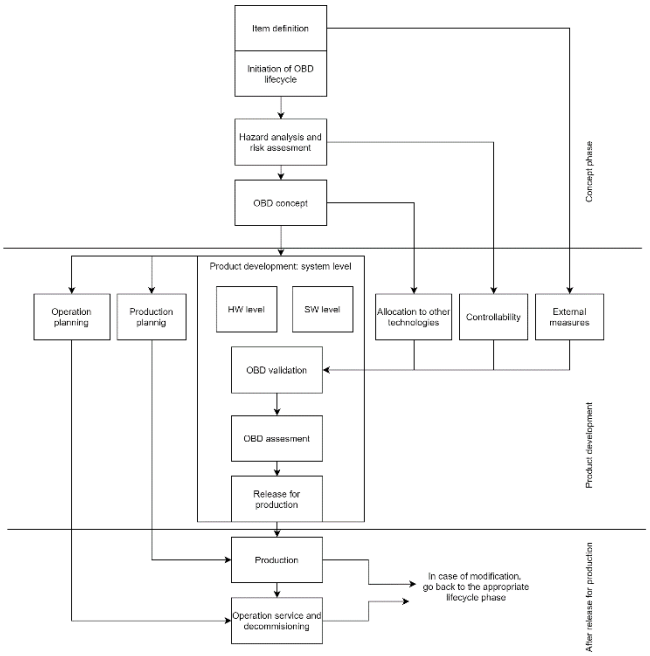

Fig. 1. OBD OBM lifecycle based on FuSa lifecycle [7]

The proposed OBD/OBM lifecycle consists of several steps that ensure systematic analysis of an item and provide argumentation for analysis completeness. The top-down approach is the most straightforward way to ensure complete NO_x supervision. In severe cases of lawsuits, it provides proof of reasonable effort taken to minimize potential risks.

– Item definition:

The very first step to conduct is to define the subject of the analysis. The scope is called an Item. The item is defined by a set of high-level functions, boundaries, interfaces, assumptions, working conditions, and other environmental influences necessary to have a strict description of the item in question. The description shall be comprehensive in the way that the Items function is well understood

– Hazard analysis and risk assessment(HARA):

The HARA procedure consists of defining potential hazards that an item can pose to the user or environment. The identified (emissions compliance) hazards are then evaluated in terms of probability, controllability, and severity. Combining those three numbers (usually rated on a scale of 1–10), one can judge the required emission integrity level (EMIL). Emission Integrity levels span from EMIL 1 to 5 grades. At EMIL 1, there is no or too little impact on emissions and the system so, unless spelled out in the regulation, no OBD monitor is needed. At EMIL 5, there is a potential HW or Mechanical redesign in order. With each EMIL level, there is more care and more amount of analysis and redundancy required. Based on such assessment, the emission goals (EG) are formulated based on

hazards. The EGs inherit the required emission integrity level (EMI) from HARA analysis.

– OBD concept:

With the knowledge from previous steps, the OBD concept is developed considering the preliminary architecture of an item. The requirements derived from emission goals are allocated to the elements of the system. The OBM concept is also added here, although that is a given from the regulation. At this level, FMEA analyses are performed on the Function and Interface level.

– Product development at the system level:

In this phase, the system is designed according to the OBD concept and other functional requirements. Also, demands following from the effect of the OBM concept on the system are taken into the design. This step may include external solutions that are out of item boundary. The system architecture and technical requirements are specified. The technical assumptions, human behavior assumptions and hazard assumptions are also validated during this phase. HSI, which is the HW-SW interface, needs to be defined at this stage as well.

– Product development at the hardware and software level:

Inheriting from system design and requirements, the HW and SW detailed design and implementation are conducted. This phase also includes testing and validation on the corresponding level of detail. FMEA analysis is repeated or extended here but at HW/SW level.

– Production, operation, service, and decommissioning:

This part of the process runs parallelly, starting with product development on the system level, ending at the SOP (start of production) date.

