EUROPEAN COMMISSION

SEVENTH FRAMEWORK PROGRAMME

Theme: ICT

Small or medium-scale focused research projects (STREP)

FP7-ICT-2013-10

Objective ICT-2013.6.5 Co-operative mobility

a) Supervised Automated Driving

GA No. 612035

Interoperable GCDC AutoMation Experience

Deliverable No.	i-GAME D4.5	
Deliverable Title	Safety analysis of scenarios and requirements	
Dissemination level	Public	
Written By	Pere Balaguer (IDIADA) Andrés Aparicio (IDIADA) Alvaro Arrue (IDIADA)	31-08-2014
Checked by	Based in D4.5.1 checked by: Reinder J. Bril (TU/e) Jonas Didoff (Viktoria Swedish ICT AB)	11-09-2014
Approved by	Almie van Asten (TNO)	07-11-2014
Status	FINAL	27-10-2014

Please refer to this document as:

D4.5.1_i-Game_Safety analysis of scenarios and requirements_public

Acknowledgement:

The author(s) would like to thank Reinder J. Bril at Technische Universiteit Eindhoven (TU/e) and Jonas Didoff at Viktoria Swedish ICT AB for valuable feedback in the review process of deliverable D4.5 on which this document is based.

Executive Summary

Functional safety becomes a key element in current vehicle specification. This importance on safety is also key when cooperative functionality is introduced to implement applications based on wireless inter-vehicle communications information.

The document is focused in two main goals. The first one is to give an overview about ISO 26262 in order to show the complexity of such standard. The second goal is to list a number of minimum safety/performance activities for the GCDC teams to guarantee that their vehicles are accepted for the competition.

Although ISO 26262 is not a requirement for the GCDC, it is important to make the participant teams familiar with the best practice automotive standard for safety.

The document starts with the functional safety section where the ISO 26262 is briefly introduced. Finally, a list of activities is mentioned in order to assure both safety and performance of the vehicles to take part on the GCDC scenarios.

This deliverable is based on D4.5 of iGAME which has restricted acces status.

Table of contents

Introduction

The iGame project

The objective of iGAME is to develop technologies that speed-up the real-life implementation of automated driving, which is supported by communication between the vehicles and between vehicles and road-side equipment.

Goal of the document

The document tries to cover the following goals:

1. The first goal is to give an overview about the ISO 26262.
2. The second goal is to list a number of minimum safety/performance activities for the iGAME teams to guarantee their vehicles are accepted in the GCDC competition.

Functional safety

Functional Safety is becoming a key factor in the development of vehicles. It is important to notice that functional safety is a vehicle property, rather than an application domain. Functional safety is applicable to every function implemented via any electric or electronic component, independent from the application domain. Functional safety compliance can only be claimed for a process, or a product, and not for an organization.

Although Tier 1 suppliers will actually provide many systems, the vehicle manufacturer is responsible for giving the functional safety target as a requirement. In the event that the supplier is providing a complete system with little involvement from the vehicle manufacturer, then the supplier must state what safety goals have been achieved and the manufacturer must state explicitly that these are acceptable.

Functional safety is defined on ISO 26262 as the absence of unreasonable risk due to hazards caused by malfunction of Electric & Electronic (E/E) systems. Zero risk cannot be achieved and, therefore, there is always a residual risk that something goes wrong.

According to Bernhard Kaiser et al (2013) [2], in order to justify freedom from unreasonable risk, a safety case argument should be developed in which the safety requirements are shown to be complete and satisfied by the evidence generated from the ISO 26262 work products. However, the standard does not provide practical guidance on the development and review of the safety argument, nor does it describe how the safety argument should be evaluated in the functional assessment process.

It is important to point out that system safety is a wider concept than functional safety and, therefore, they shall be used depending on the context. Functional safety is not the overall safety of a product; this role shall be taken by the system safety. It shall include functional safety along with fire safety, electrical safety, chemical safety, mechanical safety, radiation, toxicity, reactivity, corrosion and release of energy, since other causes different from electric & electronic could cause safety issues. Therefore, system safety shall be covered by different standards covering the above domains

1.1 ISO 26262 standard

1.1.1 ISO 26262 objective

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems (and interaction of these systems) and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3.500 kg. However, it is expected that buses and trucks will adopt that standard (or similar principles) as best practices from functional safety wise.

ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. It does not address the nominal performance of E/E systems. For example, ISO26262 does not control how powerful the brakes should be or how good the front lights should beam. Instead the ISO26262 standardize how the safety of the control system for the electrical equipment should be developed. It controls how the brake control system should be developed in order to avoid a failure from happening.

