Journal of KONBiN 2,3 (14,15) 2010
ISSN 1895-8281

ISO 26262 - THE RELEVANCE AND IMPORTANCE OF QUALITATIVE AND QUANTITATIVE METHODS FOR SAFETY AND RELIABILITY ISSUES REGARDING THE AUTOMOTIVE INDUSTRY

ISO 262626 - RELEWANTNOŚĆ I WAŻNOŚĆ JAKOŚCIOWYCH I ILOŚCIOWYCH METOD W ZASTOSOWANIU DO ZAGADNIEŃ BEZPIECZEŃSTWA I NIEZAWODNOŚCI W PRZEMYŚLE SAMOCHODOWYM

Marco Schlummer[1], Dirk Althaus[2], Andreas Braasch[3], Arno Meyna[4]

University of Wuppertal, Gaußstr. 20, 42097 Wuppertal, Germany

E-mails: (1) mschlumm@uni-wuppertal.de (2) dalthaus@uni-wuppertal.de
(3) braasch@uni-wuppertal.de (4) meyna@uni-wuppertal.de

Abstract: *Safety and reliability are key issues of today's and future automotive developments, where the involved companies have to deal with increasing functionality and complexity of software-based car functions. New functionalities cannot only be found in the area of driver assistance – most of the new car functions are and will be safety related as for example in vehicle dynamics control or active and passive safety systems. The development and integration of those functions will strengthen the need of safe processes during the system development. The new upcoming automotive standard on functional safety (ISO 26262), which is derived from the generic functional safety standard IEC 61508 to comply with the specific needs to the application sector of E/E-systems in road vehicles, will provide guidance to avoid the increasing risks from systematic faults and random hardware faults by providing feasible processes and requirements. It is evident that aspects and methods of the safety and reliability engineering are implemented and suited methods are performed in the development process at an early stage. This is one of the requirements of the new ISO 26262, which introduces a so called automotive safety lifecycle to handle all those activities that are necessary to guarantee the functional safety of automotive E/E-systems. In the following, a brief overview of the upcoming automotive standard, its new safety life cycle and the connected activities in order to ensure functional safety for safety related systems will be given. The main aim of this paper is to show the relevance and importance of one of the major tasks within the ISO 26262: the process of the hazard analysis and risk assessment as it is currently performed in the automotive industry. With the help of an example from the automotive sector, the basic steps of this method to determine the automotive safety integrity level (ASIL) are explained. Depending on the ASIL, safety requirements need to be derived as a result of the new standard regarding safety integrity attributes. Furthermore, the connection of the automotive functional safety process with methods for qualification and quantification of safety and reliability issues will be explained in this paper. The Fault Tree Analysis will be used to exemplify one of these methods which are applied subsequent to the hazard analysis and risk assessment and which make a contribution to the validation and verification of the safety process.*

Keywords: *functional safety, hazard analysis and risk assessment, automotive safety integrity level, fault tree analysis*

Streszczenie w języku polskim na końcu artykułu

1. Introduction

In the domain of automotive electrics and electronics (E/E), innovations and developments are rapidly proceeding, though the functionality of software-based car functions is more and more increasing. Many pure mechanical systems have been or are complemented or substituted by E/E to mechatronic systems. Those modern systems are characterized by a high level of complexity and they can consist of a great amount of intelligent sensors, control units and actuators, whose communication is realized by several bus systems. It is very important that those systems work reliable as well as safe in vehicles and that they only possess an insignificant extent of risk. With the shown trend of increasing complexity and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. In addition, most of the new car functions are safety related. Therefore, a guideline is needed to avoid these risks by providing feasible requirements and processes.
One step in order to achieve this is the determination of the hazards based on the considered system and the identification and evaluation of the existing risks at an early stage within the framework of a functional safety process. This can be done by means of a hazard analysis and risk assessment whose performance is a requirement of the generic safety standard IEC 61508. This standard applies as a master standard for functional safety of electric, electronic and programmable electronic safety related systems (E/E/PES) and components. One of the major goals of the IEC 61508 is that tailored standards should be derived based on it for the various fields of application of E/E/PES. An adapted standard for the functional safety within the automotive industry (ISO 26262) is in progress. Since summer of 2009, the standard is published as ISO/DIS 26262. All information in this paper about the upcoming standard is based on this publication.