Tied into this is the type approval and in service conformity preparation, which includes a dry-run test before actual approval and in-service conformity.

The process part aims to define unique characteristics of the item that are relevant for emission. This includes production repeatability, tolerances, calibration, End Of Line (EOL) tests. Additionally, operation and service instructions and unique characteristics have to be defined as well as decommissioning of faulty or worn out parts.

Most of the mentioned steps will be illustrated based on the proposed exemplary system. The development on HW/SW level and testing will be briefly mentioned due to the demonstrative character of the analysis for which detailed HW/SW solution is not relevant.

In the following chapters, we will apply the methodology to an exemplary system.

3. Example

The chosen system is based on a medium-duty diesel engine emission control system intended for Euro 6d_final/Euro 7 or Euro VI_e/Euro VII norm. Only NO_x emissions will be analysed. The turbocharger section is cut out for clarity. The system consists of two EGR loops for High and Low pressure, two urea dosers with supply, and a series of catalytic converters, including DOC, SDPF, SCR, and AMOX converter. Additionally, the system has several temperature, pressure NO_x and NH_3 sensors.

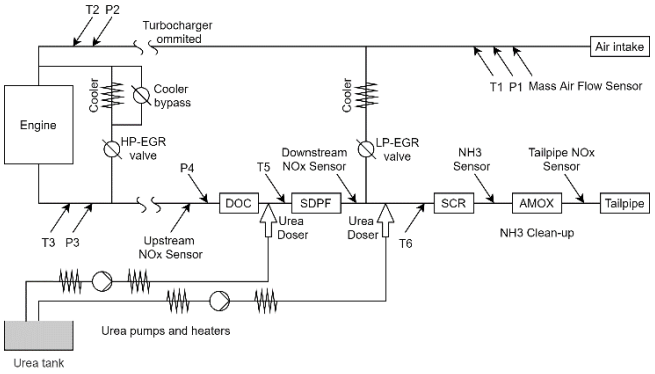

Fig. 2. Medium-duty diesel engine emission control system

3.1. System(item) definition

In the item definition, one needs to define a boundary that separates the system under consideration from the outside world. In our case, it contains engine, intake, and exhaust pipe. Consequently, the interface, which means flows or signals crossing the boundary, is air intake, tailpipe and heat exchange with the surroundings. In this example, we also do not consider the fuel system to simplify the example furtherly.

As this article is a demonstration example, we will only analyse parts relevant for NO_x control.

3.2. System(item) main function

The identification of system main function occurs on abstract level. One shall not consider the technical realisation of the system but its purpose. The system function in our case is to reduce NO_x emission.

3.3. Emission goal definition

According to the methodology of the OBD lifecycle, one should run a HARA analysis over the functionality of the emission reduction system to determine the emission goals. In this example, however, we simplify this step by using the emission goal defined in Euro 7/VII proposals [5].

Table 2. Emission goals

Emission goal ID	Emission goal
EG 1	The system NO_x emission shall not exceed the limit value of X [g/km] over the averaging window of Y km.

3.4. System elements

To analyse potential failures main functions of system elements need to be defined.

Table 3. System elements sub-functions

System element	**Sub-function**
HP-EGR loop	Increase inert gas in combustion chamber
LP-EGR loop	Increase inert gas in combustion chamber
SCR	Neutralize NO_x into harmless components
SDPF	Neutralize NO_x into harmless components shortly after cold start
AMOX	Neutralise NH_3 particles
DOC	Oxidise leftover hydrocarbons, HO and PM
Urea tank	Stores ammonia

Table 3cont.