1.1.2 ISO 26262 and the V-model concept

ISO 26262 is based on the V-model concept. The V-model contains specification of the functional requirements, technical requirements, the system architecture, the system design and implementation on the left branch and the integration, verification and validation and functional assessment on the right hand branch.

Figure 1 shows the overall structure of ISO 26262 [1] based upon a V-model as a reference process model for the different phases of product development (10 parts) and, below, the hierarchy of requirements depending on the process phase (from top level to down level) is shown:

- Safety goals (hierarchy 1; 3.Concept Phase): the vehicle in its environment
- Functional safety requirements (hierarchy 2; 3. Concept Phase): the vehicle and its systems
- Technical safety requirements (hierarchy 3; 4. Product development at the system level): the E/E system
- Hardware and software requirements (hierarchy 4; 5. Product development at the hardware level & 6. Product development at the software level): component and part level

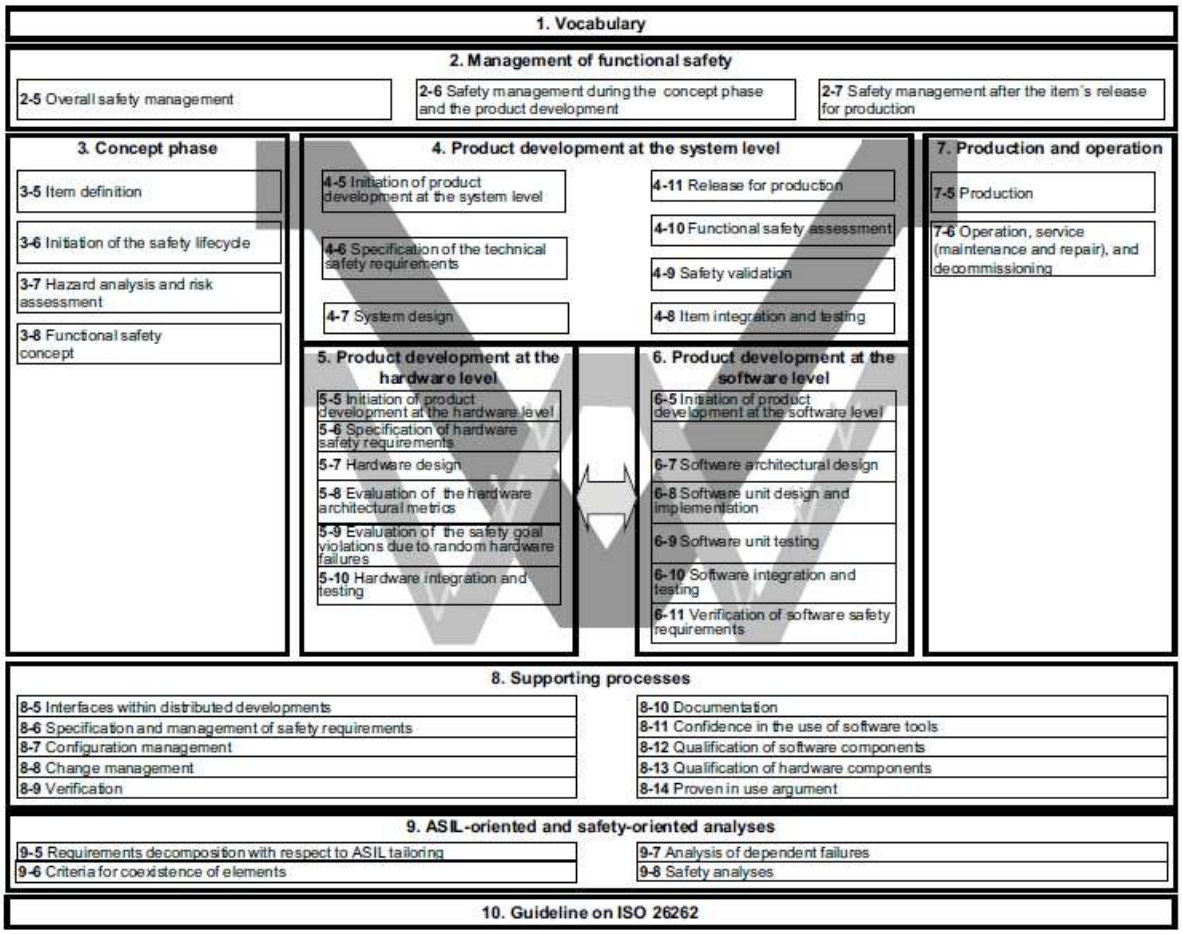

Figure 1: ISO 26262: V-model concept

- Part 1: Vocabulary
- Part 2: Management of functional safety
- Part 3: Concept phase
- Part 4: Product development at the system level
- Part 5: Product development at the hardware level
- Part 6: Product development at the software level
- Part 7: Production and operation
- Part 8: Supporting processes
- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
- Part 10: Guideline on ISO 26262

