Technical University Kaiserslautern

Department of Computer Science

Sindelfingen

Validation of Drive-train Controllers and Test Automation

Project Work

Surendra Kumar Aralapura Mariyappa

Supervisors:

Prof. Dr. Karsten Berns, Chair of Robot Systems

M.Sc. Markus Schroth, Mercedes-Benz AG

Sindelfingen, March 2020

TABLE OF CONTENTS

Table of contents	Page No.
1. Abstract	1
2. Introduction	2
3. X-By-Wire	3
3.1 Electronic Throttle Control	4
3.2 Electronic Accelerator System	4
3.2.1 Accelerator Pedal	5
3.2.2 Command Unit	5
3.2.3 Throttle Body	5
3.3 Motor Control Module	5
3.4 Shift-By-Wire	6
4. ISO 26262	7
4.1 Vocabulary	8
4.1.1 Definition of Terms	8
4.2 Management of Functional Safety	8
4.3 Concept Phase	8
4.3.1 System Definition	8
4.3.2 CPC System Definition for Conventional Vehicle	10
4.3.3 CPC System Definition for Hybrid Vehicle	11
4.3.4 CPC System Definition for Electric Vehicle	12
4.3.5 Functional Safety Concept	14
4.4 Product Development at System Level	15
4.4.1 Technical Safety Concept	16
5. 3-Level Monitoring Concept	17
5.1 Level 1	17
5.2 Level 2	17
5.2.1 Functional Monitoring Level	18
5.3 Level 3	17
6. Conclusion and Future Work	21
7. References	22

ABBREVIATIONS

AC - Alternating Current

ASIL - Automotive Safety Integrity Level

CC - Cruise Control

CPC - Central Powertrain Controller

DBW - Drive-By-Wire

DC - Direct Current

ECU - Electronic Control System

E/E - Electrical and Electronic

EGAS - Electronic Gas Accelerator System

ESP - Electronic Stability Control

ETC - Electronic Throttle Control

FMEA - Failure Modes and Effect Analysis

FTA - Failure Tree Analysis

HARA - Hazard Analysis and Risk Assessment

ISO - International Standard Organization

LIN – Local Interconnect Network

MCAS - Maneuvering Characteristics Augmentation System

CAN – Controller Area Network

OBD - On-Board Diagnostic

OEM - Original Equipment Manufacture

SBW - Shift-By-Wire

QM - Quality Management

XBW - X-By-Wire

1. Abstract

The automotive safety has been recently of a great concern among the automakers after few fatal incidents that led to the death of passengers. Since then, the development of highly reliable automotive software without faults/defects has been the top priority which also requires validation of software. Along with the validation, automakers also do the software and hardware verification of the automotive embedded software development life cycle according to V-model. But software/hardware verification will not guarantee us that developed embedded system/product will be free from faults. Verification will just ensure if all the requirements are implemented in a software/hardware or not, whereas validation provides the quality assurance before installing a system in vehicles. In automotive world, usually validation of embedded software will be conducted as a software test at both system and vehicle level. At the system level, only the developed embedded software and its interactive components (Hardware-in-Loop) will be used and will evaluate the response of software and components to the faults in the software. However, at vehicle level, we personally experience the vehicles reaction to the faults in the software. During the project work, the redundancy of automotive software was validated through injecting the faults into the software at both system and vehicle level, mainly for the conventional, electric and hybrid drivetrain controlling software.

2. Introduction

Until 1970, the perception of human beings on automobile was just that of mechanical components, starting from window, steering, braking, gearing, acceleration and other factors that used to run on principle of mechanics and gears. Nonetheless, the introduction of Electronic Control Unit (ECU) in the1970s by Volkswagen in co-ordination with Bosch group defined a new way for the innovation in automotive sector. At present, even the low-end cars are equipped with nearly 100 ECUs for controlling different functionalities like opening and closing of throttle valve depending on the driver's request. On the other hand, high-end models like BMW 7 series contain almost close to 150 ECUs. This ergonomics has paved a way to overcome the limitations of mechanically and hydraulically controlled system along with increasing the vehicles comfort, safety on road, fuel efficiency and emission control in order to meet the emission standards specific to the region [1].

Alternatively, ECU is also referred as Embedded Automotive Controller or Embedded Automotive Software. Depending upon the functional areas, different embedded automotive controllers are being designed, developed, tested, verified and validated against the requirements through Model-in-loop (MIL), Software-in-loop (SIL), Hardware-in-loop (HIL) and Process-in-loop (PIL) according to International Standard Organization (ISO) 26262 standards. Embedded automotive software experts classified entire vehicle system into four different functional areas such as Chassis, Drive train, Body and Telematics.

Over the half century, the Original Equipment Manufacturers (OEM) along with the automotive suppliers developed various ECUs for regulating the functionalities of automobile, which includes Engine Control Module, Transmission Control Module, Brake Control Module, Body Control Module, Electronic Stability Control, Anti Braking System, Suspension Control Module, Battery Management System and many other systems. In other words, the ECU is like the brain of the car which controls multiple functionalities of the car, just like the brain controls human muscles [6]. In addition to the ECUs main functionalities like Cruise Control (CC), Electronic Stability Program (ESP), anti-braking system, power steering, vehicle manufactures incorporate their high-end vehicles with ECUs for providing new features like a night vision display along with lending the assistance for driver while driving.

In contrast, providing a new feature requires a new ECU each time, which increases systems complexity and the total number of communication networks within the vehicle and demands for more space together enhancing the cost and weight of the vehicle [3].

In order to overcome above-mentioned drawbacks, Daimler AG has come up with a new embedded software architecture called '3-Level Safe Software Architecture' as shown in the

Figure 9. The 3-level safe software architecture propels for the development of Central Powertrain Controller (CPC), more importantly for Powertrain domain, which acts as an interface among driver's input devices, individual powertrain controller and other controllers of vehicle like chassis, body and telematics. The important thing to note here is that, 3-level safe software architecture is being used in all functional areas of vehicle for the development of embedded software. However, the focus here is only on drive-train embedded software.

3. X-BY-WIRE

A sophisticated technology was first introduced in aviation industry under the name 'Fly-By-Wire' technology to eliminate the mechanical connection among the pilot's input devices, controllers, actuators and other components. The goal was to reduce the weight of the flight along with providing a convenient response to the pilot's inputs by controlling the movement of actuators. The operation of flight controls by pilot will be turned into electronic signals, which are passed onto the controllers and actuators through the wire/bus system, hence the term X-BY-WIRE (XBW) [8].

Automakers have switched from mechanical to hydraulic controlled system to electronically controlled systems to resolve problems such as engine control accuracy to improve fuel economy, to avoiding uncontrolled skidding, to the latest 'Internet of Things/Connected Car' concept. The Electronically Controlled Systems are preferred due to their better precision and cost efficiency. In addition, they also facilitate emission free vehicle, comfortable driving along with new driver friendly functions. This led to implementation of Throttle-By-Wire in 1980s. Since then, XBW has emerged as a state of art of technology.

Eventually this has resulted in introduction of Drive-By-Wire, Shift-By-Wire, Door-By-Wire, Wiper-By-Wire, Lighting-By-Wire and Brake-By-Wire systems. Nevertheless, still vehicle manufactures equip their automobiles with mechanical or hydraulic controlled systems as a backup in association with Electronically Controlled System or embedded software [9].

The XBW system finds itself difficult to be accepted by the automobile manufacturers as it has to be proven that "all the necessary safety measures are followed" according to ISO 26262 during development [9].

Major automakers consider Toyota Lexus LS350 accident in 2009 as an example for the failure of XBW technology, which occurred due to "unintended acceleration". After that, Toyota recalled almost 9 million cars and paid $1.2 billion penalty in 2014 [10]. This also led 'International Organization for Standardization' (ISO) to define an international standard for functional safety of electrical/electronic systems for road vehicles in 2011 [10].