Sensors	**Sub-function**
AMF	Provides feedback for EGR loop.
Upstream NO_x	Measure NO_x coming from engine
Downstream NO_x	Measure NO_x coming from engine
NH_3	Measure NH_3 level
Exhaust NO_x	Provides final feedback on NO_x elimination efficiency
T1, P1	Provides temp and pressure of incoming air
T2, P2	Provides pressure and temp of gas entering the engine from turbocharger
T3, P3	Provides temperature and pressure of exhaust gases directly at the exhaust manifold.
P4	Provides pressure at the entrance of catalytic chain
T5	Provides gas temperature at the entrance of SDPF
T6	Provides gas temperature at the entrance of SCR
Actuators	**Sub-function**
H-EGR valve	Controls recirculation rate of HP EGR
L-EGR valve	Controls recirculation rate of HP EGR
H-EGR cooler	Controls cooling power of HP-EGR loop
L-EGR cooler	Controls cooling power of HP-EGR loop
Urea Dosers	Controls urea dosing rates
Urea Heaters	Heat the urea to prevent freezing
Urea Pumps	Provide pressure for urea installation

4. OBD concept

4.1. System analysis

The next step is to take exemplary elements and analyse them according to standard failure modes and their effects (FMEA):

Table 4. FMEA of SCR element, function neutralise NO_x

FM ID	Failure mode	Failure Mechanism	Potential Effect
1	Too Long	SCR too cool	Excessive NO_x emissions
2	Too Short	SCR too hot	Faster Aging, Excessive NO_x emissions
3	Too Slow Response	Urea doser underperformance	Excessive NO_x emissions
4	Too Fast Response	Urea doser overperformance	Excessive NH_3
5	Reverse	No effect	No effect
6	Intermittent	Urea doser malfunction/ mixer malfunction	Excessive NO_x emissions
7	Fluctuating	Urea doser malfunction/ mixer malfunction	Excessive NO_x emissions
8	No	SCR clogged	Loss of power
9	Less	SCR coating covered/aged	Excessive NO_x emissions
10	More	No effect	No effect
11	Follow Command with Different Outcome	Urea doser malfunction/ mixer malfunction	Excessive NO_x
12	Follow Command with the same outcome by accident	Urea doser has lower max efficiency than design, but the engine has a low load.	No effect
13	As Well As	NH_3 spillage	Excessive NH_3

Table 5. FMEA of H-EGR valve element, function: controls recirculation rate of HP EGR

FM ID	Failure mode	Failure Mechanism	Potential Effect
14	Too Long	see slow response	No effect
15	Too Short	see slow/fast response	No effect
16	Too Slow Response	slow-moving valve (high resistance)	In transients, the EGR mass flow stays behind
17	Too Fast Response	No effect	No effect
18	Reverse	Incorrect connection/wiring	EGR mass flow is uncontrollable
19	Intermittent	high resistance in moving (PID is struggling) / command transfer is interrupted	In transients, the EGR mass flow stays behind
20	Fluctuating	high resistance in moving (PID is struggling)	In transients, the EGR mass flow stays behind
21	No	valve is stuck in a closed position	EGR mass flow is uncontrollable
22	Less	valve is stuck/blocked below the target/blockage in flow/leakage to ambient	EGR mass flow is less than the target
23	More	valve is stuck/blocked above the target	EGR mass flow is more than the target
24	Follow Command with Different Outcome	Any of the above	EGR mass flow deviated from the target
25	Follow Command with the same outcome by accident	Any of the above	NOTE: If no transient is commanded; if low EGR is requested or high EGR is requested – any of the above failures can be hidden (latent)
26	As Well As	Any of the above	Any leakage or blockage will also impact the pressure to the intake of the turbine

Table 6. FMEA of upstream NO_x sensor element, function: measure NO_x upstream

FM ID	Failure mode	Failure Mechanism	Potential Effect
27	Too Long	No effect	No effect
28	Too Short	No effect	No effect
29	Too Slow Response	deposits on sensor	Too little urea added, L-EGR malcontrol
30	Too Fast Response	noise	Wrong amount of urea
31	Reverse	Wrong value	Excessive NO_x emissions + clogging of ECR
32	Intermittent	Loose wiring	Wrong amount of urea
33	Fluctuating	EMC noise	Wrong amount of urea
34	No	Connection lose	Lack of feedback – Excessive NO_x emissions or clogging of catalysts

Table 6cont.