Other figures about ISO 26262 are:

- More than 450 pages
- 43 chapters
- Around 600 requirements
- Around 100 work-products
- Around 180 engineering methods (risk of uninformed usage)

Safety check list

n order for teams and vehicles to participate in the GCDC a number of verifications have to be performed to insure the safety of drivers and to facilitate the planning and preparations once the teams are on site in Helmond in 2016. Verification as described below will take place approximately 6 months before the competition in Helmond with the purpose to avoid teams to be disqualified at the actual event. Verification is mandatory for all teams before participation in GCDC and are offered at IDIADA (Spain) and at AstaZero (Sweden).

In order to assess the functional safety mechanisms implemented into the vehicles a list of potential activities are listed below.

The aim of the list is to guarantee vehicles compete in the scenarios with a level of safety and, therefore, risks during competition are minimized as much as possible.

The way the tests are listed below shall be the way they are performed. These tests are grouped in stations. At each station some aspects of the required behavior shall be evaluated in a controlled way:

- Station 1 ‘Design planning activities’
- Station 2 ‘Administrative checks’
- Station 3 ‘Visual inspection’
- Station 4 ‘Vehicle manual control’
- Station 5 ‘Communication protocol checks’
- Station 6 ‘Braking safety checks’
- Station 7 ‘Data validation and accuracy checks’
- Station 8 ‘Benchmark platooning scenario’
- Station 9 ‘Benchmark intersection scenario’

Following the above process we will assure the vehicle is qualified in a gradual complexity manner.

If a participant vehicle fails in one stage, it will come back to the same stage once a review is made and there is enough time to repeat it. If it is not successful in passing the station or there is not enough time to repeat the tests, the vehicle will be disqualified.

Vehicle will be qualified as GCDC participant vehicle once ALL stages are passed satisfactorily. Moreover, the tests will be performed again in the week prior to the event to ensure that the vehicle is still up to standard.

Some check activities are new and others are based on the ones carried out during the GCDC 2011 [3]. In all cases, the participant is in always responsible for its own safety, the safety of their vehicle and for not jeopardizing the safety of other people or vehicle in its vicinity.

Each vehicle shall be equipped with a FM radio receiver to receive information from the organization via FM transmission.

Depending of the final GCDC organization and the teams participating, some of these issues need to be further discussed among the project before setting up final requirements and methodologies. At this stage of the project it is not possible to take a final decision on them. These open issues are signaled in the following descriptions by the use of TBD acronym.

2.1 Stage 1 'Design planning activities'

Apart from the implementation, the design process followed by the teams to get the final implementation is also evaluated. This evaluation is based in generic key activities highlighted in the ISO 26262 or MISRA Safety Guidelines; the idea is to get the teams familiar with current automotive standards from the safety point of view.

The following aspects below are potential ones to be evaluated.

- Is any safety engineer on the team or someone coordinating the safety design aspects?
- Do you have an overall plan showing safety activities in the overall project planning?
- What is the content of the safety plan?
- How do you carry put the functional safety assessment? Which are the judgment levels?
- Have you carried out any HARA (Hazard Analysis and Risk Assessment) activity or similar?
- Which techniques do you use for hazard identification?
- Which are the actions of the driver, or other persons potentially at risk, in order to comply with the safety goals?
- How has the team defined the technical safety requirements?
- How is software development coordinated with product development at system level and hardware level?
- How are the technical safety requirements impacting on the hardware architecture?
- Can you provide the methodology (hardware development) used to take into consideration safety aspects into the hardware design process?
- Can you provide the final hardware architecture?
- How are the technical safety requirements impacting on the software architecture?
- Can you provide the methodology (software development) used to take into consideration safety aspects into the software design process?
- Can you provide the final software architecture?
- Have you used any design system techniques? (FMEA (Failure Mode Effect Analysis), FTA (Fault Tree Analysis)…)
- Which characteristics of the hardware-software interface have you considered from safety point of view?
- Which elements of the hardware-software interface have you considered from safety point of view?
- Which test methods or combination of them are used at hardware-software level?