2. The automotive standard on functional safety

The historical background of IEC 61508 lays in the process engineering and the automation industry. As a master standard, it contains a generic solution independent from the application for all activities during the safety lifecycle of E/E/PES that are performing safety functions. One of the main goals of IEC 61508 is that tailored standards should be derived from it. This has already been done in some fields of application (e.g. IEC 61513 for the nuclear industry or IEC 60601 for medical electrical equipment). In other fields, suitable derivates are in preparation, as for example within the automotive sector.

As already mentioned, ISO 26262 is the adaptation of IEC 61508 to comply with the specific needs of the application sector of E/E-systems within road vehicles. It addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems including interaction of these systems. More details about the reasons for the necessity of the automotive standard can be seen in (Jung, 2006). More than 20 automobile manufacturers, supplier companies as well as research institutions from different countries like Germany, France, Italy, Sweden, Japan and the United States participated in the development of ISO 26262.
As the master standard, ISO 26262 is based on a safety lifecycle, too. The automotive approach encompasses principal safety activities during the three phases concept phase, product development and after product release (see Fig. 1). The management of functional safety, which has to be established and installed first, has the major tasks to plan, coordinate and keep record of all activities during these phases. The supporting processes (e.g. documentation management system, configuration management system, employee training) also apply to all activities during the safety lifecycle.

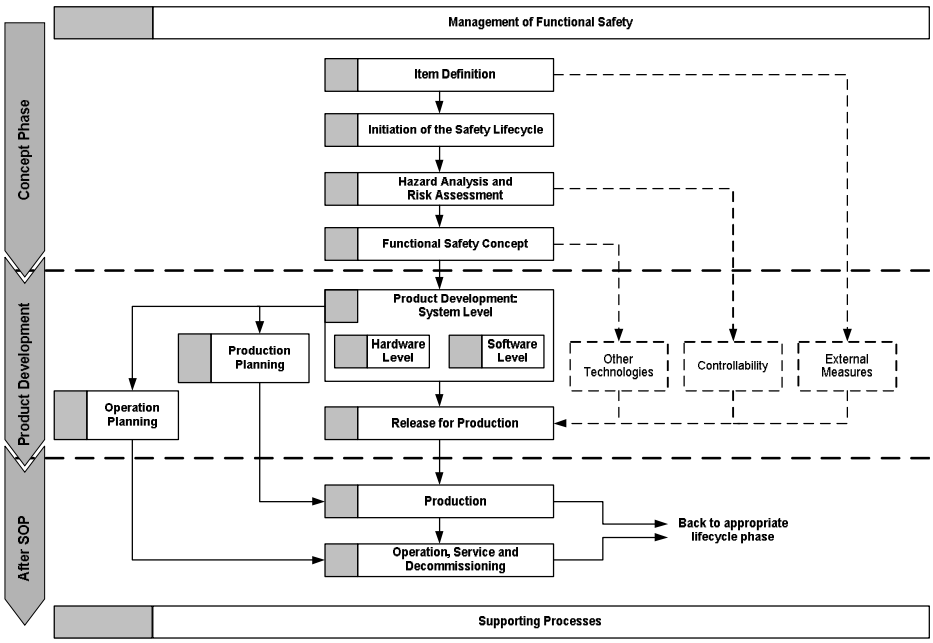

Fig. 1 Automotive safety lifecycle

As can be seen in Fig. 1, the concept phase can be separated into four sub-phases, in which the item under consideration has to be defined, the safety lifecycle needs to be initiated, a hazard analysis and risk assessment has to be performed and a functional safety concept needs to be set up. The system analysis and the allocation

of functional safety requirements, which are part of the phase product development, are separated for hardware and software level. The overall planning of operation, service and decommissioning is also content of the new standard.
ISO 26262 encompasses ten parts, whose order and contents mainly base on the lifecycle shown above.
In the next chapter, one of the major tasks of the automotive standard, the hazard analysis and risk assessment will be described more detailed.

3. The hazard analysis and risk assessment

The hazard analysis and risk assessment is part of the automotive safety lifecycle. Its modus operandi is based on the qualitative method of the risk graph, which is described in IEC 61508. The objective is to identify and categorize the hazards of the item. Furthermore, safety goals related to the prevention or mitigation of these hazards must be formulated, in order to reduce the risk to an acceptable degree.
ISO 26262 provides an automotive specific risk-based approach for determining risk classes. Those classes are called Automotive Safety Integrity Level (ASIL) and they are determined by a systematic evaluation of potentially hazardous driving or operating situations, which is based on the functional behavior of the item.