35	Less	Deposits on sensor	Too little recirculation and amount of urea clogging of catalysts – too big emissions
36	More	To thin wiring	Too significant recirculation, too much urea, clogging of catalysts
37	Follow Command with Different Outcome	No effect	
38	Follow Command with the same outcome by accident	No effect	
39	As Well As	No effect	

Beyond an FMEA (bottom-up), an FTA (top-down) is performed to have evidence of completeness and better insight into relations between failure modes.

With the SCR system, most failure modes lead to excessive NO_x emissions. FM ID 4 and 13 are the exemption as they cause excessive NH_3, but for these situations, the AMOX catalyst is still in place to break down the NH_3. FM ID 12 is a particular case; there can be Excessive NO_x emissions, but current engine out NO_x production is (e.g. due to low load) low enough that the failure mode is not currently violated. In ISO 26262, such a failure is called a Latent failure. This also forms an issue in OBD and OBM, despite previously not having a defined name for it.

The Function FMEA is, in principle, valid for both SDPF and the downstream SCR. There is a difference, however. The SDPF is more exposed to high temperatures and is critical to being operational at the lowest possible temperature following a cold start. Also, it is affected first by any substances from the engine combustion, including substances that can lead to poisoning and coverage of the coating. Should the SDPF fail, however, the downstream SCR is to a certain degree capable of compensating. Therefore, the failure modes are the same, but how they occur and the exact emissions effect they have is deviating between SDPF and downstream SCR.

In the EGR function FMEA, the failure modes correspond to the incorrectness of EGR mass flow. A too low or late EGR mass flow leads to a too-small level of inert gas in the combustion chamber, resulting in increased engine-out NO_x. Too much or too early affects the combustion stability or performance due to an excessive amount of inert gas in the combustion chamber. An EGR failure leading to an increased level of engine-out NO_x does have the benefit that SDPF and SCR can reduce some of the excess NO_x within their abilities. However, a counter effect is that some of the excess NO_x is returned to the intake side via the LP-EGR. A special note is to FM ID 22 and 26 to point out that EGR failures that are leakage or a blockage affect the turbocharger setup. This effect can disturb intake air mass availability to the combustion chamber and enhance the effect. The FM IDs 16, 19, 20, and 25 are all connected to transient operation. In theory, an engine could be operated in steady-state and/or mild transients only, hiding the failure mode of EGR. As previously stated, there is a risk for a latent fault. However, the chances are less as the transient operation does occur in both emissions test cycles and real-life vehicle operations.

The upstream NO_x sensor has a very different Function FMEA in respect to its role. Sensors in themselves are less relevant, but their incorrect reporting of measurements is disturbing the control systems. The upstream NO_x sensor is, just as the middle NO_x sensor, the main parameter for the SCR control of SDPF and SCR, respectively. Their failures disturb the reduction of NO_x.

After discussing the Fault Modes found by the FMEA, an example set of Fault Modes is selected for the further demonstration of the methodology.

In the previous approach of OBD, there was the possibility to discard some of the failure modes as not relevant for the Emission Goal. These failure modes would not be capable of pushing NO_x tailpipe emission above the limit. The OBM approach does not allow this anymore, and all fault modes need to be discussed. While it is still true that some failures on their own would not be able to push tailpipe NO_x over the limit, they would be able to do so in combination. As in this paper, the space is too limited for a complete discussion, a representative set of fault modes is chosen to proceed with the example.

With that, the following is chosen:

OBD: One SCR with reduced efficiency due to coating coverage FM ID 9 that has reached a point where, despite possible compensation of, e.g., downstream SCR, the tailpipe NO_x over an emissions cycle has reached the OBD limit.