3.1 Electronic Throttle Control

Electronic Throttle Control (ETC) is basically a Drive-By-Wire (DBW) system. DBW was first achieved by BMW in its 7 series in 1980s. The reason behind ETC concept was to replace the mechanical link between accelerator pedal and internal combustion engine with sensors, actuators and controller [8].

The problem with ETC was that it was provided with only one position sensor to perceive the angle of accelerator pedal upon the driver's action as shown in the below Figure [17].

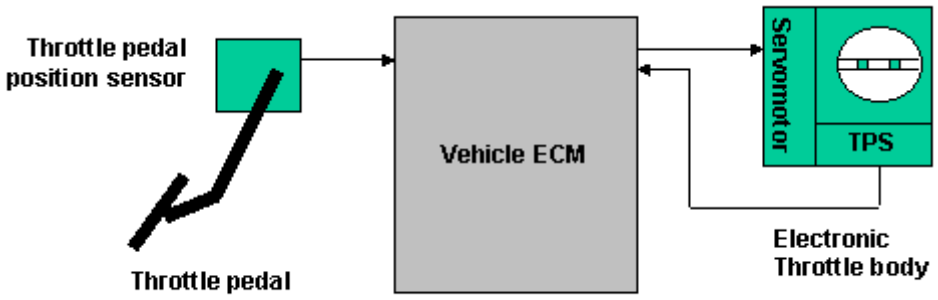

Figure 1. System definition of Electronic Throttle Control [17].

Majority of automakers consider recently occurred Boeing 737 Max 8 fatal incident as a lesson. As stated earlier, XBW was first discovered in aviation industry. Based on the XBW technology, Boeing, the world's leading flight manufactures and the rival of AIRBUS, designed and developed an electrical and electronic (E/E) system called 'Manoeuvring Characteristics Augmentation System' (MCAS). The function of MCAS was to move the horizontal stabilizer trim upwards for preventing the "plane's nose from getting too high" (Ostrower, 2018, para 4) to avoid the risk of stalling. The MCAS would be activated, when angle of plane's nose exceeds a threshold value. Conversely, there was only one sensor to sense the angle of plane's nose. The controller had no redundancy sensor 2 to verify the sensor 1 values, when the former sensor read false angle. Even after deactivating MCAS, continuous false reading from sensor reactivated the MCAS. As a result, MCAS took the flight control from the pilot leading to the death of passengers [7][15].

3.2 Electronic Accelerator System

Electronic Accelerator System, also known as EGAS has two position sensors at the accelerator pedal and a controller and electric actuator at the throttle valve as shown in Figure 2.

Sensor 1 and Sensor 2 sense the driver's torque request and transmit the driver's demand into the controller. Then controller does the calculation to the obtained value and commands the electric actuator for the opening and closing of throttle valve based on the calculation [4].

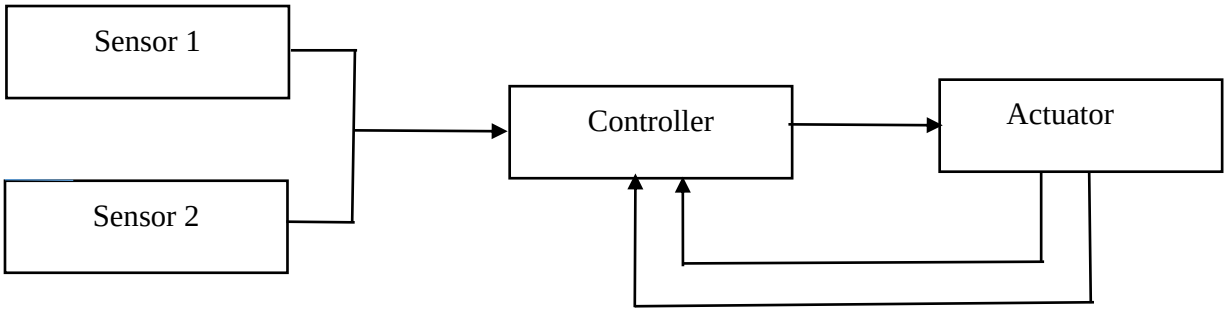

Figure 2. System definition of EGAS [4].

3.2.1 Accelerator Pedal Module:

There will be two potentiometers (accelerator pedal sensors) at the accelerator pedal, which grasp the position of accelerator pedal to trigger the throttle valve as shown in the above Figure. In doing this process, driver's request should be fulfilled. For this, the controller will determine the amount of opening and closing of throttle valve along with considering the present engine temperature and engine revolution [5].

As we see in Figure 2, we are using two sensors to sense the position of accelerator pedal. The reason for this is to provide redundancy. In case of wrong value from sensor 1, controller will validate the value of sensor 2 against value of sensor 1 and vice versa in some cases [5].

3.2.2 Command Unit:

Calculation of torque to be produced according to driver's demand will be done by command unit. Once the Controller receives driver's torque input, it will actuate the throttle body based on the calculation. Sometimes, controller has to take the request/action from other controllers like CC, ESP into account while calculating the extent of opening and closing of throttle valve as shown in the Figure 5 [5].

3.2.3 Throttle Body:

Throttle unit consists of a throttle drive (a direct current engine) and a throttle angle sensor. The throttle angle sensor senses the current position of throttle and transmits it to the controller, depending upon the current position of throttle valve and driver's input. Controller simplifies the desired position of throttle valve [5].

3.3 Motor Control Module

The drive train of electric vehicle consists of less components, controllers as compared to conventional, and hybrid vehicles as shown in Figure 8.

Figure 3. System definition of Motor Control Module.

The working principal of motor control module is similar to EGAS, except combustion engine will be replaced with electric motor. In electric vehicle, inverter is used to convert the direct current from the battery into alternating current. The electric motor/inverter controller regulates the conversion of AC to DC to generate the driver's desired torque from the electric motors.

3.4 Shift-By-Wire

Historically, the vehicle was designed to be put in drive mode, neutral mode, park mode, and reverse mode with the help of gear lever connected to manual/automatic transmission mechanically. With the changing technology, most of the modern cars are equipped with automatic transmission. As a result, increase in the number of gears, favors the elimination of mechanical space between shifter and transmission along with making a way for shift-by-wire. The reason behind the replacing the mechanical joints between the gear levers and the transmission with electronic controls is identical to Drive-By-Wire [18].

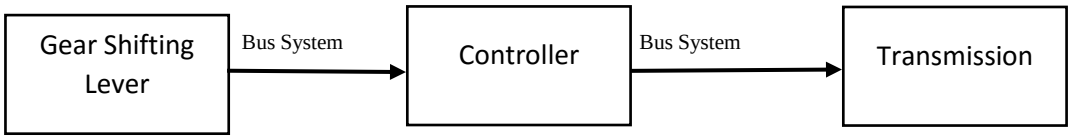

Figure 4. Overview of shift-by-wire technology.

Currently, all the technologies (SBW, DBW/EGAS, ESP, BMS, and CC) have emerged from XBW technology and are implemented independently, depending on the functions in drive-train domain. In powertrain domain, there are nearly 8 main isolated embedded software/controllers, which work autonomously. This has led to the increase in the complexity of bus system/communication network and maintenance.

The development of E/E system should be done according to ISO 26262 standards. Nevertheless, electronic embedded systems inherit complexity, which in turn demands for functional safety of E/E systems. For example, malfunctioning of electronic braking system leads to a fatal accident, which might cost the death of passengers in the car or the pedestrians. Keeping this in mind, automobile manufacturers created a framework to assure the development of safety critical automotive ECU in compliance with ISO 26262.

With the increase in volume of electrical and electronics systems in a modern automobile, it is difficult to implement ISO 26262 standard in developing an E/E system.

4. ISO 26262

Most of the modern cars are operated by automotive ECUs as a result, it is utmost of top priority to have advanced safety features [10]. The safety features are defined explicitly for road-vehicles in ISO 26262 standard. The ISO 26262 standard is a "State of Art" for the automotive ECUs, which was extracted from IEC 61508 [10].