The method is composed of three basic steps, which are illustrated subsequent:

- situation analysis and hazard identification,
- hazard classification and
- risk assessment.

The involved persons in the hazard analysis and risk assessment should have good knowledge and domain experience.

3.1. Situation analysis and hazard identification

The goal of the situation analysis and hazard identification is to identify potential unintended behavior of the item that could lead to a hazardous event. For this purpose, it is necessary to have a clear definition of the item, its functionalities and boundaries. In addition, descriptions of the item's operational situations and operating modes in which its malfunction behavior is able to trigger a hazardous event is needed. This list of operational situations shall be as precise as possible and as comprehensive as necessary. It is possible to take information into account about the conditions of the vehicle's operating and usage scenarios, the environment conditions and reasonably foreseeable driver use and misuse. While

systematically identifying potential hazards, which can result from normal functioning, malfunctioning and non-functioning of the item, the consequences of hazardous events shall be identified and described for the relevant operational situations and operating modes as well.

3.2. Hazard classification

The hazard classification is based on the general risk definition, which defines risk as the product of the probability of a particular hazard occurring and the severity of the outcome when the hazard occurs. The automotive approach describes the risk (R) as a function (F) of the frequency (f) of occurrence of a hazardous event, the ability of the avoidance of specific harm or damage because of timely reactions of the persons involved (C = Controllability) and the potential severity (S) of the resulting harm or damage:

$$R = F(f, C, S). \tag{1}$$

The frequency of occurrence is influenced by two factors:

$$f = E \cdot \lambda . \tag{2}$$

One factor is how frequently and for how long people find themselves in a situation where the considered hazardous event can occur. This factor is simplified to be a measure of the probability of the driving scenario taking place in which the hazard can occur (E = Exposure).
Another factor is the failure rate λ of the item itself, which is characterized by undetected random hardware failures and systematic faults. This factor is not considered in the risk assessment because of the fact that the resulting ASIL determines the minimum set of requirements for compliance of the item in order to avoid the aforementioned failures.

More information about the hazard analysis and risk assessment can be found in (Schlummer & Meyna, 2007).

3.2.1. Estimation of Severity

The hazard classification has its focus on the harm of endangered persons. This includes the driver of the vehicle causing the hazard, possible passengers and other traffic participants as for example cyclists, pedestrians or occupants of other vehicles. The severity of potential harm to these persons must be estimated for each hazardous event. It is assigned to one of four classes: S0, S1, S2 or S3 (see Table 1).

Table 1: Classes of Severity

Class	Description	Reference
S0	No injuries	AIS 0
S1	Light and moderate injuries	More than 10% probability of AIS 1-2
S2	Severe and life-threatening injuries	More than 10% probability of AIS 3-4

	(survival probable)	
S3	Life-threatening injuries (survival uncertain), fatal injuries	More than 10% probability of AIS 5-6

The reference AIS (Abbreviated Injury Scale) supports the above classification. The individual injury severity caused by accidents can be classified with help of the AIS. This classification uses seven steps from AIS 0 until AIS 6. A more detailed description of the AIS stages can be found in ISO 26262-3.
The severity class S0 can be assigned when the consequences of an unintended behavior of the item only lead to material damage and do not involve damage to persons. If a hazard is assigned to S0, no ASIL assignment (see chapter 3.3) is required.

3.2.2. Estimation of probability of Exposure in the operational situation

The probability of exposure of each operational situation must be estimated. It is assigned to one of five classes: E0, E1, E2, E3 or E4 (see Table 2).

Table 2: Classes of probability of exposure regarding operational situations

Class	Description	Definition of duration / probability of exposure	Definition of frequency
E0	Incredible	-	-
E1	Very low probability	Not specified	Situations that occur less often than once a year for the great majority of drivers
E2	Low probability	< 1% of average operating time	Situations that occur less often than a few times a year for the great majority of drivers
E3	Medium probability	1-10% of average operating time	Situations that occur less often than once a month or more often for the great majority of drivers
E4	High probability	> 10% of average operating time	Situations that occur almost every drive on average

The scope of ISO 26262 encompasses driving or operating situations of vehicles that range from everyday situations like parking and driving in the city or on the highway to extreme driving situations. When a situation may become hazardous if a failure occurs while the situation is present, the probability of exposure can be estimated by the proportion of total operating time. It is possible though that some estimations are more appropriate when using the frequency of occurrence. Examples for all classifications of driving and operating situations of both approaches can be found in ISO 26262-3.
Class E0 may be assigned for those situations which are considered to be extremely unusual or incredible. Examples include very unusual co-occurrences of circumstances, such as a vehicle involved in an incident

which includes an airplane landing on a highway, and natural disasters like hurricanes or earthquakes. If a hazard is assigned to E0, no ASIL assignment (see chapter 3.3) is required.