OBM 1: An amount of SDPF reduced efficiency due to coating coverage FM ID19. As the failure mode of coating coverage originates from a foreign substance or engine oil, in reality, the SDPF will be affected, but to a lesser degree, the SCR downstream will have reduced efficiency due to coating coverage. In addition, the NO_x sensors upstream of each SCR will be affected as well, which is causing them to fail as slow response (FM ID 29). These effects together reach a tailpipe NO_x value over an average time of driving that exceeds the limit.

OBM 2: The entire NO_x system under consideration has suffered from aging. The EGR systems both suffer from a small level of soot buildup (FM 22 in a minimal degree), both SCRs suffer from the aged coating and aged urea dosers (FM ID 3 and 9), and finally, the sensors have also suffered from age effects (FM ID 29 and 35). None of these deviations on its own is a reason for concern but all combined, they reach tailpipe NO_x value over an average time of driving that exceeds the limit.

The next step is to create OBD and OBM concepts based on the chosen set of fault modes.

4.2. Creating the OBD and OBM concept

For SCR, a common approach is to compare the NO_x sensor upstream and NO_x sensor readings downstream of the concerning SCR, possibly corrected or performed by NH_3 sensor readings. The OBD concept would take the SCR failure at the NO_x OBD limit on the emissions cycle and then develop a concept to detect that specific SCR with that specific failure level. As such approaches are common

in the industry and covered by literature [8], further details are not added.

To extend OBD into the OBM world, one needs to also take into account multi-point faults. This is further split into two classes: this class of faults is characterized by the fact that each fault does not violate the emission goal solely, but the sum of the faults does.

1. Dependent faults
   One fault directly leads to another fault which in turn causes a direct violation of the emission goal.
2. Independent faults
   Statistically independent random faults that combined cause emission goal violation.

The way to proceed is to define abstract failure levels first. One can consider that process a fuzzy logic membership function assignment on an abstract level. Please note that at this stage of analysis, the membership function does not have strict physical meaning. One has to assume normalization of failure level: 0% is the part that runs perfectly, 100% is the part that has failed completely. Then let the normalised deviation be divided into 3 classes: 30%, 60%, 100% where class 30% means the number is less or equal 30%, class 60% is 31–60% and so forth [9]. With this step, we discretize the spectrum so that it is possible to conduct predicate reasoning on clauses [10]. As the next step, the table with combinations of discretized failure levels of elements is constructed according to mentioned OBM. Let the given discrete deviation level be called symptom after Isermann et al. [11].

Table 7. Discretised failure combinations- symptoms and failure judgement, EG violation judgement

Element	30%	60%	100%	Judgement	EG violation
SDPF	1	0	0	normal uniform wear	0
SCR	1	0	0		
SDPF	1	0	0	Accelerated SCR wear – LP-EGR underperformance	0
SCR	0	1	0		
SDPF	1	0	0	SCR Single point failure	1
SCR	0	0	1		
SDPF	0	1	0	Early stage oil contamination	0
SCR	1	0	0		
SDPF	0	1	0	Uniform wear	0
SCR	0	1	0		
SDPF	0	1	0	LP-EGR underperformance	1
SCR	0	0	1		
SDPF	0	0	1	SDPF Single point failure	1
SCR	1	0	0		
SDPF	0	0	1	Late stage oil contamination	1
SCR	0	1	0		
SDPF	0	0	1	Uniform wear	1
SCR	0	0	1		

As can be noticed, the table will grow exponentially with an increased number of elements and failure stages. However, such a bottom-to-top approach ensures analysis of all possible combinations. As a result of analysis, one can be sure which parts of the system have to be supervised either directly or monitored by combining several measurements.

Additionally such structure can be directly converted into set of logical sentences – IF <clause 1> AND <clause2> …<clause N> THEN <Judgement> which are easily implementable in SW. The next step is to design emission monitoring mechanisms that will give the physical base to the abstract statements of failure stages.