ISO 26262 standards apply for a safety related E/E systems, which will be installed in a vehicle with a maximum weight up to 3.5 tons, not in a vehicle for physically challenged people. Only the hazards caused by the malfunctions of E/E system are addressed by ISO 26262, not the hazards caused by fire, toxic radiation, high temperature, smoke and corrosion [10].

According to Hassan (2019), ISO 26262 standards specify:

1. An automotive safety life cycle in order to reduce the risk to acceptable level
2. Classification of risk
3. Providing a safety requirement for either an item or subsystem or components using automotive safety integration level (ASIL)
4. Requirements for validation of item/subsystem/components to achieve a defined safety goal.

ISO 26262 Standard majorly consists of 10 parts which are listed below:

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level

6. Product development at the software level

7. Production and operation

8. Supporting processes

9. Automotive safety integrity level-oriented and safety-oriented analysis

10. Guideline on ISO 26262

4.1 Vocabulary

The most important terms are defined here, which will be used throughout the E/E system development process, starting from analyzing the system risk to the validation of E/E system.

4.1.1 Definition of Terms:

1) *Functional safety:* Absence of unacceptable risk due to hazards caused by the malfunctioning of E/E system.
2) *Driving cycle:* Operation time between the engine start and stop.
3) *Error:* When a response of EGAS based on driver's demand or other E/E system, in this case request from CC is not fulfilled by EGAS.
4) *Latent Error:* The error, which will not be detected by E/E system or by the driver in the next driving cycle.
5) *Fault:* When an E/E system parameters value deviates from allowed values.
6) *Failure effect:* Defines the behavior of system under faulty condition.
7) *Failure Reaction:* The measure, which will be taken after the error detection, in order to reduce the unacceptable risk to acceptable risk.

4.2 Management of Functional Safety

Managers of E/E System Development Departments work in this phase, to understand the system, software and the requirements of hardware, so that the available resources can be utilized on the development and safety activities in the safety life cycle of an item or E/E system.

4.3 Concept Phase

In this part, E/E system will be illustrated along with its subsystems and its dependency on other E/E systems.

4.3.1 System Definition:

The Preliminary system architecture is defined to analyze the E/E system as per ISO 26262 to conduct the safety life cycle process. The item or system consists of components to provide the desired function.

Intended functionalities of a system will be shown by functional block diagram.

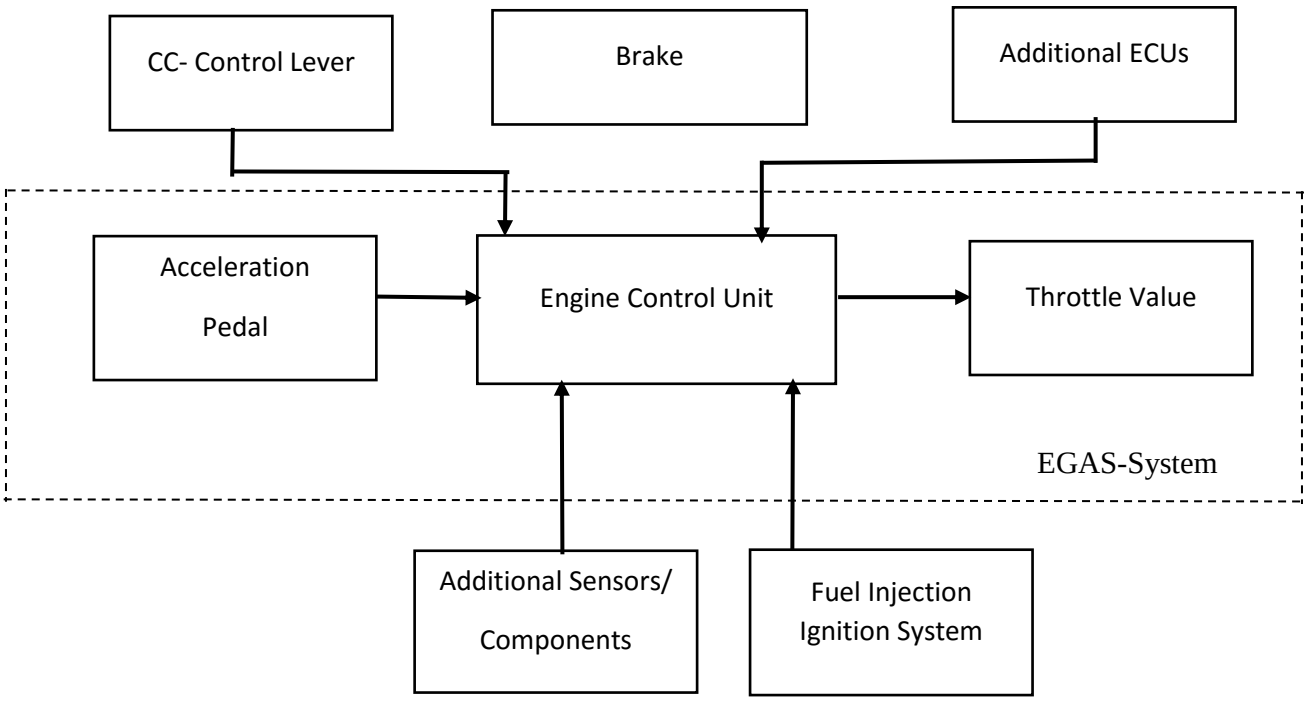

Figure 5. System definition of EGAS [4].

The function of EGAS has already been explained in the section 3.2. The above diagram shows the dependency of EGAS on other sub E/E systems like CC and ESP and components like brake pedal.

Until the recent days, automobile manufacturers were developing separate ECUs with independent bus system/communication network for different functionalities related to powertrain domain, which leads to increasing in wiring and weight of the vehicle. In a changing scenario along with increasing dependency of E/E systems on other ECUs, vehicle manufactures have decided to optimize the currently available communication network/bus system before developing a centralized ECU that access bunch of sensors, actuators and other resources for multiple functionalities. As a result of above thinking, automakers have been developing a new E/E system called Central Powertrain Controller (CPC) for powertrain domain, which interact with other powertrain E/E systems along with body, chassis and telematics E/E systems simultaneously.