3.2.3. Estimation of Controllability

One further step is the estimation of the controllability of each hazardous incident. It is assigned to one of four classes: C0, C1, C2 or C3 (see Table 3).

Table 3: Classes of Controllability

Class	Description	Definition	Examples
C0	Controllable in general	Controllable in general	Unexpected increase of radio volume
C1	Simply controllable	99% or more of all drivers or other traffic participants are usually able to avoid a specific harm	Starting with a locked steering column
C2	Normally controllable	90% or more of all drivers or other traffic participants are usually able to avoid a specific harm	Total light failure at medium or high speed on an unlighted road
C3	Difficult to control or uncontrollable	Less than 90% of all drivers or other traffic participants are usually able to avoid a specific harm	Total loss of breaking performance

The classification of the controllability is connected to the estimation of the probability that a driver or other traffic participants are able to handle and avert the imminent hazardous event. The driver is characterized by the following facts:

- he is in an appropriate condition to drive (e.g. not exhausted),
- he has the appropriate driver training (driver's license) and
- he is complying with legal regulations.

A foreseeable misuse must be considered during the hazard classification as well.

Class C0 may be assigned for hazards addressing the unavailability of the item if it does not affect the safe operation of the vehicle (fro example driver assistance systems). If a hazard is assigned to C0, no ASIL assignment (see chapter 3.3) is required.

3.3. Risk assessment

The Automotive Safety Integrity Level (ASIL) describes in four classes (ASIL A, ASIL B, ASIL C and ASIL D) the specification of the risk and its requirements for risk reduction. ASIL A represents the lowest risk reduction class and ASIL D the highest one. The estimation parameters S (severity), E

(exposure) and C (controllability) for each hazardous event have to be used and combined in accordance with Table 4 to yield the ASIL.

Table 4: ASIL determination

		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

In addition to the four ASIL, another class (QM, Quality Management) is introduced which denotes no requirement in accordance with ISO 26262.
For each hazardous event evaluated in the hazard analysis, a safety goal must be determined. Safety goals are the top level safety requirements for the item. They do not include technological solutions but rather functional objectives. Safety goals lead to functional safety requirements which are needed to avoid an unreasonable risk for each hazard. The safety goal gets the same ASIL as the corresponding hazardous event. If similar safety goals are determined, they can be combined into one safety goal. Then, the highest ASIL must be assigned to this combined safety goal.
In the next steps, functional safety requirements have to be derived from the safety goals. Furthermore, these requirements have to be allocated to the preliminary architectural elements of the item in order to ensure the required functional safety. The technical safety concept follows the functional safety concept. There, technical safety requirements have to be specified and allocated to hard- and software parts of the item. The technical safety requirements refine the functional safety concept.

3.4. Automotive example

The following example with the given information is not entitled to be correct. It shall simply describe the procedure of the hazard analysis and risk assessment.
The considered system in the example is an electronic parking brake (EPB) with the functionality to automatically activate the parking brake if the standstill of the vehicle is identified. The considered malfunction shall be the activation of the parking brake without request, which means without standstill detection. In the situation of driving on a country road the malfunction could lead to a sudden and unwanted brake actuation at the rear-wheel. This could cause skidding. The assignment to the classification of the parameters could be as follows:

- S3 (life-threatening or fatal injuries),
- E4 (situation that occurs almost every drive on average) and
- C3 (difficult to control).

The combination of these parameters in accordance with Table 4 then yields ASIL D. A possible safety goal determined for the considered hazard could be "An activation of the parking brake while driving must be avoided".