The regulator gives the OBM concept. It must be detected when tailpipe NO_x as averaged over a specific driving distance/condition exceeds the limit, regardless of what caused it.

However, if the OBM triggers due to e.g. the late stage oil contamination as in OBM 1 a parallel detection is needed, informing the symptoms of what is wrong and where the effort for repair must go. Our example would be a turbo oil seal or a piston oil ring combined with the SPDF and SCR. This diagnostic must reproduce the OBM result, but with information on the root cause.

In the simplified form, the SCR efficiency is expressed in a ratio of measured NO_x upstream of the SCR and measured NO_x downstream of the SCR. Dynamic effects and NH_3 effects on the sensors are significant disturbances in this monitor, but for the sake of simplicity, these are considered to be captured by averaging for this explanation. Typical SCR OBD algorithms used in today's vehicles use averaging over 60 minutes or more of driving. We will define a perfectly healthy SCR here as one that removes 100% of expected NO_x and 0% failing if the removal is at 98% level. A 30% failing we will define as 94% removal. The 60% failing at 90% removal and 100% failing at 86% removed NO_x or worse.

Restricting to oil contamination, this means:

1. IF SDPF efficiency is 93–90% efficiency AND SCR efficiency is 100–94%, THEN do nothing
2. IF SDPF efficiency is 89% or less AND SCR efficiency is 93–90%, THEN store fault code information that oil or other foreign substance has covered the SCR coating and point towards the relevant repair procedure. Note that the driver likely comes to the workshop with the OBM warning activated.
3. IF SDPF efficiency is 100–94% AND SCR efficiency is 89% or less, THEN store fault code information that single source failure has affected the SCR and point towards the relevant repair procedure. Note that the driver likely comes to the workshop with the OBM warning activated.
4. Etc.

4.3. Realization of the concept

Difference between OBM and OBD

With OBD, the development activities focus on the concept definition of a diagnostic. This diagnostic involves sensors to measure those parameters that indicate the single failure mode that needs to be found. Once the diagnostic concept is created, the concept must also be verified against tolerances within this sensor-to-failure mode relation and the risk for Type I and Type II errors, where Type I is a false alarm and Type II is a genuine error that is not detected [12].

With OBM, the diagnostic is given by the regulator. Here the focus lies very differently because the OEM has

the interest to ensure that failure modes are detected not only by the OBM monitor but also by own diagnostics that ensure efficient repair is possible. This implies that the existing OBD must be in place. However, in addition, a collection of multiple small failures but with a common source (OBM 1: common source is foreign substances or oil) are detected. A big delta to OBD is here that the failure modes of each individual contributing emissions system (EGR, SCR, etc.) are far smaller than in the case of pure single fault OBD. The more minor effects emphasize the issues of sensor tolerances and aging. It needs to be ensured that aging and drift, together with other noise factors, can be distinguished from the actual sensor signal.

In the situation of OBM 2, there is an added complexity. Even though none of the components or systems may be perceived to be having a failure mode, the sum is still enough to trigger tailpipe NO_x limits. Here, an OEM is interested in ensuring that this situation only occurs after at least the minimum mileage and vehicle age for emissions durability (full useful life) have been passed. For consumer satisfaction, however, likely a higher mileage or vehicle age target is demanded.

Allocation

With OBD, the allocation is a non-complicated matter. The SCR diagnostic to detect the single point fault has to be allocated to the SCR software. In that ECU or software section, the correct information is available at the correct accuracy and sample rate.

With the OBM 1 example, the situation becomes more complex. The symptom analysis, however, will help significantly. The symptoms analysis will first remove any combinations of failure modes that are irrelevant or physically impossible. It will highlight those that have a common failure mode.

With OBM 1, the deviation that each part can have due to aging is now defined. In traditional emissions control, this is defined by the aging done to demonstrate the durability of the emissions system on the emissions cycle. In the case of OBM, however, there must be a safety margin added as not every vehicle will age each component the same. Some vehicle will have increased EGR soot loading while other will have more SCR coating aging. The target for the OEM is to define an allowable aging deviation per component.