4.3.2 CPC System Definition for Conventional Vehicle:

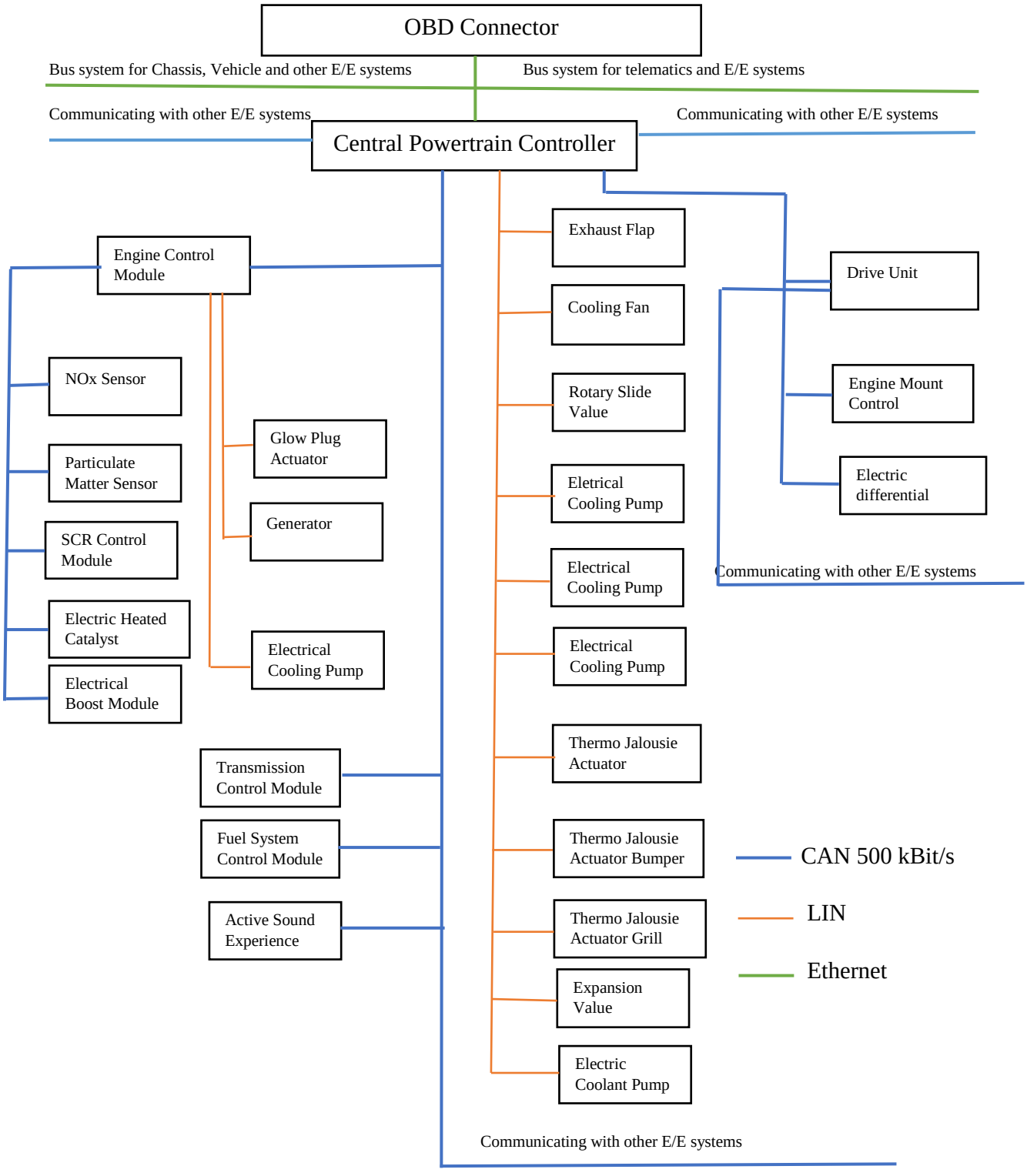

Figure 6. Network Topology of CPC for Conventional vehicle [16].

4.3.3 CPC System Definition for Hybrid Vehicle:

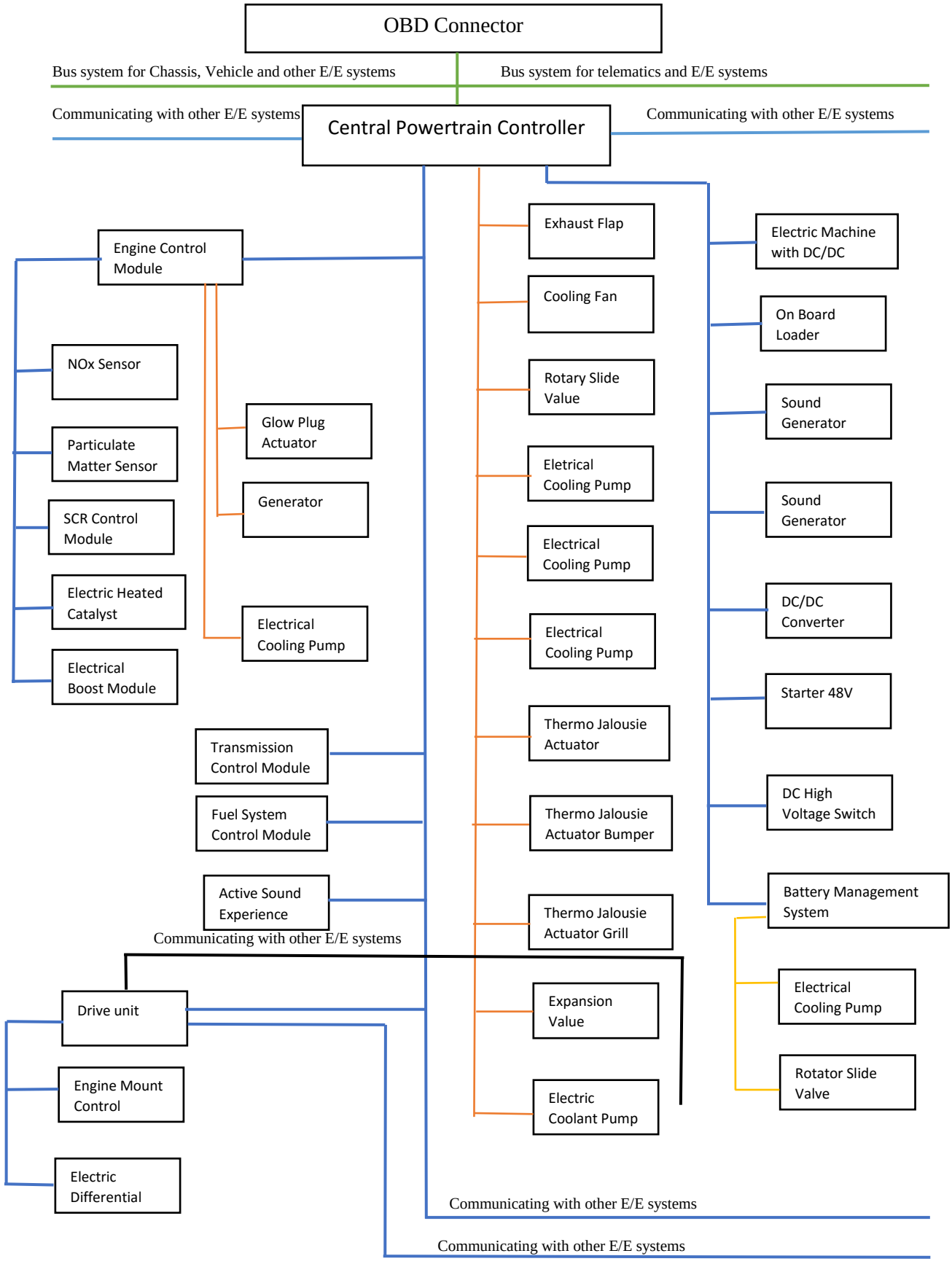

Figure 7. Network Topology of CPC for Hybrid vehicle [16].