4. Methods for qualification and quantification of safety and reliability issues

Safety and reliability analyses can support some of the above mentioned activities. Depending on the determined ASIL, inductive and/or deductive analyses have to be carried out in order to identify the causes and effects of systematic failures while specifying the system design as well as verifying and validating the safety process.
In general, safety analyses examine the consequences of faults and failures on items considering their functions, behavior and design. They contribute to the identification of new functional or non-functional hazards which were previously not considered during the hazard analysis and risk assessment. They also provide information about conditions and causes that could lead to the violation of a safety goal or safety requirement due to random hardware failures.
System safety and reliability analysis methods can be labeled as either being an inductive or deductive technique. Those terms can be defined after (Ericson, 2005) as follows. A deductive reasoning can be described as a logical process in which a conclusion is drawn from a set of premises and contains no more information than the premise taken collectively. On the other hand, an inductive reasoning is a logical process in which a conclusion is proposed that contains more information than the observation or experience on which it is based. This means that an inductive analysis would be used to identify hazards without any proven assurance of the

casual factors, while a deductive analyst attempts to find the specific causal factors for hazards that have been identified before. A combination of deductive and inductive methods guarantees a analysis of the item which is as comprehensive as possible.
Furthermore, the techniques can be divided into qualitative and quantitative analysis methods. In qualitative analyses, qualitative criteria are being used to categorize special parameters with qualitative definitions. Qualitative methods are also being used for identifying faults and failures. Examples are the FMEA (Failure Mode and Effects Analysis) and the qualitative FTA (Fault Tree Analysis). Quantitative analysis technologies involve the use of numerical or quantitative data to gain a quantitative result. These results are more an estimation than an exact number because the results can be biased by the accuracy of the inputs. Examples are the quantitative FTA, Markov models and RBD (Reliability Block Diagrams).
As seen above, the Fault Tree Analysis is a qualitative safety and reliability analysis method that can be evaluated quantitatively. The method was originally developed in the early sixties in the Bell Laboratories during a project to evaluate the Minuteman Launch Control System. Meanwhile, the FTA has become an important tool in system design and development and is an established technique for safety and reliability issues. In many engineering disciplines it has become one of the standard methods for quantitative approaches.
With the help of the FTA, it is possible to analyze, visually display and evaluate failure paths in a system. The basic concept is the translation of the failure behavior of a physical system into a logical mode and visual diagram. Relationships within the system and root failure paths can easily be found in the segments of the FTA diagram. FTA is based on the Boolean algebra and provides possible causes for a given undesired event, the so called Top Event. This event is often an undesired state of the analyzed system (usually a state that can be considered as critical from a safety or reliability standpoint). It can be determined by a hazard analysis. The system is then analyzed in the context of its environmental conditions to find all combinations of possible faults/failures of components or sub-systems which lead to the undesired event. Those faults/failures are the so called basic events of the fault tree. In order to evaluate the fault tree quantitatively, quantitative data (e.g. failure rates, probabilities of failure) must be assigned to the basic events.
The fault tree itself is a graphical presentation of these combinations. It is tailored to the Top Event and so it is not a model for all possible causes for the system failure.

For more information about the Fault Tree Analysis see (Meyna and Pauli, 2003) or (Vesely, 2002).

Part 5 of ISO 26262 gives in the informative part target values for the violation of a safety goal due to random hardware failures depending determined ASIL. The target value for ASIL D is for example $<10^{-8}h^{-1}$. Other target values can be used as well if available, for example derived from field data from well-trusted designs or derived from quantitative analysis techniques applied on similar well-trusted designs using well known failure databases.
However, in order to provide evidence that the target values are achieved, a quantitative analysis of the hardware architecture of the item can be performed. One technique to be used is the FTA.
As a result of the hazard analysis and risk assessment, safety goals are derived for each considered hazardous event. In order to get the undesired event for the FTA, the safety goal can be negated. For the automotive example from chapter 3.4 this could be "Activation of parking brake while driving". This will be the Top Event of the fault tree. Then, all realistic combinations of faults/failures that will result in the occurrence of this event must be identified and modeled in the FTA. Quantitative data must be assigned to the basic events of the fault tree to get a quantitative result for the Top Event. This result must be compared with target value from ISO 26262.

5. Conclusion

The hazard analysis and risk assessment is one of the major tasks of the upcoming standard for functional safety within the automotive industry. Potential hazards are systematically identified, which can result from normal functioning, malfunctioning and non-functioning of the item. An Automotive Safety Integrity Level as a specification of the risk and its requirements for risk reduction is assigned to each considered hazardous situation. Therefore, safety goals and safety requirements must be determined. Depending on the assigned ASIL, target values for the violation of a safety goal due to random hardware failure must be met. In order to show that these values are achieved, quantitative analysis of the hardware architecture can be performed. One of the methods for qualification and quantification of safety and reliability issues is the Fault Tree Analysis, which is an established technique in the automotive industry.