Analysis of the implementation

To analyse the implementation for OBD, a tolerance investigation is required. This can be based on computational simulation, vehicle measurements, or a mixture of both. The systems Type I and Type II errors need to be defined

For the OBM 1 situation, the approach is the same. Each diagnostic that detects the individual elements and that feeds into the symptom analysis can be wrong by itself with Type I and Type II error,

For the OBM 2, the verification requires a Monte Carlo simulation or other identification algorithms [13, 14]. As is known to be done based on new component tolerances, it is verified by the simulation what the chances are of a tolerance combination that can lead to tailpipe NO_x exceedance. Should this be the case, then either 1) the specific combination of tolerances is considered rare enough to be acceptable, 2) the specific combination of tolerances is made impossible, or 3) the tolerances that are most dominating in the analysis are reduced by demanding or developing elements with stricter tolerances. This approach is for OBM 2 repeated, however, with those tolerance deviations added caused by aging.

While practical experience with OBD has shown that starting later in the vehicle development cycle with designing OBD can sometimes result in challenges (e.g., sensor types and positions that have already been determined despite being sub-optimal for OBD) with OBM, this is a far more significant concern. If a component is chosen that has in certain situations aging to the point it would reach the OBM level, then every vehicle that is exposed to said situation would trigger an OBM warning. For an OEM to reach the demanded and internal targets, this may mean that said component cannot be used. Such information must be available as early as possible in the development cycle.

4.4. Integration and test

When applied for safety engineering, the safety methodologies can result in SW implementation of algorithms, failure rate (FIT) rate demands on hardware components, tolerance demands on mechanical components, and even redundancy in design. Also, they can demand testing from unit tests up to vehicle validation.

With OBD, this situation existed to a minor degree as apart from demanding sensors for measurements, OBD did not directly affect the hardware. Tolerances are a concern with OBD and may, at times, demand changes. Failure rates, however, are of no concern in OBD development.

OBM does take even the last step and does include failure rates, especially where it concerns aging effects that can trigger before the emissions durability or warranty term is passed. Despite the integration work and testing as demanded for OBD, for OBM, specific testing and/or simulation work is required in establishing the failure rate.

5. Conclusions

In order to fulfill the complex requirements of diagnostics development in the age of OBM new methods have to be introduced in the field. A lifecycle approach based on functional safety was proposed and described for emission system case. With a simplified system example the processes and analysis methods that make up the lifecycle were demonstrated. Each step of the lifecycle was either described or partly analysed in order to prove that the methods are fit for purpose. In authors opinion, the example and outcomes prove that such a systematic approach can handle the complexity of OBD development in the OBM environment providing additional benefits such as argumentation of completeness.

Nomenclature

AMOX	ammonia oxidation catalyst
CARB	California Air Resource Board
DOC	diesel oxidation catalyst
ECU	electronic control unit
EG	emission goal
EGR	exhaust gas recirculation
EMIL	emission integrity level
FIT	failure in time (per 10^9 hours)
FM	fault mode
FMEA	fault mode effect analysis
FMEDA	failure mode effects and diagnostic analysis
FTA	fault tree analysis
FuSa	functional safety
HARA	hazard analysis and risk assessment
HW	hardware
OBD	on board diagnostic
OBM	on board monitoring
OEM	original equipment manufacturer- car producer
PEMS	portable emission monitoring system
RDE	real driving emission
SCR	selective catalytic reductor
SDPF	SCR-catalysed diesel particle filter
SOTIF	safety of intended functionality
SW	software

Bibliography

[1] SASAKI, T. How the Japanese accelerated new car development. *Long Range Planning*. 1991, **24**(1), 15-25. https://doi.org/10.1016/0024-6301(91)90020-O