4.3.4 CPC System Definition for Electric Vehicle:

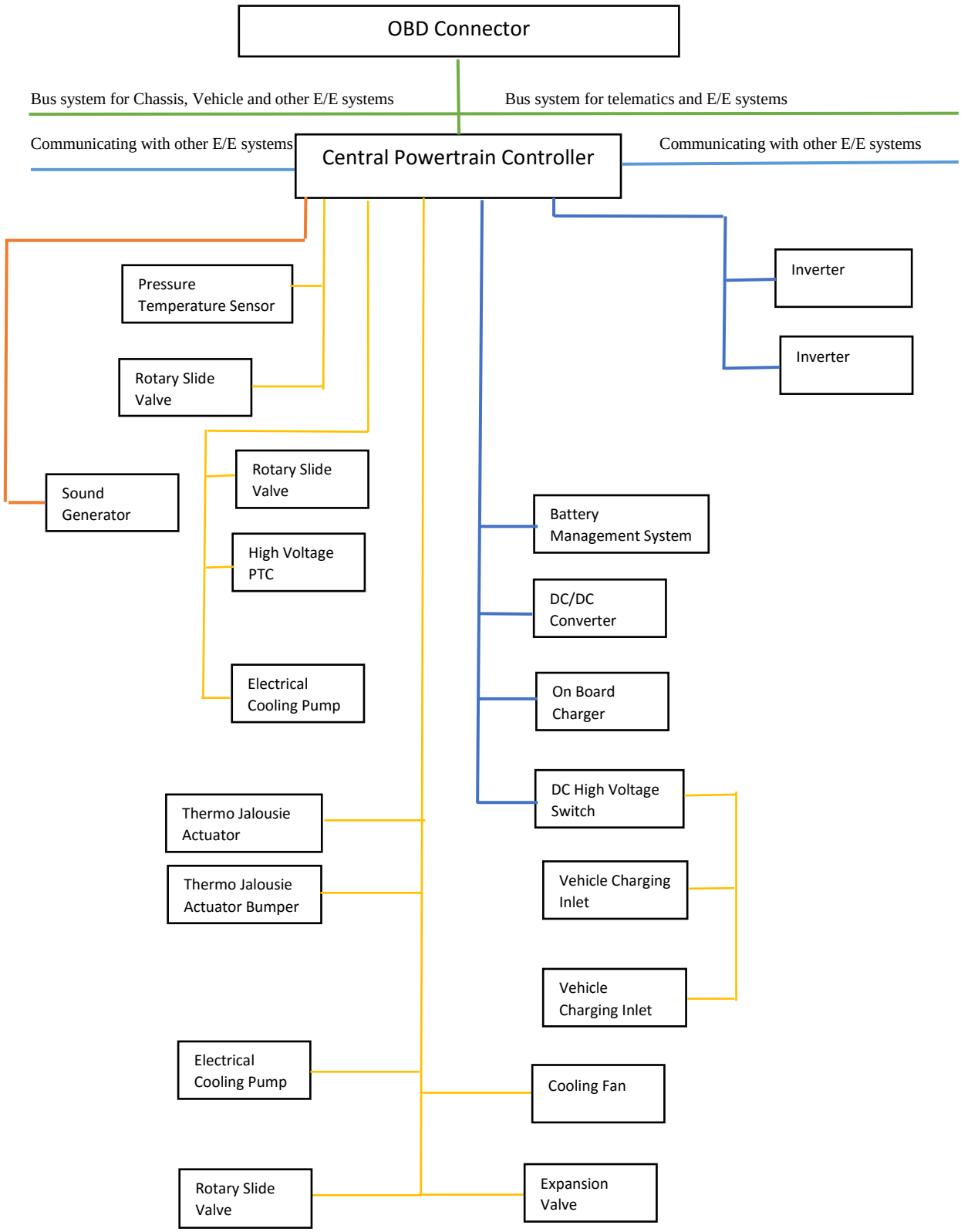

Figure 8. Network Topology of CPC for electric vehicle [16].

Therefore, in the item definition artifact, the following entries shall be included:

- The function concept: description of the item and its purpose
- The item functions list
- The functional and non-functional requirements
- The preliminary system architecture [11].

Through preliminary system architecture, functionalities of an E/E system, physical, mechanical, information energy and material interface of E/E system with other systems or components and its boundary will be depicted. Once the item definition is done, Hazard Analysis and Risk Assessment (HARA) will be started for a system/subsystem/component.

The main objectives of HARA:

a) Identification of hazardous events induced by unintended behavior of E/E system.
b) Derivation of safety goal and assignment of ASIL based on risk assessment to reduce the unacceptable risk into an acceptable risk [13].

Functional safety experts will conduct the HARA through documenting the malfunctioning behavior of E/E system/function in different driving conditions to find out the hazardous event. For each hazardous event, the result of E/E system malfunction, functional safety engineers will assign a severity of hazardous event on driver or on pedestrians along with determining the frequency of occurrence of hazardous event in each driving cycle. Based on the frequency and severity, ASIL will be determined for the prevention of hazardous events listed for an E/E system along with safety goals. The frequency of hazardous event will be determined based on controllability and exposure.

According to Mercedes-Benz AG functional safety experts, below are the safety goals defined for CPC based on HARA:

1) Safety goals for CPC in conventional vehicle:

- SG-01 Prevention of unintended acceleration → ASIL B
- SG-02 Prevention of absence of acceleration → QM
- SG-03 Prevention of unintended deceleration → QM
- SG-04 Prevention of absence of deceleration → QM
- SG-05 Prevention of wrong driving direction → ASIL B
- SG-06 Prevention of destabilization → ASIL C

2) *Safety goals for CPC in hybrid vehicle:*
    - SG-01 Prevention of unintended acceleration → ASIL B
    - SG-02 Prevention of absence of acceleration → QM
    - SG-03 Prevention of unintended deceleration → QM
    - SG-04 Prevention of absence of deceleration → QM
    - SG-05 Prevention of over braking → ASIL B
    - SG-05 Prevention of under braking → QM
    - SG-06 Prevention of destabilization → ASIL C
    - SG–07 Prevention of wrong driving direction → ASIL A

3) *Safety goals for CPC in electric vehicle:*
    - SG-01 Prevention of unintended acceleration → ASIL B
    - SG-02 Prevention of absence of acceleration → QM
    - SG-03 Prevention of unintended deceleration → QM
    - SG-04 Prevention of absence of deceleration → QM
    - SG-05 Prevention of over braking → ASIL B
    - SG-05 Prevention of under braking → QM
    - SG-06 Prevention of destabilization → ASIL C
    - SG–07 Prevention of wrong driving direction → ASIL A

Some hazardous events are controllable by the drivers. Safety goals of those hazardous events will be designated with ASIL QM. For those safety goals, no need of conducting validation of functionalities of an E/E system. ASIL A is the lowest safety integrity level, which requires lowest validation in order to meet the safety requirements. Whereas, ASIL D is the highest safety integrity level, which requires in depth validation.

4.3.5 Functional Safety Concept:

During this phase, functional safety requirements will be set for achieving the safety goals defined for each functionalities of an E/E system/ CPC or for the whole E/E system. The hazardous events will occur only when faulty calculation by the controller or wrong value is sensed by the sensor or there is a fault in the actuators.

During the case of failure, the vehicle would be taken to a controllable safe state within the defined Fault Tolerance Time (FTT).

The safety requirements are distributed among the following components:

a) *Sensors (S1/S2):* After sensing, sensors signals should be checked plausibly (e.g. driver pedal position for SG-01 in conventional vehicle).

b) *Actuators (A):* After sensing, actuators signals should be checked plausibly (e.g. throttle value position for SG-01 in conventional vehicle).

c) Central Powertrain Controller (CPC):

- CPC detects the fault in the sensor system
- CPC detects the fault in the actuator system.

According to ISO 26262, functional safety requirements should be derived from safety goals and each safety goals should have at least one-safety requirement. Through functional safety requirements, we can establish the strategies like:

i. fault avoidance
ii. fault detection
iii. fault tolerance transition to safe state
iv. Driver warning to increase controllability in case of failure.
v. Mitigation of functionality in presence of a fault [14].

4.4 Product Development at the System Level

ISO 26262-4 specifies the requirements for the E/E system development including:

1. The technical safety concept
2. System architecture design
3. Software and hardware architecture
4. Software and hardware integration including verification
5. System integration including validation
6. System validation at the vehicle level

The focus of Product development at system level lies in the development of a real system. Until the 'Concept Phase', we do the drafting of E/E system and its functionalities. The real development of E/E system will take place from Product development including the system validation, both at the system level and vehicle level. Figure 9 depicts the process of safe system development according to ISO 26262.

From this phase, many departments such as System engineering, Software development (including integration and verification), Hardware development (including integration and verification), Safety analysis department and department of validation of system both at the system and vehicle level work together for the development of a safe E/E system.

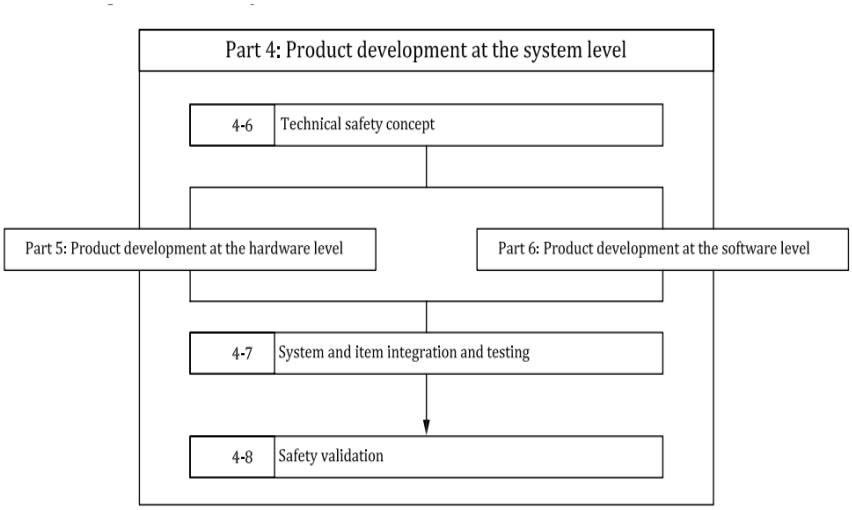

Figure 9. Overview of part 4 in ISO 26262 standards [14].