- Which test methods or combination of them are used at system level?
- Which test methods or combination of them are used at vehicle level?
- Verify above with test protocols (the supply of system test verification tools / methods TBD).

In order to evaluate the design development methodology carried out by the teams a selection of the above topics shall be selected. Depending on the importance of each one, a different weight factor may be applied.

This activity could be done independently of the other stages at some point before the functional and safety checks.

2.2 Stage 2 'Administrative checks'

The participants shall present the following documentation (further information may be required):

- Team details (drivers, assistants)
- Vehicle documentation (brand name and type, insurance, license plate number, chassis number, country, weight, size)
- List of any vehicle limitation that shall compromise the competition (speed limit, min acceleration, max deceleration…)

2.3 Stage 3 'Visual inspection'

- Are there any devices that obstruct the driver's tasks?
- Is the emergency button easily accessible for the driver and co-driver?
- Are the additional equipment safely installed into the vehicle?
- Is the participant identification number visible?
- Safety belts and other standard safety equipment shall work as intented.
- Is the advertising appropriate?

2.4 Stage 4 'Vehicle manual control'

The automatic mode must be instantly overridden by the driver (going to manual mode) by doing one of the following actions:

- Emergency button
- The throttle pedal
- The brake pedal
- Turning the steering wheel (if automated steering is installed)
- Changing the gear (TBD)
- Electric parking brake (if any vehicle is equipped with one)

In the transition from automatic mode to manual mode the driver shall regain full vehicle control when disabling the controller. This intervention is meant to be the last safety mechanism in case of a total system failure.

2.5 Stage 5 'Communication protocol checks'

Following tests can be done at different distances in order to validate communication range (the communication range shall be at least **TBD**):

- Safety messages will be checked from content and timing synchronization point of view (with other vehicle and road side unit): e.g. vehicle identification number and dimensions. As each critical time application requires a maximum latency time to be respected by the whole system involved in the communication, a maximum latency time test shall be defined in this station (**TBD**)

- Frequency of safety messages will also be checked (with other vehicle and road side unit). Frequency shall be no more than 10 Hz, although this value shall be confirmed once WP4 is finalized. The project will develop a communication simulator. Tests of communication messages sets shall be performed and approved before this event. This approval will be a 'must' to carry out the protocol checks on vehicle.

2.6 Stage 6 'Braking safety check'

The aim of this test is to evaluate the performance of the vehicles brakes. The test is carried out by the driver.

- Accelerate the vehicle from 0 to 40 km/h
- Keep this speed stable for 4 seconds
- Brake the vehicle till it stops

The vehicle shall stop within the pass range criteria:

- 15,3m (-5.2 m/s2) for a passenger car
- 18,9m (-4m/s2) for a commercial vehicle

2.7 Stage 7 'Data validation and accuracy check'

The aim of this test is to validate the vehicle in communication with another vehicle:

- Communication checks: protocol, data stream accuracy, update rate
    - Vehicle under test to GCDC reference vehicle
    - GCDC reference vehicle to vehicle under test

- Data accuracy checks:
    - Do the vehicle sensors accurately report the speed, acceleration, yaw rate and location of the vehicle as it moves in the defined trajectory? Accuracy shall be based in accuracy requirements (**TBD**)

- Acceleration and deceleration checks in autonomous mode (for all vehicles):
    - Maximum controlled acceleration between 1.5 and 2 m/s2
    - Minimum controlled acceleration between -4 and -4.5 m/s2

Morevoer, vehicle participant shall have an HMI where information about main sensors status and communication status shall be shown (TBD).

2.8 Stage 8 'Benchmark platooning scenario'

The objective of this test is to qualify the participant's ability to operate in a platoon, to follow speed commands, to communicate appropriately, and to provide the correct state information at the required update rate and with the required accuracy. It is the evaluation performance from the previous tests in a real situation.

The tests will be composed at least by the following cases:

- GCDC vehicle and the PV (Participant Vehicle) are lined up at the starting line. The GCDC vehicle starts driving and the PV must follow the direction and speed indicated by the GCDC vehicle. Communication will be validated and the vehicle-state data will be collected and used for data accuracy checks.

- The PV will accelerate in response to the acceleration of the GCDC vehicle. The GCDC vehicle will accelerate to a steady state speed and the participant vehicle should accelerate similarly to achieve the appropriate headway time. The exact value of this headway time will be given immediately.

- The PV will decelerate in response to the deceleration of the GCDC vehicle. The GCDC vehicle will decelerate to a steady state speed and the participant vehicle should decelerate similarly to achieve the appropriate headway time. The exact value of this headway time will be given immediately.