[2] VESTRENG, V., NTZIACHRISTOS, L., SEMB, A. et al. Evolution of NO_x emissions in Europe with focus on road transport control measures. *Atmospheric Chemistry and Physics*. 2009, **9**(4), 1503-1520. https://doi.org/10.5194/ACP-9-1503-2009

[3] Commission Regulation (EU) 2016/646 of 20 April 2016 amending Regulation (EC) No 692/2008 as regards emissions from light passenger and commercial vehicles (Euro 6) (Text with EEA relevance). *European Commission*. http://data.europa.eu/eli/reg/2016/646/oj

[4] Final Regulation Order for HD OBD II Regulation § 1968.2 Malfunction and Diagnostic System Requirements 2004 and Subsequent Model-Year Passenger Cars, Light-Duty Trucks, and Medium-Duty Vehicles and Engines. *California Air Resource Board* 2019.

[5] DILARA, P. The future of clean cars in Europe: EU Green Deal and EURO 7. *Sino-EU Workshop on New Emissions Standards and Regulations for Motor Vehicles* 2021. https://ec.europa.eu/jrc/sites/default/files/the_future_of_clean_cars_in_europe_eu_green_deal_and_euro_7.pdf

[6] WANG, J. China's next phase of automobile emission standards. *Sino-EU Workshop on New Emissions Standards and Regulations for Motor Vehicles* 2021. https://ec.europa.eu/jrc/en/science-update/sino-eu-workshop-presentations

[7] ISO 26262-2:2018 Road vehicles – Functional safety – Part 2: Management of functional safety. https://www.iso.org/standard/68384.html (accessed on 16.07. 2021).

[8] DE OLIVEIRA COSTA, L., ROSSIN, F. Optimizing the on board diagnostic system (OBD) to monitor for reduction of the SCR catalyst conversion efficiency using the NO_x sensor. *SAE Technical Paper* 2010-36-0198. 2010. https://doi.org/10.4271/2010-36-0198

[9] GU, Y., LI, J. Multi-state system reliability: a new and systematic review. *Procedia Engineering*. 2012, **29**, 531-536. https://doi.org/10.1016/J.PROENG.2011.12.756

[10] GELGELE, H.L., WANG, K. An expert system for engine fault diagnosis: development and application. *Journal of Intelligent Manufacturing*. 1998, **9**, 539-545. https://doi.org/10.1023/A:1008888219539

[11] ISERMANN, R. Supervision FDD methods – an introduction. *Control Engineering Practice*. 1997, **5**(5), 639-652. https://doi.org/10.1016/S0967-0661(97)00046-4

[12] GRAVES, S., BISGAARD, S., KULAHCI, M. et al. Accelerated testing of on-board diagnostics. *Quality and Reliability Engineering International*. 2007, **23**, 189-201. https://doi.org/10.1002/QRE.784

[13] DANTAN, J.-Y., QURESHI, A.-J. Worst-case and statistical tolerance analysis based on quantified constraint satisfaction problems and Monte Carlo simulation. *Computer-Aided Design*. 2009, **41**(1), 1-12. https://doi.org/10.1016/J.CAD.2008.11.003

[14] NIGAM, S.D., TURNER, J.U. Review of statistical approaches to tolerance analysis. *Computer-Aided Design*. 1995, **27**(1), 6-15. https://doi.org/10.1016/0010-4485(95)90748-5

Mateusz Kmieć, MEng. – Roben Automotive Poland.
e-mail: *mateusz.kmiec@roben-automotive.com*

Matthias Weber, Dipl.-Ing. – Roben Automotive Poland.
e-mail: *matthias.weber@roben-automotive.com*

Marcel Romijn, Dipl.-Ing. – Roben Automotive Netherlands.
e-mail: *marcel.romojn@roben-automotive.com*

Dave Matthews, MSc. – Roben Automotive USA.
e-mail: *dave.matthews@roben-automotive.com*