4.4.1 Technical Safety Concept:

In order to validate the functional safety requirements defined in the functional safety concept at the vehicle level, a separate technical safety requirement for an individual functionality or a whole E/E system will be derived from function safety requirements. This will be used during the software and hardware development and safety validation process. Together with deriving the technical safety requirements, a real system architecture will be defined as shown in the below Figure.

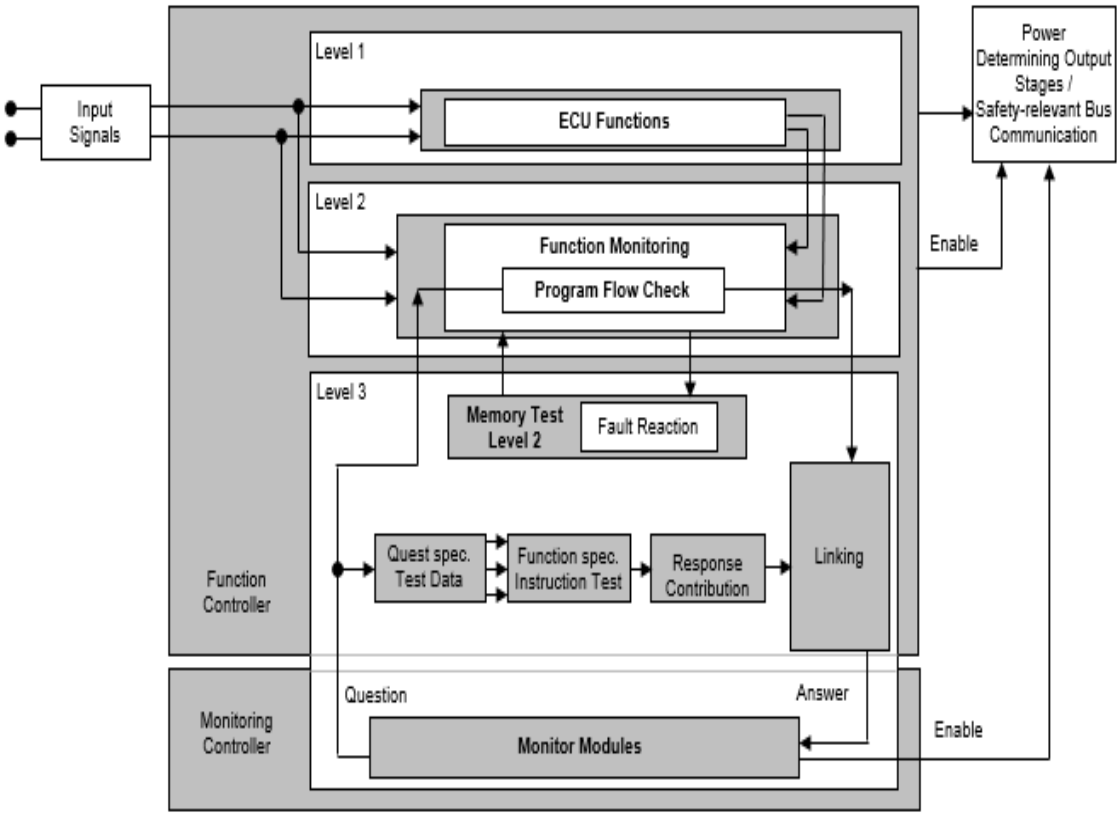

Figure 9. 3-level safe architecture of embedded software [4].

Based on the above safe software architecture, the Mercedes-Benz AG have been using the 3-layer monitoring safety concept in order to provide a safe embedded software for its vehicles. Suppliers in most of the cases will do the hardware and software development with integration and verification. Once the E/E system has been developed, Mercedes-Benz AG will do the system safety validation to ensure that defined safety goals are achieved and the defined functional and technical safety requirements are sufficient for the item or E/E system. Safety analysis of E/E system and its components (sensors, actuators, resistors, invertor and so on) will be done though FTA and FMEA to identify and prevent/mitigate the systematic faults by providing a safety mechanism like redundancy, which leads to a hazardous event.

Among the different safety validation process like diagnosis of input and output variables of E/E system and validation of sensors and actuators signals, monitoring concept is the one that is being used especially for the powertrain's E/E systems.

Here, one functionality of CPC is taken into consideration to provide the proper explanation of CPC system validation process.

5. 3-Level Monitoring Concept

5.1 Level 1

It is known as functional level. Level 1 is responsible for delivering the driver desire functionality together with diagnosing the input and output variables to and from it. In case of fault, Level 1 controls the E/E system reactions.

For example, when the engine produced torque is more than requested torque, level 1 cuts off the air-fuel mixture flow into the engine.

5.2 Level 2

It is referred as functional monitoring level. Level 2 monitors the level 1 functionalities. When the fault in the level 1 is not identified by level 1 monitoring module, level 2 will take over the level 1 functionalities.

For instance, when level 1 is engaged on commanding engine to produce more torque than requested without identifying the fault, level 2 wait until the fault tolerance time is over, then takes control of level 1 functionalities and brings the system into fail-operating level with the reduction of availability.

5.3 Level 3

It is also called as controller monitoring level. There will be no relationship between function monitoring module and controller monitoring module. Level 3 monitors the hardware in the controller like microprocessors.

In case of faults, fault reaction will be different from level 1 and level 2 reactions. The validation of level 3 will be carried out by controller manufactures.

5.2.1 Functional Monitoring Level:

Level 2 is provided as a redundancy if the level 1 monitoring module fails. The reason for validation of level 2 both at the system level and at vehicle level is:

1. Mercedes Benz AG has the highest priority in developing a safe E/E system than profit.
2. Reliability of redundant layer has the higher priority than the backup systems like mechanically controlled / hydraulically controlled systems.
3. Monitoring of E/E functionalities should be easy.
4. Development of fail-operational E/E system through monitoring of ECU functionalities.

For the validation of level 2, Mercedes Benz AG has been using two embedded testing and measurements software, Time Partition Testing (TPT) and INCA by ETAS respectively.

We have defined different driving conditions for conventional, hybrid and electric vehicles along with acceptance criteria. Then fault is injected in level 1 to observe the level 2 failure reaction to the fault in the level 1 (level 1 monitoring was off).

The driving conditions for testing defined by the functional safety experts are:

1. Auto Start-Stop
2. Forward and Backward Creeping
3. Deactivation of Cruise control
4. During Pedestrian crossing
5. Driving at different vehicle speeds
6. Destabilization
7. Over braking (Only for Hybrid and electric vehicles)

The process of modifying the ECU parameters values is known as Calibration. The accelerator pedal sensor signal values were calibrated in CPC through TPT to 100% as a fault. The failure reaction of level 2 will be validated based on the acceptance criteria defined for each driving conditions. The system was validated both at the system level and at vehicle level using the same method.

In order to explain the validation of level 2, forward creeping driving condition was considered. The acceptance criteria is that, after the fault injection, the vehicle acceleration should be below EGAS limit curve and process objective limit acceleration curve as shown in the below figure.