6. References

1. C.A. Ericson: *Hazard analysis techniques for system safety*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2005.
2. ISO/DIS 26262: *Road Vehicles – Functional Safety*. International Organization of Standardization, 2009.

3. C. Jung: *Introduction in ISO WD 26262*. ISO TC22 SC3 WG16 Functional Safety, 2006.
4. A. Meyna, B. Pauli: *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik*. Hanser Verlag, München, 2003.
5. M. Schlummer, A. Meyna: *Risikoanalyse in der Automobilindustrie*. Zeitschrift für die gesamte Wertschöpfungskette Automobilwirtschaft (ZfAW), Heft Nr. 2/2007.
6. W. Vesely: *Fault Tree Handbook with Aerospace Applications*. NASA, 2002.

Streszczenie: *Bezpieczeństwo i niezawodność stanowią kluczowe zagadnienia aktualnego i przyszłego postępu w dziedzinie pojazdów samochodowych, przy którym firmy muszą się uporać z wzrastającą funkcjonalnością i złożonością funkcji samochodu opartych na oprogramowaniu. Nowe funkcje nie znajdują się wyłącznie w zakresie wspomagania kierowcy – większość nowych funkcji samochodu jest i będzie związana z bezpieczeństwem jak np. kontrola dynamiki pojazdu lub aktywne i pasywne systemy bezpieczeństwa. Rozwój i integracja tych funkcji zwiększy potrzebę bezpieczeństwa przy opracowywaniu systemu. Nowa ukazująca się norma samochodowa bezpieczeństwa funkcjonalnego (ISO 26262), która pochodzi od rodzajowej normy bezpieczeństwa funkcjonalnego IEC 61508 i winna spełniać specyficzne potrzeby dziedziny zastosowań systemów E/E w pojazdach drogowych, dostarczy wytycznych pozwalających uniknąć wzrastających ryzyk wynikających z błędów systemu i losowych błędów sprzętowych poprzez dostarczenie wykonalnych procesów i możliwych do spełnienia warunków. Jasnym jest, że aspekty i metody bezpieczeństwa i niezawodności techniki są wdrożone, a we wczesnych stadiach procesu opracowania stosuje się odpowiednie metody. Jest to jednym z wymagań nowej ISO 26262, która wprowadza tzw. żywotność bezpieczeństwa samochodowego, aby poradzić sobie z wszystkimi tymi czynnościami i przebiegami, które są konieczne dla zagwarantowania funkcjonalnego bezpieczeństwa samochodowych systemów E/E. Niżej przedstawimy krotki przegląd nadchodzącej normy samochodowej, wg niej nowy cykl trwałości bezpieczeństwa i związanych czynności w celu zapewnienia funkcjonalnego bezpieczeństwa systemów związanych z bezpieczeństwem. Głównym celem tego artykułu jest wykazanie relewantności i ważności jednego z głównych zadań w ramach ISO 26262: procesu analizy ryzyka i oceny ryzyka, tak jak to jest obecnie praktykowane w przemyśle samochodowym. Na przykładzie z sektora samochodowego tłumaczymy podstawowe kroki tej metody dla określenia* ***poziomu nienaruszalności bezpieczeństwa*** *(ASIL). W zależności od ASIL konieczne jest wyprowadzenie wymagań bezpieczeństwa jako wyniku nowej normy dotyczącej cech nienaruszalności bezpieczeństwa. Ponadto artykuł ten tłumaczy związek pomiędzy procesem funkcjonalnego bezpieczeństwa samochodowego z metodami kwalifikacji i kwantyfikacji zagadnień bezpieczeństwa i niezawodności. W celu podania przykładu jednej z tych metod, które są używane do analizy ryzyka i jego oceny i które przyczyniają się do walidacji i weryfikacji procesu bezpieczeństwa, posłużymy się* ***„Analizą Drzewa Uszkodzeń”****.*

Słowa kluczowe: *bezpieczeństwo funkcjonalne, analiza ryzyka i ocena ryzyka, poziom nienaruszalności bezpieczeństwa samochodowego, Analiza Drzewa Uszkodzeń*