- The GCDC vehicle passes the PV and asks for permit to "merge" in front of the PV. Confirmation of negotiation and PV´s ability open gap. Then the scenario is performed with the PV passing and starting a medication to merge in front of the GCDC vehicle. (In the competition there will be no actual instructions from the vehicles to each other – only confirmation of gap to be opened, gap ready from the vehicle that is behind).

2.9 Stage 9 'Benchmark intersection scenario'

The objective of this test is to qualify the participant's ability to operate in an intersection scenario, simulating a negotiation/coordination between the PV and other vehicles on the

upcoming road intersection. The same methodology and data accuracy checks will be carried out as shown in the ‘platoon scenario’.

Two separate tests for all PVs are required:

1) Vehicle with intention to turn (left) into oncoming road:

- PV will increase speed till get a constant speed of 30 km/h in a specific area delimited by cones. The PV will establish contact with vehicles on the upcoming road
- If necessary communication may be routed via a roadside unit for extended range.
- The PV will negotiate the option to enter the road without stopping. The oncoming vehicles will allow passage for the PV to the road.

2) PV is on the main road and will allow approaching GCDC vehicle passage at the upcoming intersection

- PV receives request from the GCDC vehicle on oncoming road and confirms contact
- PV negotiates optimal speed / time / distance to the intersection to allow the oncoming vehicle to pass into the main road without stopping and with minimum delays.
- In addition the same tests will be performed with incorrect behavior from the GCDC vehicle. It will then approach the intersection with a speed of 20 km/hr – hence forcing the PV to decide whether to stop/ adapt and wait or to proceed and send an ABORT message to the GCDC vehicle.

Conclusions

Functional safety is becoming more and more important in current vehicle functions. It is a fact that standards are increasing requirements, work-products and engineering methods when depeloping and validating safety functions.

Automotive industry is, step by step, assuming ISO 26262 as a safety standard reference.

ISO 26262 standard is not a requirement for the GCDC competition organized by iGAME. However a 'Design planning activities' check is planned to be carried out with the teams by iGAME members to understand the development process that GCDC teams follow on their design/validation processes.

The idea is to make ISO 26262 standard familiar to the teams as key standard from functional safety point of view. However, although ISO 26262 is not a requirement, a safety/performance check list is mandatory for all the teams participating on the GCDC in order to comply with a minimum of safety.

References

[1] ISO International Standard, “Road vehicles – Functional safety,” ISO Standard 26262, Rev. Nov. 2011.

[2] Bernhard Kaiser et al, Integrating Functional Safety and Nominal Performance Requirements for Advanced Driver Assistance Systems, VDA Automotive SYS Conference, 13./14.06.2013 Berlin

[3] GCDC 2011, Rules and Technology Document, Grand Cooperative Driving Challenge, Final version 2.0

List of abbreviations & terminology

Architecture

Representation of the structure of functions or systems that allows identification of building blocks, their boundaries and interfaces, and includes the allocation of functions to hardware and software elements. It could be applied to vehicle, software & hardware architecture

ASIL

Automotive Safety Integrity Level is one of four levels to specify the necessary requirements of ISO 26262

E/E System

Electric & Electronic System consists of electrical and/or electronic elements, including programmable electronic elements

FMEA

Failure Mode Effect Analysis. Failure mode refers to the way in which something might fail and includes any potential error that may occur; Effect analysis involves deciphering the consequences of those failures by determining how frequently a failure might occur, making sure that failures can be detected and identifying which potential failures should be prioritized

FTA

Fault Tree Analysis is a top down deductive failure analysis in which an undesired state of a system analyzed using Boolean logic to combine a series of lower-level events

Functional safety concept

Specification of the functional safety requirements, with associated information, their allocation to architectural elements, and their interaction necessary to achieve the safety goals

Functional requirement:

Specification of implementation-independent behavior, or implementation-independent measure, including its related attributes

Hazard

Potential source of harm

HARA

Hazard Analysis and Risk Assessment is a method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk

ISO

International Organization for Standardization

Item

System or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied

PV

Participant vehicle

Requirement

What the end user expects from a system

Risk

Combination of the probability of occurrence of harm and the severity of that harm

Safety integrity

Degree of confidence in a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

System

Set of elements that relates at least a sensor, a controller and an actuator with one another

Validation

System fulfills its requirements implicit human needs (it shall answer the question: Did we build the right product?

Verification

System fulfills its requirements explicit specification (it shall answer the question: Did we build the product right?)

List of Figures

List of Tables