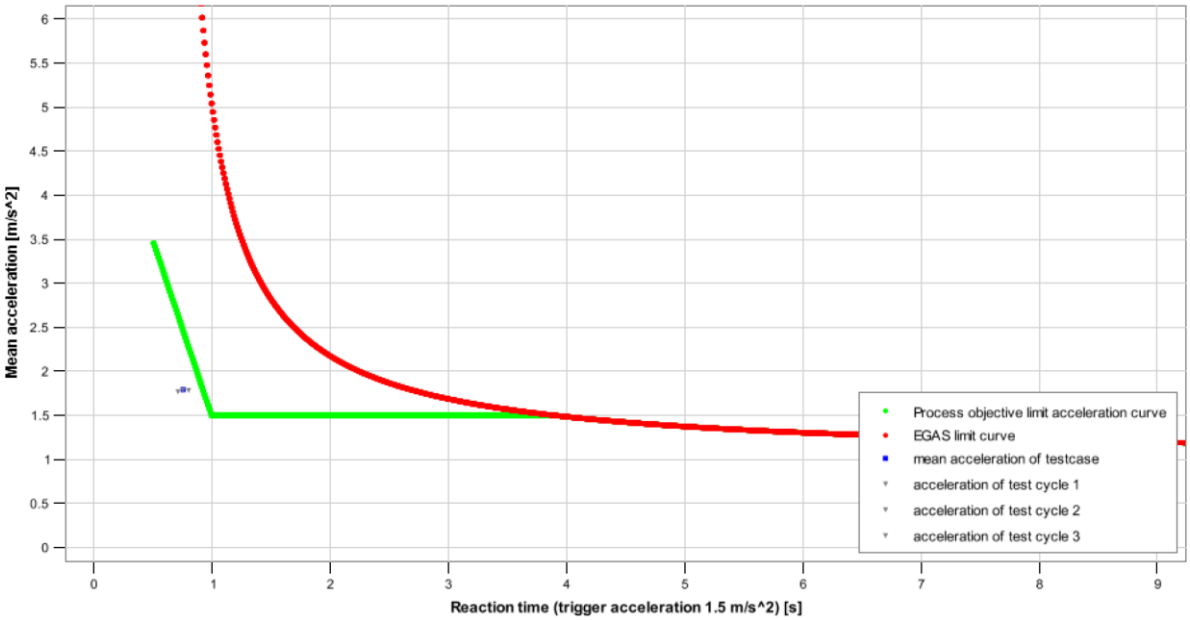

Figure 11. EGAS limit curve for validation of level 2 in CPC.

In Figure 12, we can see level 2 reaction after the fault injection in level 1.

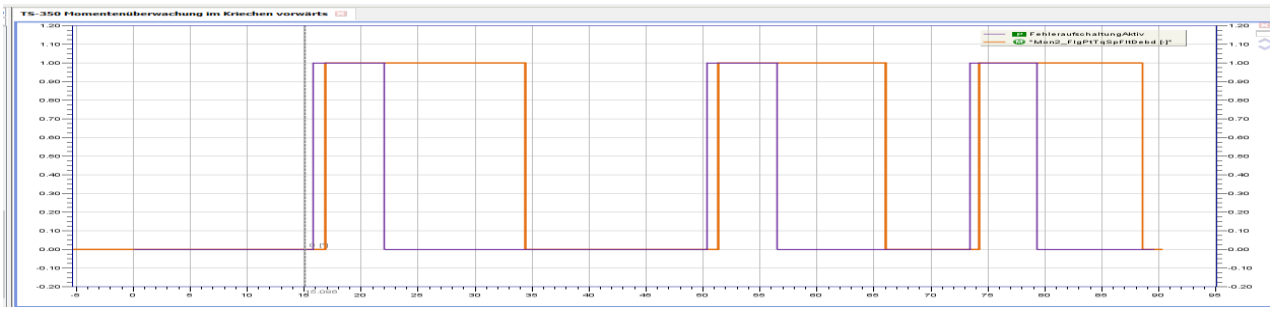

Figure 12. Reaction of level 2 to the fault in level 1.

Similarly, CPC system was validated for shift-by-wire functionality through calibrating the operating mode in level 1.

The driving conditions for testing are:

1. Operating mode in Reverse (R)
2. Operating mode in Driving (D)
3. Operating mode in Neutral (N)
4. Operating mode in Parking (P)

When the vehicle is in R, fault injection was in D/N/P. The error reaction of level 2 was R.

Figure 12 shows the clear insight into the testing.

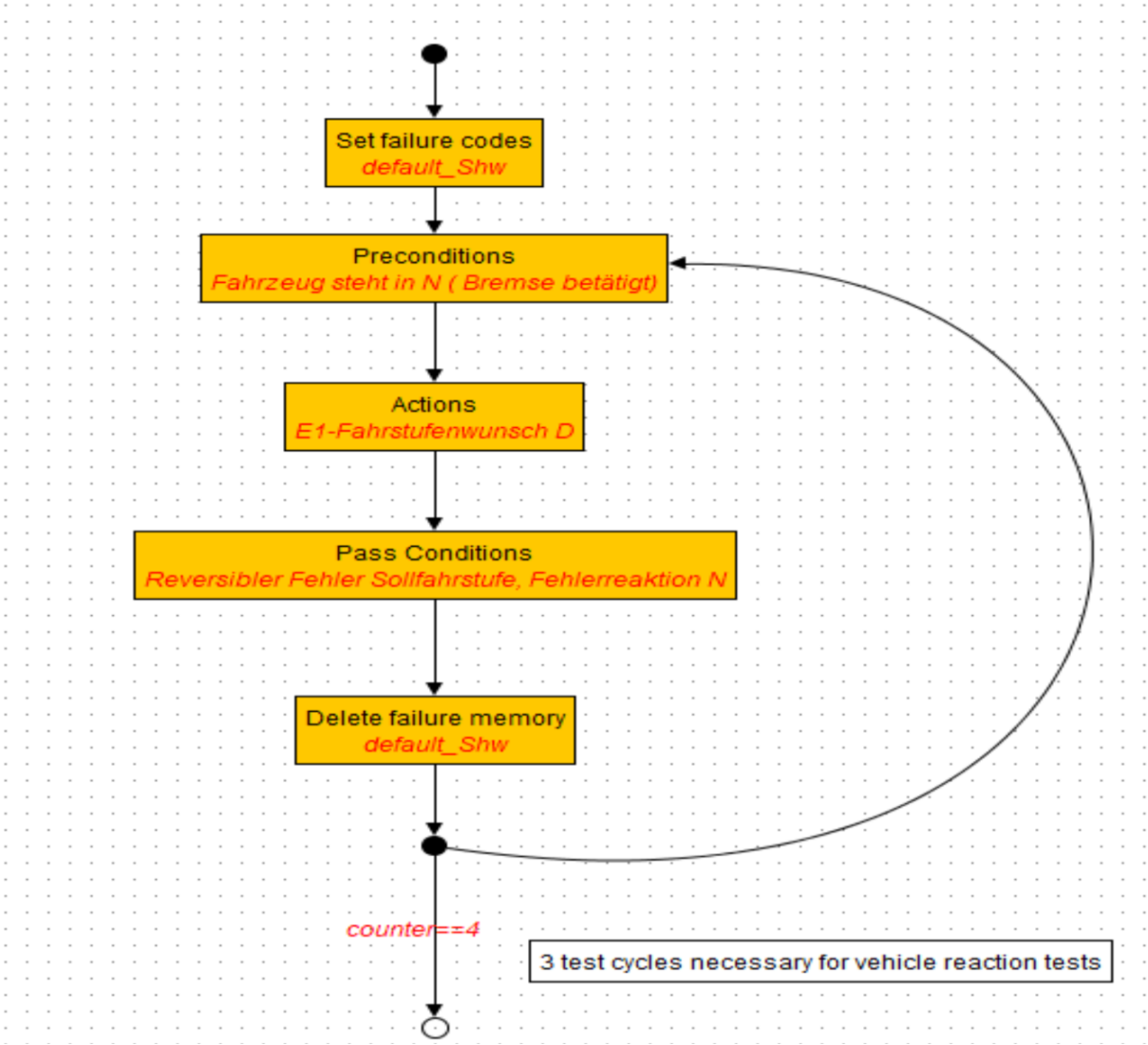

Figure 12. TPT model used for level 2 validation according to state machine.

Mercedes-Benz AG has provided certain safety mechanisms based on the E/E system functionalities both at the system and ECU level.

Safety mechanism for the fault in the level 1 when level 1 monitoring fails (ECU level):

1. Injection cut off /Correction of operating mode
2. Level 2 activation
3. ECU reset

Safety mechanism for the fault in the level 3 will be given by controller manufactures and at the system level will be given by the safety experts like redundancy.

If the level 2 is activated due to the error flag raise irrespective of the CPC functionalities, availability of the vehicle will be reduced until the driver reaches the nearest car care.

A safety mechanism is implemented in the CPC, which detects the faults in the impermissible drive torque for SG-01 and brings the system into a safe state as a failure reaction.

6. Conclusion and Future Work

The validation of automotive embedded software takes a longer duration than development. The result of it, most of the OEMs are yet to equip their developed software in their vehicle model. Any mistake during the validation process leads to the fatal accidents and companies lose their brand name along with paying big amount of money as penalty. According to software development experts, longer the fault exists in the software, more will be the development costs.

Automakers have already come up with new software architecture in order to reduce the communication network in the vehicle and validation duration. The below software architecture shows that how we can do the consolidation of multiple ECUs into one ECU. With the new software architecture, we can use single ECU for controlling the entire functionalities of the drive-train/chassis /vehicle-body/telematics. But, arrival of embedded software with new software architecture will take some more time.

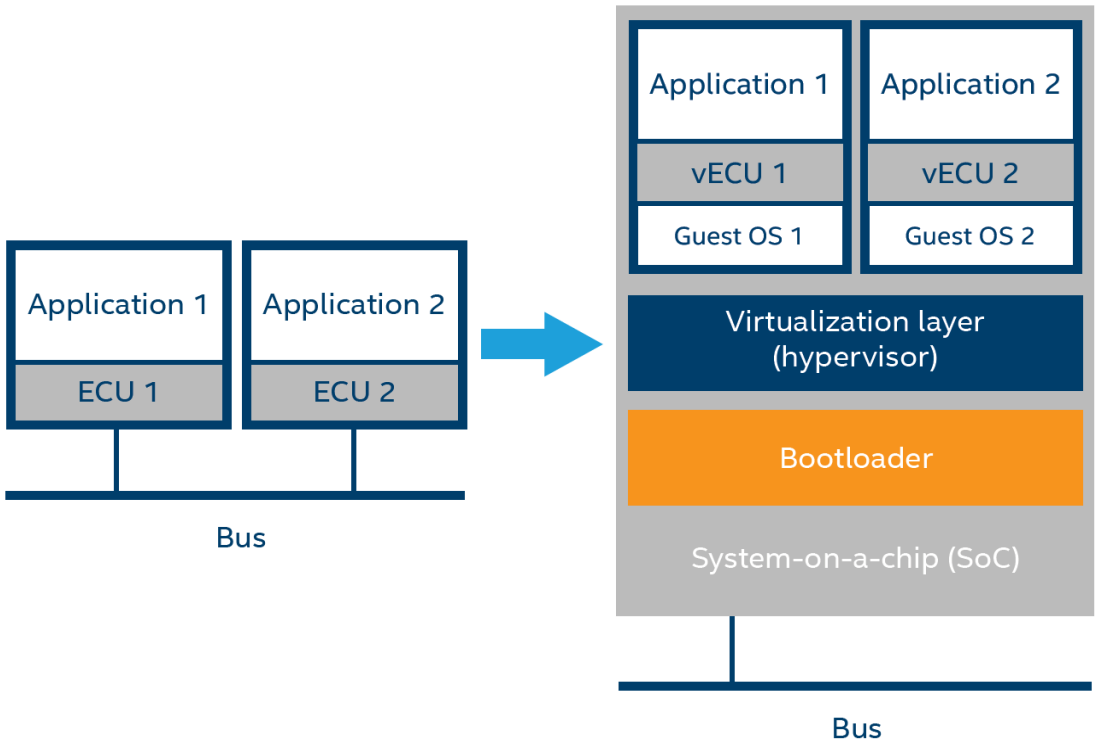

Figure 14. Preliminary architecture of consolidated ECU [3].

7. References

1. Automtoive & loT Blog. (n.d.). Retrieved February 20, 2020 from https://www.embitel.com/blog/embedded-blog/automotive-control-units-development-innovations-mechanical-to-electronics
2. Cédric Wilwert, Nicolas Navet, Ye-Qiong Song, Françoise Simonot-Lion. Design of automotive X-byWire systems. Richard Zurawski. The Industrial Communication Technology Handbook, CRC Press, 2005, 0849330777. ffinria-00000562f
3. ECU Consolidation Reduces Vehicle Cost, Weight, and Testing. (n.d.). Retrieved February 20, 2020 from https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/ecu-consolidation-white-paper.pdf
4. EGAS, Monitoring Systems Powertrain, Research & Development Power electronics development. Mercedes-Benz, Sindelfingen, Germany.
5. E-Gas (Electronic accelerator system). (n.d.). Retrieved February 20, 2020 from http://br.bosch-automotive.com/en/internet/parts/parts_and_accessories_2/motor_and_sytems/benzin/more_sensors/sistema_egas_pedal_acelerador_eletronico/sistema_egas__pedal_acelerador_eletronico.html#
6. Electronic control unit. (n.d.). In Wikipedia. Retrieved February 22, 2020 from https://en.wikipedia.org/wiki/Electronic_control_unit
7. Evers, M. (2019, March 13). What's Wrong with Boeing's 737 Max 8. Retrieved February 23, 2020 from https://www.spiegel.de/international/europe/what-s-wrong-with-the-boeing-737-max-8-a-1257608.html
8. Fly-by-wire. (n.d.). In Wikipedia. Retrieved February 26, 2020 from https://en.wikipedia.org/wiki/Fly-by-wire
9. Frank, R. (2004, October 1). X-By-Wire: For Power, X Marks the Spot. Retrieved February 23, 2020 from https://www.electronicdesign.com/markets/automotive/article/21797531/xbywire-for-power-x-marks-the-spot
10. Hassan, A. (2019, August 03). Functional Safety Mirror [LinkedIn page]. Retrieved February 21, 2020 from https://www.linkedin.com/pulse/functional-safety-mirror-abdelrahman-hassan/

11. Hassan, A. (2019, August 09). Functional Safety Mirror [LinkedIn page]. Retrieved February 21, 2020 from https://www.linkedin.com/pulse/functional-safety-mirror-abdelrahman-hassan-1c/
12. Hassan, A. (2019, August 31). Functional Safety Mirror [LinkedIn page]. Retrieved February 22, 2020 from https://www.linkedin.com/pulse/functional-safety-mirror-abdelrahman-hassan-3c/
13. Hassan, A. (2019, October 02). Functional Safety Mirror [LinkedIn page]. Retrieved February 22, 2020 from https://www.linkedin.com/pulse/functional-safety-mirror-abdelrahman-hassan-6c/
14. Hassan, A. (2019, November 09). Functional Safety Mirror [LinkedIn page]. Retrieved February 22, 2020 from https://www.linkedin.com/pulse/functional-safety-mirror-abdelrahman-hassan-10c/
15. Ostrower, J. (2018, November 18). What is the Boeing 737 Max Maneuvering Characteristics Augmentation System?. Retrieved February 25 from https://theaircurrent.com/aviation-safety/what-is-the-boeing-737-max-maneuvering-characteristics-augmentation-system-mcas-jt610/
16. Network Topology, Monitoring Systems Powertrain, Research & Development Power electronics department. Mercedes-Benz AG, Sindelfingen, Germany.
17. Pico Technology. Electronic Throttle Control (Drive By Wire). Retrieved from https://www.picoauto.com/library/training/electronic-throttle-control-drive-by-wire-or-fly-by-wire
18. Shift by wire. (n.d.). In Wikipedia. Retrieved March 01, 2020 from https://en.wikipedia.org/wiki/Shift_by_wire